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

WSOU INVESTMENTS, LLC D/B/A BRAZOS LICENSING AND DEVELOPMENT, Plaintiff, v. ARISTA NETWORKS, INC. Defendant.	CIVIL ACTION NO. 6:20-cv-1083 JURY TRIAL DEMANDED

BRAZOS COMPLAINT FOR
PATENT INFRINGEMENT AND JURY DEMAND

Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development ("Brazos"), by and through its attorneys, files this Complaint for Patent Infringement against defendant Arista Networks, Inc. ("Arista") and alleges as follows:

1.   This Complaint arises from Arista's unlawful infringement of the following United States patents owned by Brazos: United States Patent Nos. 7,409,715 ("'715 Patent"); 8,472,447 ("'447 Patent"); and 9,450,884 ("'884 Patent") (collectively, the "Asserted Patents").

Parties

2.   Plaintiff Brazos is a limited liability corporation organized and existing under the laws of Delaware, with its principal place of business at 605 Austin Avenue, Suite 6, Waco, Texas 76701.

3.   Defendant Arista Networks, Inc. is a corporation organized under the laws of the State of Delaware, with its principal place of business at 5453 Great America Parkway, Santa Clara, California 95054. Arista is doing business, either directly or through its agents, on an ongoing basis in this judicial district and elsewhere in the United States, and has a regular and

established place of business in this judicial district. Arista may be served with process through its registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

Jurisdiction & Venue

4.   This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

5.   This Court has personal jurisdiction over Arista in this action because Arista has committed acts of infringement of the Asserted Patents within this District giving rise to this action, and has established minimum contacts with this forum such that the exercise of jurisdiction over Arista would not offend traditional notions of fair play and substantial justice. Arista, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, making, using, importing, offering to sell, and selling products that infringe the Asserted Patents. Notably, Arista has repeatedly admitted or failed to dispute that this Court has personal jurisdiction over Arista in patent actions. *See, e.g.*, Answer ¶ 8, *Proven Networks, LLC v. Arista Networks, Inc.*, 6:20-cv-00281 (W.D. Tex. Jun. 22, 2020), ECF No. 13; Answer ¶ 5, *Intellectual Ventures I LLC et al v. Arista Networks, Inc.*, 6:20-cv-00749 (W.D. Tex. November 5, 2020), ECF No. 9. Notably *Proven Networks* involves many of the same accused products that are at issue here.

6.   Venue is proper in this District under 28 U.S.C. § 1400(b). Arista is registered to do business in Texas, and upon information and belief, Defendant has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, importing, offering to sell, and selling products that infringe the Asserted Patents. Arista

has a regular and established place of business in the District, including corporate offices at The

Terrace, Building II, Suite 420, 2700 Via Fortuna, Austin, Texas 78746.[1]

7.   In a recent case, Arista admitted that this federal judicial district is a proper venue

for patent infringement actions against it. *See, e.g.*, Answer ¶ 9, *Proven Networks, LLC v. Arista*

Networks, Inc., 6:20-cv-00281 (W.D. Tex. Jun. 22, 2020), ECF No. 13 (admitting venue is proper

in this district). Notably, *Proven Networks* involves many of the same accused products that are at

issue here. Arista also admitted it has transacted business in this district. *See, e.g.*, Answer ¶ 9,

Proven Networks, LLC v. Arista Networks, Inc., 6:20-cv-00281 (W.D. Tex. Jun. 22, 2020), ECF

No. 13.

Count 1
(Infringement of the '715 Patent)

8.   Brazos repeats and re-alleges the allegations in the preceding paragraphs as if fully

set forth herein.

9.   On August 5, 2008, the U.S. Patent & Trademark Office duly and legally issued the

'715 Patent entitled "Mechanism for detection of attacks based on impersonation in a wireless

network." A true and correct copy of the '715 Patent is attached as Exhibit A to this Complaint.

10.   Brazos is the owner of all rights, title, and interest in and to the '715 Patent,

including the right to assert all causes of action arising under the '715 Patent and the right to any

remedies for the infringement of the '715 Patent.

11.   Claim 1 of the '715 Patent recites:

> 1. A method for detecting impersonation based attacks at a wireless node of
> a wireless communication network, comprising the steps of:

---

[1] *See, e.g.*, https://www.arista.com/en/company/contact-us, last visited November 25, 2020
(showing Austin office address).

a) operatively connecting the wireless node with an intrusion detection module and providing the intrusion detection module with a copy of original data frames transmitted by the wireless node over a wireless interface;

b) detecting at the intrusion detection module incoming data frames received over the wireless interface;

c) comparing at the intrusion detection module the information in the copy with the information in the incoming data frames; and

d) recognizing an impersonating attack when the intrusion detection module determines that the information in the copy differs from the information in the incoming data frames.

12.   Arista has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 1, of the '715 Patent in violation of 35 U.S.C. § 271(a) because Arista makes, uses, offers for sale, sells, and/or imports certain products ("'715 Accused Products"), including within this Judicial District, such as the Arista Wireless Intrusion Prevention System (WIPS) with Marker Packet auto-classification technology implemented on including but not limited to the C–120, C-110. C–100, C-230, C-260, C-230E, C-130, C-130E, W–118, O-235, O-235E, O-105, O-105E Access Points ("AP"). Arista's infringing use of the '715 Accused Products includes its internal use and testing of the '715 Accused Products.

13.   The '715 Accused Products satisfy all claim limitations of one or more of the claims of the '715 Patent, including at least claim 1.

14.   For example, the '715 Accused Products implement a method for detecting impersonation based attacks at a wireless node of a wireless communication network. The Arista Wireless Intrusion Prevention System (WIPS) is used to provide various threat detection, classification and prevention techniques while minimizing the number of false alarms raised. Arista WIPS implements a Marker Packet technology which performs network connectivity-based

AP autoclassification to automatically enforce network security.[2] The WIPS classification systems classify the visible APs that are part of the network and marks them as "Authorized", "External" and "Rogue" APs.[3] Rogue APs are unauthorized APs that may be installed in the enterprise wired network without administrator knowledge. One of the most common types of threats that occur in a wireless network are caused by these Rogue APs since they allow unauthorized access to private networks (*i.e.*, impersonation based attacks).[4] The WIPS system classifies the rogue and external APs.[5] Thus it detects impersonation based attacks at a wireless node of a wireless communication network.

15.   The '715 Accused Products also comprise operatively connecting the wireless node with an intrusion detection module and providing the intrusion detection module with a copy of original data frames transmitted by the wireless node over a wireless interface. A WIPS sensor (an intrusion detection module) is connected with an authorized AP and Rogue AP (a wireless node) through the enterprise wired network.[6] The WIPS sensor (or the intrusion detection module) injects the Marker packets or those with a unique identifier (or original data frames) into the wired network. The packets (or data frames) are relayed to the wireless side (or wireless interface) of the WIPS sensor (or intrusion detection module) by the APs (or wireless node) present in the network. They (data frames) are detected over the air by the wireless side (or wireless interface) of WIPS

---

[2] https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf,
 Page 1, Last accessed on July 26, 2020.
[3] *Id.* at Page 2.
[4]https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/Arista-Review-of-Detection-
Classification-and-Prevention-Techniques-in-WIPS.pdf, Page 2, Last accessed on July 26, 2020.
[5] https://wifihelp.arista.com/post/rogue-aps-and-marker-packets/?pdf=445, Page 4, Last accessed
on July 26, 2020.
[6] https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf,
 Page 4, Last accessed on July 26, 2020.

sensor (or intrusion detection module).[7] The WIPS sensor can also inject the marker packets from the wireless-side (or wireless interface) of the sensor.[8]

16.   The '715 Accused Products also comprise detecting at the intrusion detection module incoming data frames received over the wireless interface. The marker packets (or incoming data frames) relayed by the AP are detected at the wireless side (or wireless interface) of the WIPS sensor (or intrusion detection module).[9] Likewise, the '715 Accused Products compare at the intrusion detection module the information in the copy with the information in the incoming data frames. As per the WIPS Marker-packet auto classification technology, marker packets (or data frames) are injected through the wire-side (or the wire interface) of the WIPS sensor (or intrusion detection module), which are then relayed by the AP and are detected at the wireless side (or the wireless interface) of the WIPS sensor (or the intrusion detection module).[10]

17.   The '715 Accused Products also comprise recognizing an impersonating attack when the intrusion detection module determines that the information in the copy differs from the information in the incoming data frames. The AP auto-classification segregates APs into three categories: authorized (managed APs in the enterprise wired network which the administrator is aware of), external (unmanaged APs in the wireless network which are not connected to the monitored enterprise wired network), and rogue (unauthorized APs installed in the enterprise wired network which is the administrator is not aware of).[11] As per the WIPS Marker-packet auto

---

[7]   https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/Arista-Review-of-Detection-Classification-and-Prevention-Techniques-in-WIPS.pdf, Page 3, Last accessed on July 26, 2020.
[8]   https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf, Page 4, Last accessed on July 26, 2020.
[9]   https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/Arista-Review-of-Detection-Classification-and-Prevention-Techniques-in-WIPS.pdf, Page 3, Last accessed on July 26, 2020.
[10] *Id.*
[11]   https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf, Page 2, Last accessed on November 18, 2020.

classification technology, marker packets (or data frames) are injected through the wire-side of the WIPS sensor (or intrusion detection module), which are then relayed by the AP and are detected at the wireless side of the WIPS sensor.[12] This technique avoids false alarms in that it never marks rogue APs (recognizing they are an impersonating attack) when the WIPS Marker-packet is not received at the target host (determining that the information in the copy differs from the information in the incoming data frames).[13]

18.   Arista has received notice and actual or constructive knowledge of the '715 Patent and the infringing nature of the accused product since at least the date of service of this Complaint.

19.   Since at least the date of service of this Complaint, through its actions, Arista has indirectly infringed and continues to indirectly infringe the '715 Patent in violation of 35 U.S.C. § 271(b). Arista has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to directly infringe the '715 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the '715 Accused Products. Examples of such advertising, promoting, and/or instructing include the documents at:

- https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/Arista-Review-of-Detection-Classification-and-Prevention-Techniques-in-WIPS.pdf

- https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf

---

[12] *Id.* at Page 4.
[13] *Id.*

- https://wifihelp.arista.com/post/rogue-aps-and-marker-packets/?pdf=445

- https://www.arista.com/assets/data/pdf/Whitepapers/Arista-WIPS-Whitepaper.pdf

20.   Arista does so knowing and intending that its customers and end users will commit these infringing acts. Arista also continues to make, use, offer for sale, sell, and/or import the '715 Accused Products, despite its knowledge of the '715 Patent, thereby specifically intending for and inducing its customers to infringe the '715 Patent through the customers' normal and customary use of the '715 Accused Products.

21.   In addition, Arista has indirectly infringed and continues to indirectly infringe the '715 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '715 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

22.   For example, Arista is aware that the Arista Wireless Intrusion Prevention System (WIPS) with Marker Packet auto-classification technology included in the '715 Accused Products enables such products to operate as described above and that such functionality infringes the '715 Patent, including claim 1. Arista continues to sell and offer to sell such products in the United States after receiving notice of the '715 Patent and how the products' functionality infringes that patent.

23.   The infringing aspects of the '715 Accused Products can be used only in a manner that infringes the '715 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

24.   Brazos has suffered damages as a result of Arista's direct and indirect infringement of the '715 Patent in an amount adequate to compensate for Arista's infringement, but in no event less than a reasonable royalty for the use made of the invention by Arista, together with interest and costs as fixed by the Court.

Count 2
(Infringement of the '447 Patent)

25.   Brazos repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

26.   On June 25, 2013, the U.S. Patent & Trademark Office duly and legally issued the '447 Patent entitled "IP multicast snooping and routing with multi-chassis link aggregation." A true and correct copy of the '447 Patent is attached as Exhibit B to this Complaint.

27.   Brazos is the owner of all rights, title, and interest in and to the '447 Patent, including the right to assert all causes of action arising under the '447 Patent and the right to any remedies for the infringement of the '447 Patent.

28.   Claim 15 of the ''447 Patent recites:

15. A method for performing Internet Protocol (IP) multicast snooping on an aggregation switch in a multi-chassis system, comprising:

receiving snooping information via at least external ports coupled to at least one edge node and at least one network node;

storing the snooping information within a database;

sharing the snooping information substantially in real-time with a remote aggregation switch via a virtual fabric link (VFL) therebetween, wherein the remote aggregation switch is active and in a separate physical chassis

building respective forwarding vectors for multicast traffic flows received from the at least one network node based on the snooping information; and

determining a multicast index for a received multicast traffic flow to set-up hardware paths for forwarding the received multicast traffic flow to the external ports in a virtual local area network (VLAN) that requested the received multicast

traffic flow via the at least one edge node, the multicast index being used globally between the aggregation switch and the remote aggregation switch.

29.   Arista has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 15, of the '447 Patent in violation of 35 U.S.C. § 271(a) because Arista makes, uses, offers for sale, sells, and/or imports certain products ("'447 Accused Products"), including within this Judicial District, such as Arista's switches that support Internet Group Management Protocol (IGMP) snooping + Multi-chassis Link Aggregation (MLAG) including but not limited to Arista 7260X, 7280R, 7250X, 7280R2, 7260X3, 7280R3, 7280E, 720XP 7020R, 7050X, 7050X2, 7060X, 7060X2, 7050X3, 7050, 7160, 7170, 7150, 7010, 7500R2, 7500R, 7500E, 7300X, 7320X, 7300X3, 7368, and 7500R3 Series switches. Arista's infringing use of the '447 Accused Products includes its internal use and testing of the '447 Accused Products.

30.   The '447 Accused Products satisfy all claim limitations of the one or more claims of the '447 Patent, including at least claim 15.

31.   By way of example, the Arista 7500R Series modular switches are high-performance universal spine switches. They combine 100G density with Internet scale table sizes and comprehensive L2 and L3 features. These switches can do internet protocol (IP) multicast snooping when the switches are operating in multi-chassis link aggregation mode (to interconnect two switches and use them as one logical switch), as described in claim 15.[14] The other '447 Accused Products support the same accused features.[15]

---

[14]   https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf,   Page   2-7,   Last accessed November 18, 2020.
[15]   https://www.arista.com/en/support/product-documentation/supported-features,   Last   accessed April 23, 2020.

32.   The '447 Accused Products practice a method for performing Internet Protocol (IP) multicast snooping on an aggregation switch in a multi-chassis system. The '447 Accused Products support multicast transmissions through IGMP, IGMP Snooping (*i.e.*, IP multicast snooping), and PIM-SM.[16] The '447 Accused Products also support Multi-Chassis Link Aggregation (MLAG) feature, which allows interconnection of two Arista 7000 Family switches (*i.e.*, an aggregation switch in a multi-chassis system) and for use as one logical switch. They further support MLAG to work in conjunction with IGMP snooping.[17]

33.   Further, the method practiced by the '447 Accused Products comprises of receiving snooping information via at least external ports coupled to at least one edge node and at least one network node. The '447 Accused Products support multicast transmissions.[18] IP Multicasting works by forming multicast groups. The host nodes (*i.e.*, network nodes) send IGMP packets to a multicast router to join or leave a multicast group. The '447 Accused Products examine these IGMP packets to extract information about hosts that want to join a multicast group.[19] The '447 Accused Products in MLAG configuration are deployed at various places in the network wherein the network node is connected to the accused product via an edge node.[20]

---

[16] *Id.*

[17] *Id.*; https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, Page 1, Last accessed April 23, 2020.

[18] https://www.arista.com/en/um-eos/eos-section-38-1-overview#ww1151209, Last accessed November 24, 2020.

[19] https://www.arista.com/en/support/product-documentation/supported-features, Last accessed April 23, 2020; https://www.arista.com/en/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Page 2676, Last accessed April 23, 2020.

[20] https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, Page 2, Last accessed April 23, 2020.

34.   The snooping information is stored within a database in the on-chip memory on the switch.[21]

35.   When the '447 Accused Products are in MLAG configuration, the MLAG peer switches (*i.e.*, aggregation switches) are connected by a peer link (*i.e.*, virtual fabric link (VFL)). This peer link acts as an interface for the two switches to communicate with each other, and the snooping information is synchronized over this peer link (*i.e.*, sharing the snooping information substantially in real-time with a remote aggregation switch).[22] In this configuration, the remote aggregation switch is both active and in a separate physical chassis.[23]

36.   The '447 Accused Products examine the IGMP join or leave packets to extract snooping information about hosts (*i.e.,* network nodes) that want to join multicast group. This extracted snooping information is used to build the group multicast list (*i.e.*, the forwarding vector), which is stored in the switch. This multicast list includes information of various multicast groups, the network nodes that are part of the group and the port to which these nodes are connected. The MLAG peers use this multicast list to forward multicast packets to the external ports that are connected to the nodes of the multicast group.[24]

---

[21] https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Page 2676,   Last   accessed   April   23,   2020; https://www.arista.com/assets/data/pdf/Whitepapers/Arista7500RSwitchArchitectureWP.pdf, Page 1, Last accessed April 23, 2020.
[22] https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Page 739, Last accessed April 23, 2020; https://eos.arista.com/forum/igmpsnooping-in-mlag/, Page 1, Last accessed April 23, 2020.
[23] https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, Page 2, Last accessed April 23, 2020; https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Pages 748, 766, Last accessed April 23, 2020.
[24] https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Page 2676, Last accessed April 23, 2020.

37.   The method practiced by the '447 Accused Products comprises determining a

multicast index for a received multicast traffic flow to set-up hardware paths for forwarding the

received multicast traffic flow to the external ports in a virtual local area network (VLAN) that

requested the received multicast traffic flow via the at least one edge node, the multicast index

being used globally between the aggregation switch and the remote aggregation switch. The '447

Accused Products store the snooping information that is extracted from IGMP packets to the group

multicast list. The switch uses this multicast list to forward multicast packets to nodes that joined

the group and to prune multicast traffic from links that are not in the group.[25] The '447 Accused

Products support the IEEE 802.1Q standard. When a multicast frame from a network node which

is part of a virtual local area network (VLAN) arrives at a port, the multicast frame is tagged with

a VLAN tag (*i.e.*, multicast index) based at least on the VLAN that it came from. This frame

enables the switch to set up a hardware path for forwarding the frame to a VLAN that the frame

belongs to (*i.e.*, set-up hardware paths for forwarding the received multicast traffic).[26] The ports

on the switch use this VLAN tag to determine whether to forward the frame or not. If the frame is

tagged for a VLAN that is connected to that port, the port forwards the frame. If the frame is tagged

for a VLAN that is not connected to that port, the port drops the frame. Ports on both the switches

can use this tag to make forwarding decisions (*i.e.*, being used globally between the aggregation

switch and the remote aggregation switch) and this tag is removed once the frame reaches the

egress port of either of the two switches.[27]

---

[25] *Id.*

[26] https://www.arista.com/en/support/product-documentation/supported-features, Last accessed
April 23, 2020.

[27] https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf, Page
1127, Last accessed April 23, 2020.

38.   Arista has received notice and actual or constructive knowledge of the '447 Patent and the infringing nature of the accused product since at least the date of service of this Complaint.

39.   Since at least the date of service of this Complaint, through its actions, Arista has indirectly infringed and continues to indirectly infringe the '447 Patent in violation of 35 U.S.C. § 271(b). Arista has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to directly infringe the '447 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Examples of such advertising, promoting, and/or instructing include the documents at:

- https://www.arista.com/assets/data/pdf/Whitepapers/Arista7500RSwitchArchitectureWP.pdf

- https://www.arista.com/en/support/product-documentation/supported-features

- https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.23.2F-Manual.pdf

- https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag

- https://eos.arista.com/forum/igmpsnooping-in-mlag/

40.   Arista does so knowing and intending that its customers and end users will commit these infringing acts. Defendant also continues to make, use, offer for sale, sell, and/or import the '447 Accused Products, despite its knowledge of the '447 Patent, thereby specifically intending for and inducing its customers to infringe the '447 Patent through the customers' normal and customary use of the '447 Accused Products.

41.   In addition, Arista has indirectly infringed and continues to indirectly infringe the

'447 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or

importing into the United States, the '447 Accused Products with knowledge that they are

especially designed or adapted to operate in a manner that infringes that patent and despite the fact

that the infringing technology or aspects of the products are not a staple article of commerce

suitable for substantial non-infringing use.

42.   For example, Arista is aware that the Internet Group Management Protocol (IGMP)

snooping and Multi-chassis Link Aggregation (MLAG) technology included in the '447 Accused

Products enables such products to operate as described above and that such functionality infringes

the '447 Patent, including claim 15. Arista continues to sell and offer to sell such products in the

United States after receiving notice of the '447 Patent and how the products' functionality infringes

that patent.

43.   The infringing aspects of the '447 Accused Products can be used only in a manner

that infringes the '447 Patent and thus have no substantial non-infringing uses. The infringing

aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-

infringing use.

44.   Brazos has suffered damages as a result of Arista's direct and indirect infringement

of the '447 Patent in an amount adequate to compensate for Arista's infringement, but in no event

less than a reasonable royalty for the use made of the invention by Arista, together with interest

and costs as fixed by the Court.

Count 3
(Infringement of the '884 Patent)

45.   Brazos repeats and re-alleges the allegations in the preceding paragraphs as if fully

set forth herein.

46.   On September 20, 2016, the U.S. Patent & Trademark Office duly and legally

issued the '884 Patent entitled "Software defined networking based congestion control." A true

and correct copy of the '884 Patent is attached as Exhibit C to this Complaint.

47.   Brazos is the owner of all rights, title, and interest in and to the '884 Patent,

including the right to assert all causes of action arising under the '884 Patent and the right to any

remedies for the infringement of the '884 Patent.

48.   Claim 1 of the '884 Patent recites:

1. A method of adjusting bandwidth allocation by a network switching element in
a communications network, the network switching element including a target port,
the method comprising:

monitoring, by the network switching element, a data flow traversing the target port
of the network switching element;

determining, by the network switching element, a bandwidth allocation for the
target port, the bandwidth allocation for the target port being a bandwidth that is
currently allocated for the data flow;

determining, by the network switching element, a fair-share bandwidth allocation
for the target port, the fair-share bandwidth allocation being a proportional
allocation of a total bandwidth of the network switching element; and

adjusting, by the network switching element, the bandwidth allocation for the target
port based on the fair-share bandwidth allocation.

49.   Arista has directly infringed and continues to directly infringe, literally and/or

under the doctrine of equivalents, one or more claims, including at least claim 1, of the '884 Patent

in violation of 35 U.S.C. § 271(a) because Arista makes, uses, offers for sale, sells, and/or imports

certain products ("'884 Accused Products"), including within this Judicial District, such as Arista's

switches including but not limited to Arista 7500R Series, 7500R3 Series, 7800R3 Series, 7280R3

Series, 7280R Series, and 7020R Series switches. Arista's infringing use of the '884 Accused

Products includes its internal use and testing of the '884 Accused Products.

50.   The '884 Accused Products satisfy all claim limitations of at least one or more of the claims of the '884 Patent, including at least claim 1.

51.   By way of example, The Arista 7500R series switches are designed for large virtualized and cloud networks. Arista 7500R series switches use Advanced EOS features for network monitoring, precision timing, VXLAN network virtualization, and EVPN, etc. Arista 7500R series switches use deep buffer virtual output queue (VOQ) architecture to ensure fair allocation of bandwidth among all traffic classes across ports as described in Claim 1. The other accused switches also have infringing functionality.

52.   The '884 Accused Products practice a method of adjusting bandwidth allocation by a network switching element in a communications network, the network switching element including a target port. The '884 Accused Products are switches designed for large virtualized and cloud networks. The '884 Accused Products use Advanced EOS features for network monitoring, precision timing, VXLAN network virtualization, and EVPN. The '884 Accused Products also use deep buffer virtual output queue (VOQ) architecture to ensure fair allocation of bandwidth among all virtual output queues of ports.[28]

53.   The '884 Accused Products provide an architecture of deep buffer virtual output queue (VOQ) for congested network scenarios. The '884 Accused Products also provide an advanced traffic scheduler to fairly allocate bandwidth (*i.e.*, a method of adjusting bandwidth allocation) between all virtual output queues of ports. The VOQ bandwidth allocation is per traffic class and per port.[29]

---

[28] https://www.arista.com/en/products/7500r-series, Page 1, Last accessed on May 28, 2020.
[29] https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf, Page 4, Last accessed on May 28, 2020; https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 1, Last accessed on May 28, 2020.

54.   The method practiced by the '884 Accused Products comprises monitoring, by the network switching element, a data flow traversing the target port of the network switching element. The '884 Accused Products provide a system for managing big data workloads with the help of deep buffer, advanced VOQ architecture, and analysis tools. The analysis tools monitor and analyze the data flow across the switch (*i.e.*, ports of the switch).[30] The '884 Accused Products provide an architecture of deep buffer virtual output queue (VOQ) for congested network scenarios. The '884 Accused Products also provide an advanced traffic scheduler to fairly allocate bandwidth between all virtual output queues of ports. Based on monitoring and analyzing, the VOQ architecture enables fair bandwidth allocation across traffic classes (*i.e.*, flows with different traffic classes) across the ports.[31]

55.   The method practiced by the '884 Accused Products comprise determining, by the network switching element, a bandwidth allocation for the target port, the bandwidth allocation for the target port being a bandwidth that is currently allocated for the data flow. The '884 Accused Products provide a virtual output queuing architecture (VOQ) that fairly allocates bandwidth across traffic classes (*i.e.*, flows with different traffic classes) across the ports. Packets enqueued for transmission in the VOQ are monitored within the software for the '884 Accused Products via per-port interface counters (*i.e.*, a bandwidth allocation for the target port).[32] For example, when a new traffic Class (*e.g.*, traffic flow with Class-A) enters a port, the accused product monitors the

---

[30] https://www.youtube.com/watch?v=KaEFvEib7WY&feature=emb_logo, Timestamp [5:34], Last accessed on May 28, 2020.
[31] https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf, Page 4, Last accessed on May 28, 2020; https://www.arista.com/assets/data/pdf/Whitepapers/BigDataBigBuffers-WP.pdf, Page 4, Last accessed on May 28, 2020; https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 4, Last accessed on May 28, 2020.
[32]   https://eos.arista.com/troubleshooting-egress-queue-drops-on-7280-7500-devices,   Last accessed November 18, 2020.

flow and provides bandwidth to the port as per the bandwidth of incoming data flow (*i.e.*, bandwidth that is currently allocated for the data flow).[33]

56.   The method practiced by the '884 Accused Products comprises determining, by the network switching element, a fair-share bandwidth allocation for the target port, the fair-share bandwidth allocation being a proportional allocation of a total bandwidth of the network switching element. The '884 Accused Products provide an architecture of deep buffer virtual output queue (VOQ) for congested network scenarios. The '884 Accused Products also provide an advanced traffic scheduler to allocate bandwidth fairly (*i.e.*, fair-share bandwidth) between all virtual output queues of ports through at least weighted fair queueing, fixed priority queueing, and hybrid queuing schemes.[34] The VOQ architecture also enables fair bandwidth allocation across traffic classes (*i.e.*, flows with different traffic classes) across the ports.[35] The '884 Accused Products also provide a fair allocation of bandwidth per port and the bandwidth allocation among the shared ports is proportionate to the data flow.[36]

57.   The method practiced by the '884 Accused Products comprises adjusting, by the network switching element, the bandwidth allocation for the target port based on the fair-share bandwidth allocation. The deep buffer VOQ architecture allocates a fair distribution of bandwidth

---

[33] https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf, Page 4, Last accessed on May 28, 2020; https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 1, Last accessed on May 28, 2020.
[34] https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf, Page 4, Last accessed on November 18, 2020.
[35] https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf, Page 4, Last accessed on May 28, 2020; https://www.arista.com/assets/data/pdf/Whitepapers/BigDataBigBuffers-WP.pdf, Page 4, Last accessed on May 28, 2020; https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 4, Last accessed on May 28, 2020.
[36] https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 6, Last accessed on May 28, 2020.

based on monitoring tools. The bandwidth of the flow is adjusted based on fair-share bandwidth allocation.[37]

58.   Arista has received notice and actual or constructive knowledge of the '884 Patent and the infringing nature of the accused product since at least the date of service of this Complaint.

59.   Since at least the date of service of this Complaint, through its actions, Arista has indirectly infringed and continues to indirectly infringe the '884 Patent in violation of 35 U.S.C. § 271(b). Arista has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to directly infringe the '884 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Examples of such advertising, promoting, and/or instructing include the documents at:

- https://www.arista.com/en/products/7500r-series

- https://www.arista.com/assets/data/pdf/Datasheets/7500RDataSheet.pdf

- https://www.arista.com/assets/data/pdf/Whitepapers/BigDataBigBuffers-WP.pdf

60.   Arista does so knowing and intending that its customers and end users will commit these infringing acts. Arista also continues to make, use, offer for sale, sell, and/or import the '884 Accused Products, despite its knowledge of the '884 Patent, thereby specifically intending for and inducing its customers to infringe the '884 Patent through the customers' normal and customary use of the '884 Accused Products.

---

[37] https://www.arista.com/en/products/7500r-series, Page 4, Last accessed on May 28, 2020; https://inog.net/files/iNOG8-Arista-Deep-Buffers.pdf, Page 6, Last accessed on May 28, 2020.

61.   In addition, Arista has indirectly infringed and continues to indirectly infringe the '884 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '884 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

62.   For example, Arista is aware that the technology described above included in the '884 Accused Products enables such products to operate as described above and that such functionality infringes the '884 Patent, including claim 1. Arista continues to sell and offer to sell such products in the United States after receiving notice of the '884 Patent and how the products' functionality infringes that patent.

63.   The infringing aspects of the '884 Accused Products can be used only in a manner that infringes the '884 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

64.   Brazos has suffered damages as a result of Arista's direct and indirect infringement of the '884 Patent in an amount adequate to compensate for Arista's infringement, but in no event less than a reasonable royalty for the use made of the invention by Arista, together with interest and costs as fixed by the Court.

Demand for Jury Trial

65.   Brazos hereby demands a jury trial for all issues so triable.

Prayer for Relief

WHEREFORE, Brazos requests the that the Court:

(a)   enter judgment that Arista infringes one or more claims of the Asserted Patents

literally and/or under the doctrine of equivalents;

(b)   enter judgment that Arista has induced and/or contributed to infringement literally

and/or under the doctrine of equivalents and continues to induce and/or contributed to infringement

of one or more claims of the Asserted Patents;

(c)   award Brazos damages, to be paid by Arista in an amount adequate to compensate

Brazos for such damages, together with pre-judgment and post-judgment interest for the

infringement by Arista of the Asserted Patents through the date such judgment is entered in

accordance with 35 U.S.C. § 284;

(d)   declare this case exceptional pursuant to 35 U.S.C. § 285; and

(e)   award Brazos its costs, disbursements, attorneys' fees, and such further and

additional relief as is deemed appropriate by this Court.

Dated: November 25, 2020   Respectfully submitted,

                                                          By: */s/ Max L. Tribble, Jr.*
                                                              Max L. Tribble, Jr.
                                                              State Bar No. 2021395
                                                              Shawn Blackburn *(pro hac vice)*
                                                              State Bar No. 24089989
                                                              Bryce T. Barcelo *(pro hac vice)*
                                                              State Bar No. 24092081
                                                              SUSMAN GODFREY L.L.P.
                                                              1000 Louisiana Street, Suite 5100
                                                              Houston, Texas 77002-5096
                                                              Telephone: (713) 651-9366
                                                              Fax: (713) 654-6666
                                                              mtribble@susmangodfrey.com
                                                              sblackburn@susmangodfrey.com
                                                              bbarcelo@susmangodfrey.com

                                                              Kalpana Srinivasan *(pro hac vice)*
                                                              State Bar No. 237460
                                                              SUSMAN GODFREY L.L.P.

1900 Avenue of the Stars, 14th Floor
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Fax: (310) 789-3150
ksrinivasan@susmangodfrey.com

**COUNSEL FOR PLAINTIFF WSOU
INVESTMENTS, LLC D/B/A BRAZOS
LICENSING AND DEVELOPMENT**