IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	No. 2:17-cv-00383 (HCM-LRL)
	)	
vs.	)	
	)	
KEYSIGHT TECHNOLOGIES, INC., and IXIA,	)	
	)	
	)	
Defendants.	)	
	)	
	)	

PLAINTIFF CENTRIPETAL NETWORKS, INC.'S OPENING *MARKMAN* BRIEF

I. INTRODUCTION

Centripetal's proposed constructions follow the "canons of construction" that the Federal Circuit has prescribed and this Court follows in construing disputed claim terms and phrases. *See, e.g. Vir2us, Inc. v. Invincea, Inc.*, No. 15-cv-162, 2016 WL 8711512, at *4 (E.D. Va. Feb. 19, 2016). These constructions, based on the clear context of the claims and patent specification, provide clarity and align with the patent which relates to computer networks. Defendants' litigation inspired proposed constructions unnecessarily import limitations from the specification into the claims, provide no additional clarity, and are inconsistent with the teachings of the patent and, in the end, violate fundamental tenets of claim construction. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (holding that the district court should avoid importing limitations from the specification into the claims); *see also Innovad Inc. v. Microsoft Corp.*, 260 F.3d 1326, 1332-33 (Fed. Cir. 2001) (aligning meaning of term with purpose of the patented invention).

A. OVERVIEW OF THE ASSERTED PATENTS

Centripetal was the first in the cybersecurity field to address one of the most serious problems facing information technology today: real-time detection of cybersecurity threats using threat intelligence at the packet level of network data. It is extremely difficult to collect, process, and activate cyber threat intelligence on a network given the sheer volume of data that flows in and out of the system. As the inventor of the first threat intelligence gateway, Centripetal provided a solution to next-gen firewalls that were unable to effectively and efficiently discover and block attacker's activities in real-time due to the increasing amount of network traffic. Centripetal's patented technologies efficiently collect, process, and activate cyber threat intelligence on a network, stopping significant breaches that has allowed the industry to recognize Centripetal as notable leader in the cybersecurity field.

The U.S. Patent Office has awarded Centripetal numerous patents for its innovative and groundbreaking cybersecurity technology. Four of those patents are asserted in the Complaint in this case: U.S. Patent No. 9,264,370 ("the '370 Patent"), U.S. Patent No. 9,413,722 ("the '722 Patent"), U.S. Patent No. 9,560,077 ("the '077 Patent"), and U.S. Patent No. 9,137,205 ("the '205 Patent") (collectively, "Asserted Patents")(*see* Exhibits 1-4[1]). Each of these four patents cover methods and systems for protecting a computer network using steps focused on the configuring of devices to monitor, generate, manipulate, and analyze data packets sent across a network. At a high level, a packet is a particularized unit of data that generally contains the address of its origin and destination, and information connecting it to other related packets that are being sent over a network.

The '205 Patent

Filed on October 22, 2012, the '205 Patent described methods and systems that efficiently analyze large amounts of network traffic at a high resolution and proactively protecting a system from malicious attacks. Generally, the '205 Patent relates to proactive security systems that receive and apply dynamic security policies that perform transformation functions on data packets "on-the-fly," changing them from one state to another.

The '077 Patent

The '077 Patent is related to the '205 Patent and has an effective filing date of October 22, 2012, claiming priority to the '205 Patent. The '077 Patent also relates to proactive (rather than reactive) security systems, and generally concerns configuring a device to receive packets and actively respond to determination by the device based on application of security rules including the modification of a switching matrix of a local area network (LAN). Such security

[1] All exhibits are attached to the Declaration of Hannah Lee in Support of Centripetal's Opening *Markman* Brief.

rules can be generated based on the boundary of a different network than the boundary where the device is, or will be, deployed. The '077 Patent may operate in a network-layer transparent manner, and help conserve processing resources. *See, e.g.*, '077 Patent, Col. 20:53-58; 21:53-58, 22:56-61, 24:8-13. The systems and methods described in the '077 Patent solved the problem of distributing rules generated at one network boundary to other network boundaries, ensuring that threats discovered in one network boundary may be addressed at other network boundaries that may not yet be aware of any such threat.

The '370 Patent

The '370 Patent was filed on February 10, 2015. The '370 Patent solves a variety of problems, including when network devices alter data packets associated with a flow and obfuscate the flow in which a particular packet is associated, making it difficult to ascertain where the packet came from, its destination, and its relationship with other packets of data sent across a network. This disassociation of a particular packet and its original header information can result in the failure of network devices to know if that packet came from a potentially malicious host. The systems and methods described in the '370 Patent solved this problem by finding a way to generate log entries stored in the computer memory that corresponds to packets and helps identify the packets that are sent across a network between devices. Generally, the systems of the '370 Patent take information received from analyzing packets coming into a network, e.g. information regarding the source, destination, time, and application used, and compares it to packets that are leaving the network. For example, the claimed packet correlator described in the '370 Patent employs a novel and highly complex analysis to identify the true source of the packets, e.g. network-layer information, transport-layer information. *See, e.g.*, '370 Patent, Col. 8:25-31. Once the host of the packets has been identified, the identity of the host is

communicated to other devices in the network to prevent other packets with the same network threat identifiers from infiltrating the network. *See, e.g., id.*, Col. 19:57-59.

The '722 Patent

The '722 Patent has an effective filing date of April 17, 2015. The '722 Patent solves a variety of problems, particularly those with newly evolving network threats. *See, e.g.*, '722 Patent, Col. 1:20-34. In one example, the systems described in the '722 Patent identify network threats based on the unique configuration of a "packet-filtering device" to selectively prevent data packets from continuing on to their respective destinations by implementing dynamically created packet-filtering "rules." The packet-filtering device can apply packet-filtering rules based in-part on network threat indicators that can be used by the packet-filtering device to dynamically modify packet flow by selectively preventing packets from continuing to their destination.

II. ARGUMENT

A. '205 PATENT[2]

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet transformation function/functions (Claims 1, 4, 7, 17, 20, 23, 33, 36, 39, 91, 93, 95)[3]	function that transforms one or more packets from one state to another	an operation performed on a packet specified by the dynamic security policy, such as forward or drop

[2] The asserted claims of the '205 Patent are: Claims 1, 4, 7, 17, 20, 23, 33, 36, 39, 91, 93, and 95. Since the service of the parties' preliminary claim constructions, the parties met and conferred and agreed upon the meaning of certain terms which are not included in this brief. The parties agree that the term "packet security gateway" means a gateway computer configured to receive packets and perform a packet transformation function on the packets, and "security policy management server" means a server configured to manage policies and communicate a dynamic security policy to a packet security gateway.

[3] The asserted claims where the relevant term is used are included in parentheses in the tables in this brief.

Centripetal's proposed construction of this term is consistent with the claim language and the specification and covers all the embodiments in the specification. By contrast, Defendants' proposed construction wrongly limits the term to only "forward or drop" and inappropriately removes any act of "transformation." This narrowed construction is clearly wrong as the patent teaches that "patent transformation function/functions" transform one or more packets from one state to another by manipulating packets in order to forward, drop, or route the packets. This can be done in a variety of ways, including replacing headers in the packets, remove information from the headers in the packets, or encapsulating them. *See, e.g.*, '205 Patent, Col. 2:36-40; 2:52-56; 6:56-7:36, 9:44-52; 9:59-10:17; 10:29-46; 10:66-11:30; 14:52-59; 14:66-15:3; 15:18-42; Declaration of Dr. Nenad Medvidovic ("Medvidovic Decl."), ¶¶ 14-15. One of skill in the art would understand that a "patent transformation function" in the context of the claims is a function that transforms one or more packets from one state to another depending on the configuration of the system. *Id.*

Defendants' construction will confuse the jury and is not consistent with the claim language or specification. Some of the asserted claims specifically state that the claimed packet transformation function is "***other*** than forwarding or dropping the packets," but Defendants intentionally include those excluded functions in its claim term. *See* '205 Patent, Col. 20:52-53; 23:11-13; 25:40-42 (emphasis added). The specification also explicitly describes examples of patent transformation functions "other than forwarding or dropping the packets" such as accept, deny, encapsulate, alter/modify the destination address, assign, allow, and route functions. *Id.*, Col. 2:36-40; 2:52-56; 6:56-7:36, 9:44-52; 9:59-10:17; 10:29-46; 10:66-11:30; 14:52-59; 14:66-15:3; 15:18-42; Medvidovic Decl., ¶¶ 14-15. Defendants' construction intentionally adds these excluded packet transformation functions as described in the specification. *See Thorner v. Sony*

Comp. Entmt. Am. LLC, 669 F.3d 1362, 1366 (Fed. Cir. 2012) (holding the district court must not read in limitations from the specification without clear intent to do so). For such reasons, Centripetal's construction, which is most naturally aligned, with the claims and specification is appropriate. *Phillips*, 415 F.3d at 1316 ("The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction") (citation omitted).

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
dynamic security policy/policies (Claims 1, 4, 7, 17, 20, 23, 33, 36, 39, 91, 93, 95)	a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria

Centripetal's proposed construction of this term provides further clarity to the term and keeps it consistent with the definition that the patentee intended as used in the context of the claims and specification as a whole. As well understood by persons of skill in the art, the term "dynamic" means that the policy can be updated based on a set of criteria, and is not a static policy. In contrast to a dynamic policy, a static policy is usually a set policy. Medvidovic Decl., ¶ 16. The claimed "dynamic" security policy, however, is not set and can be updated with additional information. For example, as set forth in Claim 1, the "dynamic security policy" may be updated with different sets of network addresses (e.g. "first set of network addresses," "second set of network addresses," "third set of network addresses"). '205 Patent, Col. 20:28, 20:31, 20:35; Medvidovic Decl., ¶ 16. In addition, the specification describes how dynamic

security policies may include rules that may be configured in time-shifted phases. '205 Patent, Col. 8:63-9:19; Medvidovic Decl., ¶ 16.

Defendants' proposed construction also should be rejected because it makes the claim term redundant of what is already stated in the claim, i.e. "identifies a packet transformation function to be performed on packets corresponding to the specified criteria." *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1237-38 (Fed. Cir. 2016) (construing a claim term to include features of that term already recited in the claims would make those expressly cited feature redundant). The claims state that the dynamic security policy identifies a packet transformation function, and adding this to the definition of the term is unnecessary and creates redundancy. *See, e.g.*, '205 Patent, Col. 20:43-53, 23:3-13, 25:33-42, 33:59-66, 34:5-12, 34:57-61, 35:9-12, 36:4-9, 36:17-22. Thus, the Court should adopt Centripetal's construction which is supported by the well understood meaning of the term to one of skill in the art reading the claims.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
rule/rules (Claims 1, 4, 7, 17, 20, 23, 33, 36, 39, 91, 93, 95)	condition or set of conditions that when satisfied cause a specific action to occur	(i) packet-identifying criteria and (ii) a function to be performed on the identified packets

Centripetal's proposed construction of this term is consistent with how this term is used in the claims, specification as a whole, and commonly understood to those skilled in the art. As used in the claims, the claimed "rules" have an "if, then" purpose by causing specific actions to occur. *See, e.g.*, '205 Patent, Col. 20:23-27 ("at least one rule specifying that all packets associated with network addresses outside of the set of network addresses for which packets should be forwarded should be dropped…"); 21:38-42 ("at least one rule specifying the method comprising routing…"); 26:31-37 ("at least one rule specifying a parameter, and wherein the instructions, when executed, cause the one or more packet security gateways to route…"); *see*

also id., 21:8-14; 22:48-53, 25:10-15, 26:4-7. Centripetal's construction of rule(s) also is consistent with how one of skill in the art would understand the term in the relevant field. *See* Medvidovic Decl., ¶ 17. As the Dictionary of Computer and Internet Terms (2016) states, a "rule" is a "condition-action pair that prescribes the action taken when the condition is met." Ex. 5 at 438. In the context of the claims, the commonly understood meaning makes sense as it encompasses the meaning of rules set forth in the claims and patent specification. *See Hyperphrase Techs., LLC v. Google, Inc.*, 260 Fed. Appx. 274, 280 (Fed. Cir. Dec. 6, 2007) ("A claim construction that excludes an embodiment of the relevant claim(s) is typically incorrect") (citations omitted). Thus, the Court should adopt Centripetal's construction which is supported by the commonly understood meaning of the term to one of skill in the art, in the context of the claims and specification.

B. '077 PATENT[4]

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
rule/rules (Claims 1, 3-5, 7, 9-11, 13, 15-17, 19)	condition or set of conditions that when satisfied cause a specific action to occur	(i) packet-identifying criteria and (ii) a function to be performed on the identified packets

Similar to the construction of this term above in the related '205 Patent, Centripetal's proposed construction of this term is consistent with how this term is used in the claims, specification as a whole, and commonly understood by those skilled in the art. *See, e.g., Superior Indus., Inc. v. Masaba, Inc.*, 650 Fed. Appx. 994, 999 (Fed. Cir. 2016) (holding that the same claim term in related patents is presumed to have the same meaning). As used in the

[4] The asserted claims of the '077 Patent are: Claims 1, 3-5, 7, 9-11, 13, 15-17, and 19. The parties agree that "LAN switch" means a network device configured to send and receive data between computers on a local area network, and a "network-layer address" means an address that identifies a device for communication on the network layer, such as an IP address.

specification, the claimed "rules" have an "if, then" purpose by causing specific actions to occur. *See, e.g.*, '077 Patent, Col. 20:62-66 ("responsive to a determination...corresponds to criteria specified by the one or more rules..."); 23:23-26 ("with at least one rule configured to identify malicious network traffic..."); *see also id.,* Col. 21:22-26; 21:62-66, 22:22-28, 22:36-42, 22:65-23:2, 23:42-48, 24:17-28. Centripetal's construction of rule(s) is how one of skill in the art understands the term in the relevant field. *See* Medvidovic Decl., ¶ 18. As the Dictionary of Computer and Internet Terms (2016) states, a "rule" is a "condition-action pair that prescribes the action taken when the condition is met." Ex. 5 at 438. In the context of the claims, the commonly understood meaning makes sense as it encompasses the meaning of rules set forth in the claims and patent specification. *See Hyperphrase Techs.*, 260 Fed. Appx. at 280 ("A claim construction that excludes an embodiment of the relevant claim(s) is typically incorrect") (citations omitted). Thus, the Court should adopt Centripetal's construction which his supported by the commonly understood meaning of the term to one of skill in the art, in the context of the claims and specification.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
switching matrix of local area network (LAN) switch (Claims 1, 3-5, 7, 9-11, 13, 15-17)	a matrix contained within a local area network switch that may be configured to direct traffic from one device to another device in the network	a structure configured to switch packets received from one or more computers on a local area network to one or more computers on the local area network

Centripetal's construction clarifies that this claim term means a matrix that may be configured to direct traffic from one device to another device in the network. Defendants' construction omits mention of a matrix, which one of skill in the art would understand as a component that is directing traffic from one device to another in the network. Medvidovic Decl.,

¶ 19. In addition, Defendants improperly propose that the claim term be restricted to "computers on a local area network," but the switching matrix may be configured to direct traffic between different types of devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, Internet of Things ("IoT") devices, or any network-capable computing device). *Id.* To avoid any confusion, Centripetal's proposed construction uses the term "device" rather than the term "computers" to align the definition more closely to the claims and specification. *Id.*

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
provision/provisioning each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located (Claims 1, 3-5, 7, 9-11, 13, 15-17, 19)	change a device from one state to another based on one or more rules derived from the boundary of a different network	no construction needed/plain meaning

Construction of this term is necessary to clarify this term and interpret its meaning according to what the patentee intended. *Arlington Indus., Inc. v. Bridgeport Fittings, Inc.*, 759 F.3d 1333, 1338 (Fed. Cir. 2014) (holding that claim construction is a matter of clarifying and when necessary explaining what the patentee covered by the claims). In the context of the claims and consistent with its plain and ordinary meaning, "provisioning" a device is a change in a device from one state to another. *See* Medvidovic Decl., ¶ 20. The '077 Patent's systems are focused on devices in a network that are changed when rules are generated based on rules from a

different network. The claims of the '077 Patent set forth that the state of the devices located in one network are changed (i.e. "provision[ed]") with rules generated based on the boundary of the network with another network. *See, e.g.*, '077 Patent, Col. 20:53-58; 21:53-58, 22:56-61, 24:8-13. Therefore, the Court should adopt Centripetal's proposed construction that is supported by the claims which provides clarity to the terms and will aid the jury.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
subscription service (Claims 3, 9)	service that provides aggregated information related to malicious network traffic	service that aggregates information associated with malicious network traffic

The term "subscription service" as used in the claims provides aggregated information related to malicious network traffic and does not necessarily need to be an aggregation service or performing the aggregation itself. Centripetal's construction is consistent with the commonly understood meaning of "subscription" as a service that provides information. The claims only require that the subscription service provide the aggregated information related to malicious network traffic which is received by the claimed computing system. *See, e.g.*, '077 Patent, Col. 21:19-20, 23:24-26 ("identify malicious network traffic based on information ***received from*** a subscription service") (emphasis added); 21:25-26, 23:30-32 ("the information ***received from*** the subscription service") (emphasis added); 22:20-22 ("based on information ***received from*** a subscription service") (emphasis added); Medvidovic Decl., ¶ 21. Thus, the Court should adopt Centripetal's construction which is supported by the claims, specification, and commonly understood meaning.

C. '370 PATENT[5]

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
network device (Claims 22-27, 33, 40, 43-48, 54, 61, 187, 188, 191, 194-195, 198, 201, 202, 205)	a computing device in a network that is capable of transmitting and receiving packets	device that interfaces hosts with a network

Centripetal's proposed construction of this term aligns with the teachings of the patent. *See, e.g., Innovad*, 260 F.3d at 1332-33. The claims of the '370 Patent concern the correlation of packets across a network. In the context of the claims, the claimed network device is capable of transmitting and receiving packets of data. *Phillips*, 415 F.3d at 1314 ("the context in which a term is used within a claim can be highly instructive"); *see also, e.g.*, '370 Patent, Claims 22-26, 33, 43-47, 54, 187-188, 191, 194-195, 198, 201-202, 205 ("plurality of packets received by the network device" and then a "plurality of packets transmitted by the network device"). The patent specification also describes a network device as a device that receives and transmits packets: "packets received by a network device" and "packets transmitted by the network device." '370 Patent, Col. 13:36-14:9. Thus, Centripetal's construction is supported by the claims and the specification.

Defendants' proposed construction of the term is redundant of the claims themselves and recites a single mode of operation of a network device, i.e. one that interfaces hosts with a network. *See* '370 Patent, Fig. 1; Col. 2:44-52 ("Network device(s) 120 ***may include***...interface hosts 114, 116, and 118 with network 106.") (emphasis added). However, the '370 patent specification also describes examples where the claimed network device interfaces with a tap

[5] The asserted claims of the '370 Patent are: Claims 22-27, 33, 40, 43-48, 54, 61, 160, 162, 164, 166, 169, 171, 173, 175, 178, 180, 182, 184, 187, 188, 191, 194, 195, 198, 201, 202, and 205.

device, and it is not limited to interfacing hosts with a network. *See, e.g., id.*, Col. 2:63-65; 3:42-47. In fact, in Figure 1 of the '370 Patent, a network device may sit between hosts and a network, or between two different networks (e.g. Networks A and C; Networks B and C), or sit between two tap devices (124 and 126). *See id.*, Fig. 1 (Network Devices 120 and 122); Claims 22, 23, 43, 44 (a "device in a communication link interfacing a network device and a first [second] network"); Claim 194, 201 ("a packet-filtering device in a communication path that interfaces the network device and the first network"); Medvidovic Decl., ¶ 23. A network device can have many different functionalities, such as being configured to perform network address translation, comprise a proxy, or comprise a gateway. *See, e.g.*, '370 Patent, Col. 5:4-51; Medvidovic Decl., ¶ 22. Thus, Defendants' proposed construction does not account for all of the embodiments in the extrinsic record including the different modes of operation of the network device that are illustrated in the specification and in the claims themselves. The Court should adopt Centripetal's construction which is supported by the claims and the teachings of the patent.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
host (Claims 22-27, 33, 40, 43-48, 54, 61, 160, 162, 164, 166, 169, 171, 173, 175, 178, 180, 182, 184, 187, 188, 191, 194, 195, 198, 201, 202, 205)	a computer device within a network that provides services other than simply acting as a store and forward processor or communications switch	computing or network devices (e.g. servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, switches, access points, or the like), or a communication interface thereof

Centripetal's proposed construction of this term is consistent with how this term is used in the claims, specification as a whole, and commonly understood to those skilled in the art. In contrast, Defendants' proposed construction incorrectly infers that a host must be a passive switch in the context of the claims. While the specification states that the host may be a

computing or network device, the host is not just a simple store and forward processor or communications switch in the context of the claims and as understood by persons of skill in the art. Medvidovic Decl., ¶¶ 24-25. For example, the patent teaches identification of a host for a variety of reasons including for performance reasons or to identify malicious threats. *Id.* All the embodiments of a "host" discussed in the specification describe hosts that do more than store and forward packets *See, e.g.*, '370 Patent, Col. 3:37-39, 4:36-38, 4:52-63, 5:23-30, 5:33-39, 6:41-43, 6:50-53, 7:13-23, 9:20-22, 9:31-35, 9:55-63, 10:26-35, 12:41-13:25, 13:36-47.

Dr. Medvidovic, as a person of skill in the art, opines that, identifying a store and forward device provides less value because generally an administrator would want to know who originated the data or manipulated the data rather than a device that is merely relaying the data. Medvidovic Decl., ¶¶ 24-25. Centripetal's construction of this claim term is consistent with the commonly understood meaning of the term in the field. *See, id.*; Ex. 6 at 256 (Oxford Dictionary of Computer Science, Seventh Edition, 2016) (computer dictionary stating that a host computer (host) is "a computer that is attached to a network and provides services other than simply acting as a store and forward processor or communication switch."). Therefore, the Court should adopt Centripetal's proposed construction that is supported by the intrinsic evidence.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
rule/rules (Claims 22-27, 33, 40, 43-48, 54, 61, 187, 188, 191, 194, 195, 198, 201, 202, 205)	condition or set of conditions that when satisfied cause a specific action to occur	(i) packet-identifying criteria and (ii) a function to be performed on the identified packets

Centripetal's proposed construction of this term is consistent with common sense and how this term is used in the claims, specification as a whole, and with the understanding of those skilled in the art. Defendants' proposed construction, on the other hand, improperly attempts to

inappropriately restrict a "rule" or "rules" to only that which involves "packet-identifying criteria" and "a function to be performed on the identified packets."

As used in the specification, the claimed "rules" have an "if, then" purpose by causing specific actions to occur, e.g. configuring devices to generate log data. They may specify network addresses and may "be configured to cause tap devices 124 and 126 to generate log data for packets destined for the network address associated with host 108 but not for packets destined for the network address associated with host 110..." *See, e.g.*, '370 Patent, Col. 9:48-52; Claim 22. Thus, the claimed "rules" can be more than just "(i) packet-identifying criteria and (ii) a function to be performed on the identified packets" because they can do a variety of functions with log data.

Centripetal's construction of rule(s) is how one of skill in the art understands the term in the field. *See* Medvidovic Decl., ¶¶ 26-27. As the Dictionary of Computer and Internet Terms states, a "rule" is a "condition-action pair that prescribes the action taken when the condition is met." Ex. 5 at 438. In the context of the claims and the patent specification, the commonly understood meaning makes sense as it encompasses the various different examples of rules that are set forth in the patent specification. *See Hyperphrase Techs.*, 260 Fed. Appx. at 280 ("A claim construction that excludes an embodiment of the relevant claim(s) is typically incorrect"). Therefore, the Court should adopt Centripetal's proposed construction that is supported by common sense and the meaning of this term to one of skill in the art reading the patent.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
log entries (Claims 22-27, 33, 40, 43-48, 54, 61, 160, 162, 164, 166, 169, 171, 173, 175, 178, 180, 182, 184, 187,	plain and ordinary meaning	notations of unique identifying information for each packet

188, 191, 194, 195, 198, 201, 202, 205)		

The claim term "log entries" has a plain and ordinary meaning to a person of skill in the art and requires no particular construction. A person of skill in the art understands that "log entries" are simply entries in a log. Medvidovic Decl., ¶ 28. Defendants' proposed construction improperly adds unnecessary requirements to the term by requiring the entries be "unique" identifying information for "each packet." The '370 Patent specification, however, does not restrict the entries to "unique" information for "each packet," and the term "unique" is not found in the patent. For example, the specification only describes log entries that "correspond" to packets, without any requirement of "unique" information for "each packet." *See, e.g.*, '370 Patent, Col. 1:30-37 ("log entries corresponding to the packets received by the network device" and "log entries corresponding to the packets transmitted by the network device"); 3:18-19 ("one or more log entries corresponding to the identified packets in log(s)"); *see also id.*,13:43-44, 13:52-53; *Dayco Prods., Inc. v. Total Containment, Inc.*, 258 F.3d 1317, 1327 (Fed. Cir. 2001) ("Our cases make clear, however, that adding limitations to claims not required by the claim terms themselves, or unambiguously required by the specification or prosecution history, is impermissible"). Thus, the term "log entries" need not be defined differently from its plain and ordinary meaning.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
correlate/correlating (Claims 22-27, 33, 40, 43-48, 54, 61, 160, 162, 164, 166, 169, 171, 173, 175, 178, 180, 182, 184, 187, 188, 191, 194, 195, 198, 201, 202, 205)	programming instructions that cause a packet correlator to determine whether a portion of data in one log entry corresponds to a portion of data in another log entry	determining by hardware or software (e.g. a packet correlator) whether log entries in different files correspond to the same packet

Centripetal's proposed construction of the term is consistent with how it is used in the claims and specification. The specification makes clear that a "packet correlator" is the device that does the correlating and applies programming instructions that cause it to determine whether a portion of data in one log entry corresponds to a portion of data in another log entry. *See, e.g.*, '370 Patent, Col. 8:23-67, 9:1-19, 9:45-54, 11:33-12:27, 13:56-59.

Defendants' proposed construction injects unnecessary verbiage into the term which is not helpful for a jury. *Id.* Defendants' also improperly attempt to add an extra step of correlating log entries to the same single packet, which is not required by the '370 Patent. *See, e.g., Smith & Nephew, Inc. v. Hologic, Inc.*, No. 2017-1008, 2018 WL 618589, at *2 (Fed. Cir. Jan. 30, 2018) (holding improper to import limitations into the construction that are not found anywhere in the intrinsic record); Medvidovic Decl., ¶ 29. The claims only require that there is correlation between log entries, and does not require the extra step of attempting to correlate the log entries to the same packet. *See, e.g.*, '370 Patent, Col. 19:45-54; 20:26-34, 21:41-46, 24:9-19, 24:59-67, 26:13-21, 50:14-27, 50:44-48, 50:57-65, 51:59-52:5, 52:24-28, 52:42-49, 53:44-57, 54:7-11, 54:27-34, 55:27-36, 55:54-61, 56:11-20, 56:50-59, 57:12-20, 57:40-48, 58:13-23, 58:42-48, 59:4-12. Accordingly, the Court should adopt Centripetal's construction which is well-supported by the scope of the claims.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
device in a communication link (Claims 22-27, 33, 40, 43-48, 54, 61)	device in a computer network	device in a communication path

Centripetal's proposed construction of this term aligns with the teachings of the patent. *See, e.g., Innovad*, 260 F.3d at 1332-33; *Phillips*, 415 F.3d at 1316 ("Ultimately, the

interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim") (citing *Reinshaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998)). The claims of the '370 Patent concern the correlation of packets across a network including specific steps involving devices. A "device in a communication link," as used in the claims, is a device in a computer network. *See, e.g.*, '370 Patent, Claims 22, 43 ("provision the device in the communication link interfacing the network device and the first network..."... "configure the device in the communication link interfacing the network device with the first network..."), Claims 23, 44 (the latter). The focus of the claims is a method or system that operates with a computer network, and Centripetal's proposed construction is in line with the teachings of the patent. Medvidovic Decl., ¶ 31.

Defendants' proposed construction of the term does not even mention a computer network. Defendants' only purported support for its construction is extrinsic evidence in the form of general dictionary definitions that are not in the field of computer science. *Phillips*, 415 F.3d at 1322 ("a general-usage dictionary cannot overcome art-specific evidence of the meaning of a claim term") (internal quotations and citations omitted); Medvidovic Decl., ¶ 31. The present-day Merriam Webster dictionary definition and the Newton's Telecom Dictionary from 1999 (approximately 16 years before the priority date of the patent), are not relevant to the '370 Patent. Ex. 7 (Defendants' Preliminary Claim Construction) at 4. Moreover, neither dictionary definition mentions "path" in its definition of "link." *Id.*

Based on the fact that the patent is about computer network technology, and understanding the context of the claims, the Court should adopt Centripetal's definition of "a device in a communication link" which is simply a device in a computer network.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
provision a device in a communication link interfacing a network device and a first/second network (Claims 22-27, 33, 40, 43-48, 54, 61)	changing a device from one state to another where the device is communicatively coupled to a network device and a first/second network	no construction needed/plain meaning

Construction of this term is necessary and will help the jury understand what provisioning means in the context of the claims. *Arlington Indus.*, 759 F.3d at 1338 (holding that claim construction is a matter of clarifying and when necessary explaining what the patentee covered by the claims). In the context of the claims, "provisioning" a device is a change in a device from one state to another. This is also the plain and ordinary meaning of the term to one of skill in the art. *See* Medvidovic Decl., ¶ 32. The patent teaches provisioning devices to be in a state that they can communicate with a network device and network, for example, based on rules that identify packets and that specify network addresses. *See, e.g.*, '370 Patent, Col. 19:8, 19:13, 19:21, 23:40, 23:45, 23:53. One of skill in the art would understand this term to mean allowing the device to function based on rules set forth in the claims and "interfac[e]" (or communicate) with a network device and a first or second network. Medvidovic Decl., ¶ 32. Thus, the Court should adopt Centripetal's construction which provides further clarity to this term consistent with what the patentee intended to convey.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
identify the plurality of packets received/transmitted by the network device (Claims 22-27, 33, 40, 43-48, 54, 61)	determine the network-layer or transport-layer data contained within the plurality of packets received/transmitted by the network device	no construction needed/plain meaning

Centripetal's construction is consistent with how the patentee described how packets are identified in the intrinsic record. Medvidovic Decl., ¶ 33. In the '370 patent specification, packets are identified according to rules that specify destination network addresses based on network-layer information or transport-layer data. *See, e.g.*, '370 Patent, Col. 3:48-54 ("identify the packets (e.g. P1, P2, and P3) by determining that the packets are destined for the network address associated with host108 (e.g. based on network-layer information contained in their headers)..."); Col. 5: 8-18 ("the packets received from host 114 (e.g. P1, P2, and P3) may comprise network- or transport-layer header information identifying their source as a network address associated with host 114 (e.g. a network address associated with network 104 (or a private network address)), and the corresponding packets...may comprise network- or transport-layer header information identifying their source as a network address associated with network device(s) 122 (e.g., a network address associated with network 106 (or a public network address))"); Col. 5: 58-64 ("identify the corresponding packets generated by network device(s) 122 (e.g. P1', P2', and P3') by determining that the packets meet the criteria included in rule(s) 140. The criteria may include any combination of the network-layer information, transport-layer information, application-layer information or environmental variable(s)..."); *see also id.,* Col. 3:31-32; Col. 5:65-6:5; 6:43-50; 7:35-58; 10:49-11:4; 12:63-66. The analysis is based on the network-layer or transport-layer data contained within the packets. *Id.* Because Centripetal 's proposed construction is aligned with the specification, it is the proper construction.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
configured to cause the system/computing system to log packets (Claims 22-27, 33, 40, 43-48, 54, 61)	programming instructions that cause the system to generate a log file containing packet data	no construction needed/plain meaning

Centripetal's construction is appropriate as it gives meaning to this term consistent with what the patentee intended to be covered, and its plain and ordinary meaning. The claims themselves support Centripetal's construction. They describe a system that "generates a plurality of log entries corresponding to the plurality of packets received/transmitted by the network device" based on the configured rules, and then correlates the packets based on the log entries. *See, e.g.*, '370 Patent, Col. 19:28-30, 19:38-40, 19:45-51, 23:60-61, 24:3-5, 24:10-16. Centripetal's construction provides clarity that this process involves the generation of log file(s) containing packet data.

The specification also supports Centripetal's construction and specifically describes how the rules result in the generation of log file(s) containing packet data. *See, e.g.*, '370 Patent, Col. 3:13-20 ("rule(s) 140, which may configure tap device(s) 124 and 126 to identify packets meeting criteria specified by rule(s) 140 and to communicate data associated with the identified packets...utilize the data to generate one or more log entries corresponding to the identified packets in log(s) 142"); Col. 3:54-56 ("At step 6, tap device 126 may generate log data associated with the packets received by network device(s) 122..."); Col. 6:5-7 ("At step 9, tap device 124 may generate log data associated with the corresponding packets generated by network device(s)..."); 13:42-43 ("...the computing system may generate log entries corresponding to the packets received by the network device"); *see also* Col. 6:50-51; 7:59-60, 9:49-50, 9:64-67; 11:4-7; 13:7-9; 13:48-50. As set forth in these examples from the specification, the system logs packets by implementing programming instructions that cause the computing system to generate a log file containing packet data. Medvidovic Decl., ¶¶ 34-35. For these reasons, the Court should adopt Centripetal's construction which is consistent with the patentee's intended meaning of the term in the context of the claims and specification.

D. '722 PATENT[6]

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
network-threat indicators (Claims 1-5, 24-25)	characteristic of network traffic signaling a network threat (e.g. unauthorized requests or data transfers, viruses, malware, or large volumes of network traffic designed to overwhelm network resources)	indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like

Centripetal's proposed construction of this term is consistent with how it is used in the claims and specification. A "network-threat indicator" is characteristic of network traffic signaling a network threat which, according to the specification, "may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of network traffic designed to overwhelm network resources, and the like)." '722 Patent, Col. 1:16-19. Centripetal's construction uses the definition of a "network threat" that comes from the specification. Defendants' construction unnecessarily specifies examples of network-threat indicators, when the term simply means a characteristic of network traffic signaling different types of network threats. Medvidovic Decl., ¶ 36; *see also Thorner*, 669 F.3d at 1356-66 (holding the district court must not read in limitations from the specification without clear intent to do so). Thus, the Court should adopt Centripetal's construction which is consistent with the well understood meaning of network-threat indicators as used in the patent.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
packet-filtering device (Claims 1-5, 24-25)	a device programmed to filter packets based on data associated with a packet	no construction needed/plain meaning

[6] The asserted claims of the '722 Patent are: Claims 1-5, 24, and 25.

A packet-filtering device as used in the claims and specification is a device that is programmed to filter packets based on data associated with a packet. The specification describes examples of a "packet-filtering device" located at boundary between networks that filters packets by, for example, receiving rules, applying rules, generating and logging data, updating rules, assigning scores to threats, reconfiguring the operator. *See, e.g.*, '722 Patent, Col. 1:52-2:10; 3:44-4:4, 4:59-5:6, 5:19-24, 5:37-42, 5:49-67, 6:6-11, 6:25-26, 7:22-24, 9:14-22, 9:39-52, 10:23-28, 10:35-41, 11:3-14, 15:33-42, 15:53-16:34. The "packet-filtering device" can use the data associated with a packet for the filtering, including a source address, a destination address, a port number, a protocol number, a protocol type, a domain name, URL, URI, or the like. *Id.*; Medvidovic Decl., ¶ 37; *see, e.g.*, '722 Patent, Col. 6:32-37, 7:14-21, 8:8-14, 17:18-20. Accordingly, the Court should adopt Centripetal's construction which is consistent with the intrinsic record. *See, e.g., Innovad*, 260 F.3d at 1332-33.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
packet-filtering rules (Claims 1-5, 24-25)	condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet	(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets

Centripetal's proposed construction is consistent with how this term is used in the context of the patent claims and specification, and with the understanding of persons of skill in the art. Packet-filtering rules are simply a condition or set of conditions that when satisfied cause a computing device to filter packets based on data associated with a packet. As used in the claims and the specification, the "packet-filtering rules" are "configured to cause the packet-filtering device to identify packets corresponding to network-threat indicators." '722 Patent, Col. 1:47-49.

Defendant's improper construction omits any mention of the term "packet-filtering" from their proposed construction. In addition, the term as used in the claims and specification include more than "(i) packet-identifying criteria and (ii) an operator to be performed on the identified packets," as Defendants propose. Rather, the specification also states that the "network-intelligence rules (e.g. packet-filtering rules...") "may comprise: one or more criteria that correspond to one or more of network-threat indicators...to cause packet-filtering device to identify packets...;an operator...;and information distinct from the criteria (e.g. a Threat ID) that identifies one or more of the network-threat indicators upon which the rules is based, one or more network threats associated with the network-threat indicators, one or more network-threat-intelligence reports...one or more network-threat-intelligence providers...or other information contained in the network-threat-intelligence reports...." '722 Patent, Col. 5:11-36 (emphasis added); *see also, e.g.*, Col. 5:40-44, 5:58-59, 7:1-11, 13:21-28, 13:41-42. Defendants failure to account for the additional examples in the '722 Patent is fatal to its construction. *See Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008) ("We normally do not interpret claims in a way that excludes embodiments disclosed in the specification" unless those embodiments are clearly disclaimed in the specification).

Centripetal's proposed construction, on the other hand, is consistent with how it is used in the claims and specification, and with the commonly understood meaning of "rule(s)" to one of skill in the art. Medvidovic Decl., ¶¶ 38-39. A person of skill in the art understands that rules are a condition or set of conditions that when satisfied cause a specific action to occur. *Id.* A "packet-filtering rule," therefore, is a rule that causes a computing device to filter packets based on data associated with a packet. This is consistent with how it is used in the claims and the specification in connection with a "packet-filtering device" that is a device programmed to filter

packets based on data associated with a packet. *See supra* at 23. Thus, the Court should adopt Centripetal's construction.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
interface (Claims 1-5, 24-25)	plain and ordinary meaning	a display visible to the user that allows a user to provide input

The term "interface" is well understood to one of skill in the art and requires no particular construction. Medvidovic Decl., ¶ 40. An interface is understood as an object that allows two things to communicate with each other. The term "interface" is used throughout the patent in different contexts to describe the communication between two different things, which are not always a display and a user. For example, the patent describes networks that interface networks ('722 Patent, Col. 3:3-4), communication interfaces (*id.*, Col. 4:8), and interface of a packet-filtering device (*id.*, Col. 6:39-40). None of these examples in the specification are restricted to Defendants' construction of "a display visible to the user that allows a user to provide input." *See Hyperphrase Techs.*, 260 Fed. App. at 280 ("A claim construction that excludes an embodiment of the relevant claim(s) is typically incorrect") (citation omitted). Consistent with the meaning of the term as used in the patent, the Oxford Dictionary of Computer Science (2016) also states that an "interface" is a "specification of the communication between two program units." Ex. 6 at 278; Medvidovic Decl., ¶ 40. Furthermore, the claims provide the necessary context for "interface," and adding in additional limitations into the definition of "interface" makes the claim redundant. *See, e.g.*, '722 Patent, Col.17:40-47; *Apple, Inc.*, 842 F.3d at 1237-38 (construing a claim term to include features of that term already recited in the claims would make those expressly cited feature redundant). For this reason, the plain and ordinary meaning of interface is appropriate in the context of the '722 Patent.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
operator (Claims 1-5, 24-25)	an adjustable instruction that causes the packet filtering device to either prevent or allow a packet to continue to a destination	function to either block a packet corresponding to criteria or allow it to continue to its destination

Centripetal's construction is consistent with the understanding of the term to one of skill in the art in light of the claims and specification. Defendants' construction wrongly omits that the operator can be adjustable instruction. The claims and patent specification describe that an operator can change its instruction from preventing a packet to allowing a packet, and also the reverse. For example, the specification states that there may be a "change in the operator of the packet-filtering rule associated with the threat" ('722 Patent, Col. 11:1-10); "The operator may be configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination" (*id.*, Col. 1:55-57), and the operator may be "reconfigure[d]" based on the generation of "data comprising an update for the interface associated with packet-filtering device" (*id.*, Col. 11:60-12:3); *see also id.*, Col. 9:33-39; 12:15-28; 13:62-14:21; 14:53-67. That the operator be "adjustable" is how one of skill in the art understands the meaning of this term. Medvidovic Decl., ¶¶ 41-42.

Defendants' construction also includes the term "block" which may confuse a jury because it could infer the act of stopping packets rather than simply preventing a packet from continuing to its destination or rerouting them to a different destination, as the patent describes. The operator, in the context of the patent claims and specification, may prevent the packets from continuing to a destination and reroute them to a different destination, without necessarily "blocking" them. *See, e.g.*, '722 Patent, Col. 9:57-10:14; Medvidovic Decl., ¶¶ 41-42. For these reasons, the Court should adopt Centripetal's construction which is consistent with the patent

claims and specification.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators (Claims 1-5, 24-25)	if the packet-filtering device determines the first packet meets one or more conditions associated with one or more network threat indicators from a packet filtering rule	no construction needed/plain meaning

Centripetal's construction provides clarity to the meaning of this claim term which will be helpful for a jury. This claim term is focused on what occurs before other actions are taken. *See, e.g.*, '722 Patent, Col. 17:15-18:2. For this term, the packet-filtering device first makes a determination based on conditions associated with network threat indicators from a packet-filtering rule and then prevents the "second packet" from continuing to its destination. *Id.*, Col. 17:50-18:2. Centripetal's proposed construction clarifies the term so it is understandable for a jury and is consistent with the understanding of one of skill in the art. *See, e.g., id.*, Col. 1:46-2:10, 6:55-7:12; 9:3-10:52; 12:33-13:47; 15:63-16:34; Medvidovic Decl., ¶ 43. For such reason, the Court should adopt Centripetal's proposed construction.

Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the	causing a packet-filtering device to generate and communicate a record that identifies (1) a network threat indicator based on a rule and (2) data that indicates that the first packet	no construction needed/plain meaning

first packet was allowed to continue toward the destination of the first packet (Claims 1-5, 24-25)	was allowed to continue toward the destination	

Centripetal's construction clarifies that, consistent with the specification, the "communicating" element means the causing of a packet-filtering device to generate and communicate a record of data regarding the first packet. This construction is consistent with the specification which describes the packet-filtering device generating a record, for example, as log data or a display identifying: (1) a network threat indicator based on the packet-filtering rule and (2) data that indicates that the first packet was allowed to continue toward the destination. *See, e.g.*, '722 Patent, Col. 6:13-54; 6:59-7:11; 7:48-8:7; 8:27-39, 11:16-37; 11:45-59; 12:34-57; 13:3-14; 16:8-33. Centripetal's construction is also consistent with the plain and ordinary meaning of the term to one of skill in the art, and includes the generation of a record of data as this term is used in the patent. Medvidovic Decl., ¶ 44. Therefore, the Court should adopt Centripetal's construction.

Claim Term	**Plaintiff's Proposed Construction**	**Defendants' Proposed Construction**
modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations (Claims 1-5, 24-25)	modifying the state of the packet-filtering device to cause an adjustable instruction to prevent a packet from continuing toward its destination	no construction needed/plain meaning

Centripetal's construction of this term is supported by its use in the claims and the specification. In the claims, the packet-filtering device modifies at least one operator, which

results in modification of the state of the packet-filtering device to prevent packets from continuing towards their destination. *See, e.g.,* '722 Patent, Col.1:55-57 ("The operator may be configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination…"); Col. 2:7-10 ("the user device to instruct the packet-filtering device to reconfigure the operator to prevent future packets corresponding to the criteria from continuing toward their respective destinations"); Col. 9:46-49 ("…to instruct packet-filtering device 144 to reconfigure an operator associated with Rule...to cause packet-filtering device 144 to prevent packets…"); Col. 17:50-55; Abstract ("The operator may be configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination"); Col. 14:13-21 ("packet-filtering device 144 to reconfigure the operator…(e.g. to reconfigure the packet-filtering device 144 to prevent packets…"); Col. 1:55-57, 5:19-22, 10:47-52, 13:33-47; Medvidovic Decl., ¶ 45. To persons of skill in the art, the packet-filtering device can have different modes or states, such as log-data processing states (start log processing, continue ongoing log processing, generate data for the interface based on the log, communicating the data to the host). *See, e.g.*, '722 Patent, Col. 9:14-26; Medvidovic Decl., ¶ 45. The term "operator" means an "adjustable instruction" as discussed above consistent with the meaning of the term in the claims and specification and its plain and ordinary meaning. Centripetal's proposed construction provides clarity to this term which will be helpful to a jury. Therefore, the Court should adopt Centripetal's proposed construction.

III. CONCLUSION

For the foregoing reasons, Centripetal respectfully requests the Court adopt Centripetal's proposed constructions for the above claim terms.

Dated: April 20, 2018

By: */s/ Stephen E. Noona*
Stephen Edward Noona

Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre
Lisa Kobialka
James Hannah
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

Christina L. Martinez (pro hac vice)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-9000
Facsimile: (212) 715-8000
cmartinez@kramerlevin.com

ATTORNEYS FOR PLAINTIFF CENTRIPETAL NETWORKS, INC.

CERTIFICATE OF SERVICE

I hereby certify that on April 20, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to:

William R. Poynter
Virginia State Bar No. 48672
KALEO LEGAL
4456 Corporation Lane, Suite 135
Virginia Beach, VA 23462
Telephone: (757) 238-6383
Facsimile: (757) 304-6175
wpoynter@kaleolegal.com

Christine M. Morgan (*pro hac vice*)
James A. Daire (*pro hac vice*)
John P. Bovich (*pro hac vice*)
Jonah D. Mitchell (*pro hac vice*)
Doyle B. Johnson (*pro hac vice*)
Christopher J. Pulido (*pro hac vice*)
REED SMITH LLP
101 Second Street, Suite 1800
San Francisco, CA 94105
Telephone: (415) 543-8700
Facsimile: (415) 891-8269
cmorgan@reedsmith.com
jdaire@reedsmith.com
jbovich@reedsmith.com
jmitchell@reedsmith.com
dbjohnson@reedsmith.com
cpulido@reedsmith.com

Attorneys for Defendants
Keysight Technologies, Inc. and Ixia

/s/ Stephen E. Noona
Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com