Floyd G. Short (*pro hac vice*)
Matthew R. Berry (*pro hac vice*)
Steven M. Seigel (*pro hac vice*)
P. Ryan Burningham (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, Washington 98101-3000
Telephone: (206) 516-3800
Facsimile: (206) 516-3883
fshort@susmangodfrey.com
mberry@susmangodfrey.com
sseigel@susmangodfrey.com
rburningham@susmangodfrey.com

Kalpana Srinivasan (237460)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Facsimile: (310) 789-3150
ksrinivasan@susmangodfrey.com

Attorneys for Plaintiff NetFuel, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETFUEL, INC.,

Plaintiff,

vs.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 3:18-cv-2352 EJD (NMC)

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

Plaintiff NetFuel, Inc. ("NetFuel") files this Complaint for patent infringement against Defendant Cisco Systems, Inc. ("Cisco" or "Defendant"), and alleges as follows:

NATURE OF THE ACTION

1. This is an action under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.*, for infringement by Cisco of certain claims of U.S. Patent Nos. 7,747,730 and 9,663,659 (collectively referred to as the "Patents-in-Suit").

THE PARTIES

2. NetFuel is a corporation duly organized and existing under the laws of Delaware and has its principal place of business in Los Gatos, California. NetFuel was co-founded by James Harlow, inventor of the Patents-in-Suit.

3. NetFuel is the assignee and owner of the Patents-in-Suit. NetFuel was founded in 2000, in part to provide programmable network solutions for financial-services organizations and banks and their high-speed stock and futures trading platforms. NetFuel CEO James Harlow is the inventor of the Patents-in-Suit and has long been an entrepreneur in the field of computer software and networking technology. Starting as a teenager in the late 1970s, when he taught himself computer programming languages including assembly language, Harlow immersed himself in computer programming and network design and became a pioneer in the field of software-defined networking.

4. On information and belief, Cisco is a corporation duly organized and existing under the laws of California, having its principal place of business at 170 West Tasman Drive San Jose, California 95134, and with a registered agent at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833-3505.

5. Cisco is a company that, among other things, develops and sells computer networking, security, collaboration, and cloud-based technology products, and provides technology-related services, including technical support, consulting, network optimization, migration, and analytics. Among other things, Cisco

develops and sells or licenses hardware and software for computer networks, including routing, switching, storage, wireless, collaboration, and network security products.

JURISDICTION AND VENUE

6. 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*.

7. This Court has personal jurisdiction over Cisco because, *inter alia*, upon information and belief: (i) Cisco has its principal place of business in San Jose, California; (ii) Cisco has done and continues to do business in California; and (iii) Cisco has committed and continues to commit acts of patent infringement in California, including by at least making, using, offering to sell, and/or selling accused products and services in California, and/or inducing others to commit acts of patent infringement in this District. For example, Cisco refers to its office at 170 West Tasman Drive in San Jose, California, as its Americas Headquarters in user manuals for Cisco's accused products.

8. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b) because, *inter alia*, upon information and belief: (i) Cisco has its principal place of business in San Jose, California; (ii) Cisco has done and continues to do business in this District; and (iii) Cisco has committed and continues to commit acts of patent infringement in this District, including by making, using, offering to sell, and/or selling accused products and services in this District, and/or inducing others to commit acts of patent infringement in this District.

PATENTS-IN-SUIT

9. Plaintiff is the assignee and owner of United States Patent No. 7,747,730 (the "'730 patent"), entitled "Managing Computer Network Resources," a true and correct copy of which is attached hereto as **Exhibit A**. The '730 patent

bears a filing date no later than June 28, 2002, and was duly and legally issued by the United States Patent and Trademark Office ("PTO") no later than June 29, 2010. Mr. Harlow is the inventor of the '730 patent.

10. Plaintiff is the assignee of United States Patent No. 9,663,659 (the "'659 patent"), entitled "Managing Computer Network Resources," a true and correct copy of which is attached hereto as **Exhibit B**. The '659 patent is designated a continuation of the application resulting in the '730 patent, bears a domestic filing date of no later than October 10, 2012, and was duly and legally issued by the PTO no later than May 30, 2017. Mr. Harlow is the inventor of the '659 patent.

11. NetFuel owns all right, title, and interest in and to the Patents-in-Suit and possesses all rights of recovery.

12. The inventions disclosed in the Patents-in-Suit were revolutionary, and have been cited over 100 times by the largest security and network companies in the world. For example, the Patents-in-Suit have been cited by patents assigned to international companies such as International Business Machines, Juniper Networks, Palo Alto Networks, Hewlett Packard, Boeing, and Symantec.

13. The Patents-in-Suit, generally speaking, disclose systems, machine-readable media, and methods for managing computer networks, comprising the use of agents which, in at least one embodiment, are assigned goals in accordance with network policies (relating to operational characteristics of the network), achieve those goals by executing predefined tasks, and have those assigned goals dynamically modified as necessary during network operations to improve performance.

14. For example, in one embodiment, software agents operate within a runtime environment, which is hosted on a particular network device. The runtime environment allows agents operating within it to communicate with the host device, with other agents, and with an agent control mechanism. Each agent has at least one assigned goal which is expressed in the form of policy and can be dynamically

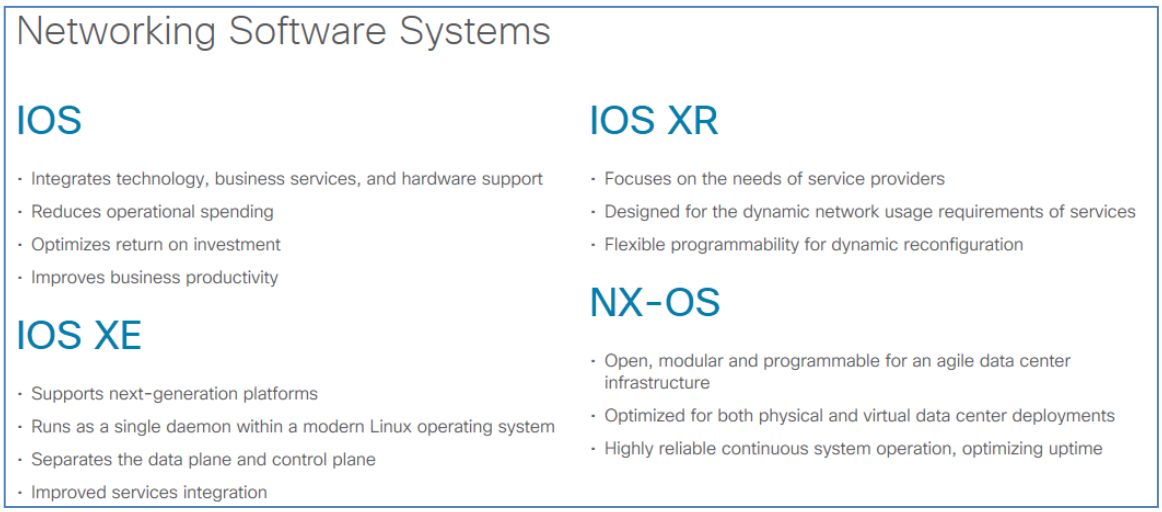
modified based on desired operational characteristics of the network. *See* '730 Patent, Col. 2, lines 10-20.

15. The systems, machine-readable media, and methods disclosed and claimed by the Patents-in-Suit yield substantial benefits for individuals and institutions that desire reliable, secure, fast, and uninterrupted network services by, *inter alia*, reducing the amount of human input and expense required to manually troubleshoot, monitor, administer and/or oversee computer networks. *See* '730 Patent, Col. 1, lines 11-24.

16. Users of the patented systems, machine-readable media, and methods benefit from, *inter alia*, improved network functionality and performance, including reliability, scalability (*i.e.*, the ability of a network to function regardless of the number of connected network nodes), robustness (*i.e.*, the ability of a network to continue operating even if network nodes fail), and quality of service (*e.g.*, measurements of network-service performance metrics such as transmission quality and service availability and/or uptime). *See id.*

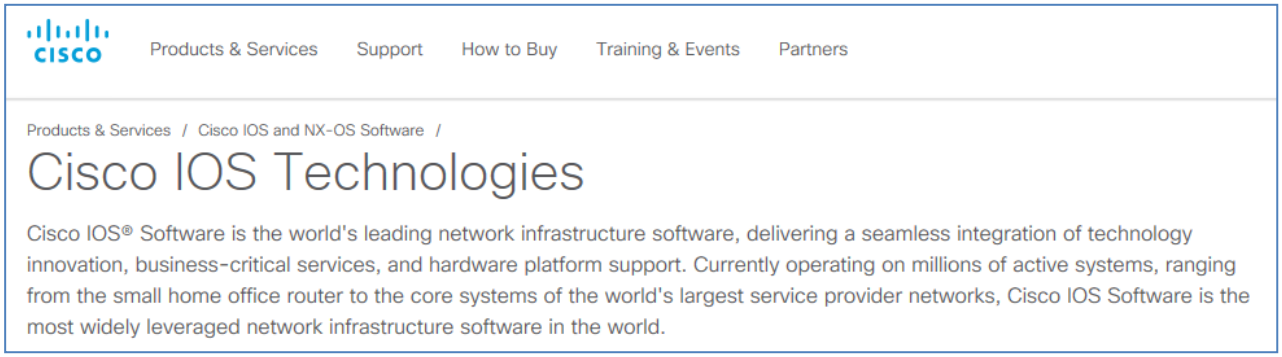
DEFENDANT'S INFRINGING PRODUCTS

17. Cisco is one of the world's largest developers and purveyors of computer-networking technologies, including network appliances such as routers, switches, and storage devices, and related services. Cisco also designs, sells, and/or licenses a range of networking software systems—specifically, IOS, IOS XE, IOS XR, and NX-OS—which are deployed and operate on Cisco's network devices, as illustrated below.



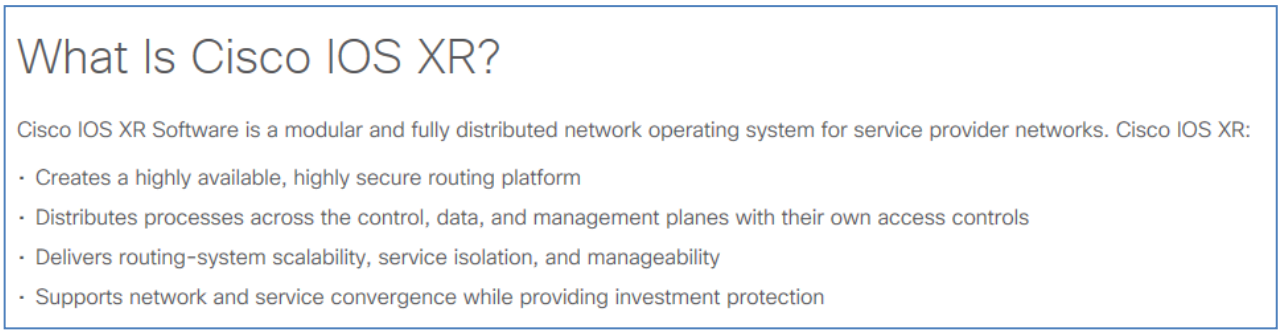
See Cisco Networking Software, *available at*: https://goo.gl/q869UG.

18. Cisco's IOS Software is widely deployed on Cisco routers, switches, and other network devices, and is further described by Cisco as follows:



See Cisco IOS Technologies, *available at*: https://goo.gl/symEdg.

19. Cisco's IOS XR Software is designed for use by service provider networks, and is deployed on Cisco routers, switches, and other network devices, and is further described by Cisco as follows:



See Cisco IOS XR, *available at* https://goo.gl/ZQ72J8.

20. Cisco's IOS XE Software is a modular networking software system that runs on Cisco's next-generation networking appliances, including routers, switches, and other network devices, and is further described by Cisco as follows:

> **Cisco IOS XE: Open, Programmable, Secure**
>
> Cisco IOS® XE has been designed to allow you to deploy services more quickly with lower TCO and minimized complexity. Cisco IOS XE 16, combined with Cisco DNA™ Center and Software-Defined Access, can reduce training and upgrade time, simplify qualification, speed testing and device monitoring, and improve network operations with a consistent OS across access, distribution, core, wireless, and WAN.

See Cisco IOS XE 16 *available at* https://goo.gl/TS8wxX.

21. Cisco's NX-OS software is designed for next-generation devices and appliances, is designed to support data-center operations, and is deployed on Cisco routers, switches, and other network devices; it is further described by Cisco as follows:

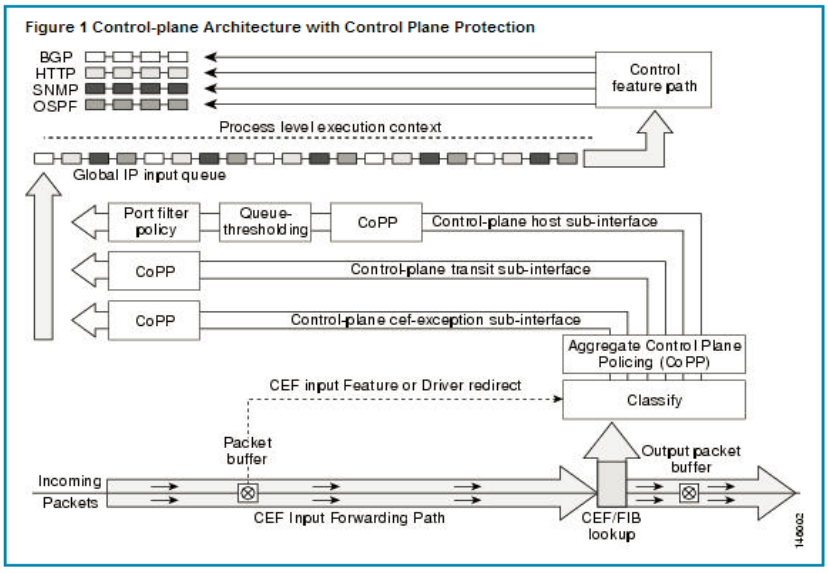
> **Open, extensible operating system for data center**
>
> Open Cisco NX-OS Software is the industry's most extensible, open, and programmable network operating system. It enables network automation and allows customers to programmatically provision and configure switches through comprehensive APIs, utilizing tools provided by Cisco and open-source third party solutions. Powerful capabilities include zero touch provisioning and network telemetry for top notch security.

See Cisco NX-OS, *available at* https://goo.gl/LLUvmW.

22. Cisco has infringed and continues to infringe one or more claims of the Patents-in-Suit by at least making, distributing, selling, offering for sale, and/or importing products, platforms, systems, services, and offerings that practice the inventions described in the Patents-in-Suit, and by inducing its customers and others to infringe the Patents-in-Suit. The accused infringing products include Cisco networking software systems—*i.e.*, IOS, IOS XE, IOS XR, and NX-OS—and Cisco network devices running and/or incorporating said networking software, including but not limited to Catalyst Routers, Integrated Services Routers, Catalyst

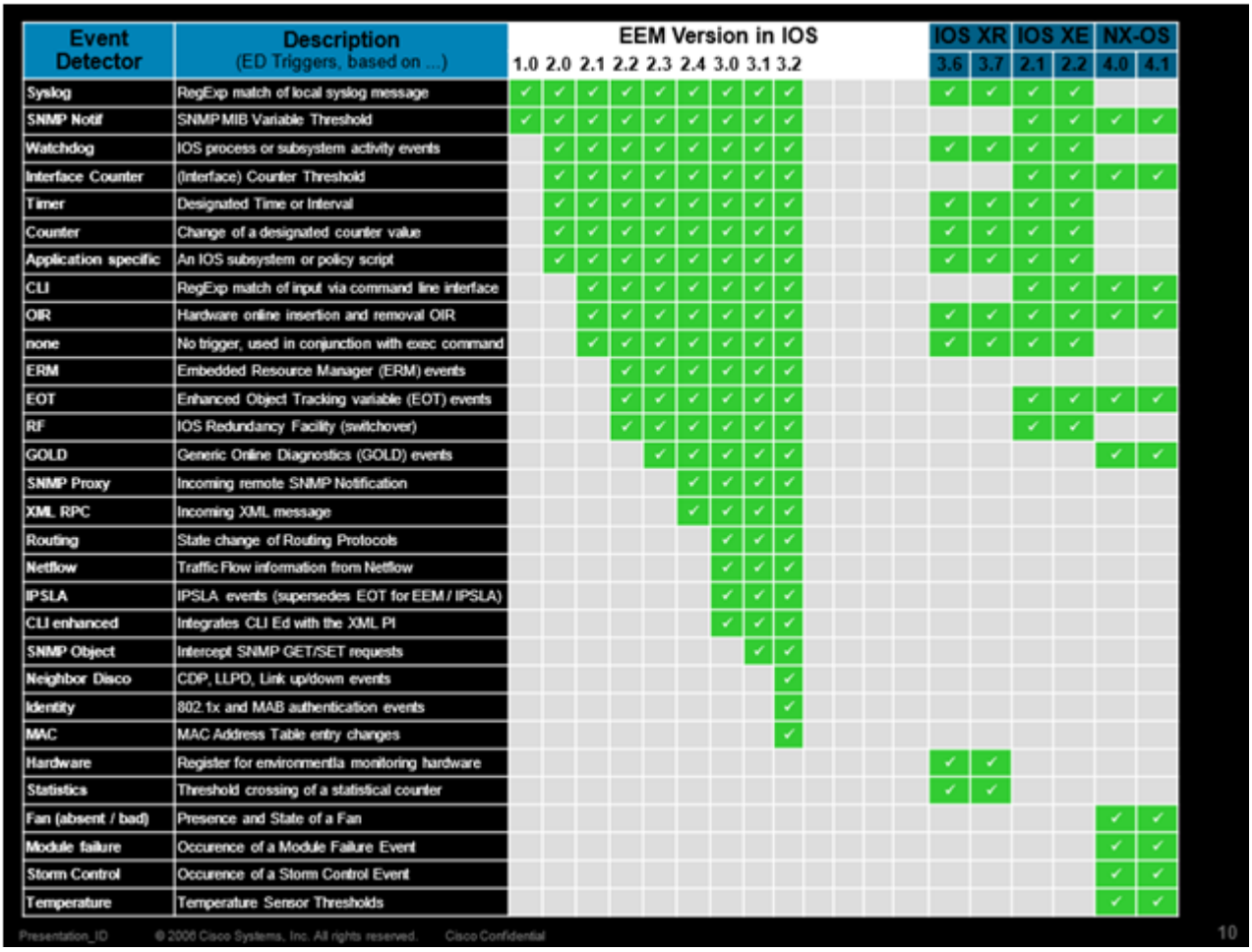
Switches, Connected Grid Switches, Industrial Ethernet Switches, 800 Series Routers, 7600 Series Routers, Aggregation Services Routers, ME Routers and Switches, 10000 Series Routers, Carrier Routing Systems, 6000 Series Routers, and Nexus Switches (the "Accused Products"). A representative list of infringing products is included as **Exhibit C**. This representative list is based on publicly available information, and it will be supplemented with information learned through discovery in this action.

23. The Accused Products employ, *inter alia*, a range of infringing data traffic monitoring and management software features, including Control Plane Policing ("CoPP") and/or Local Packet Transport Services ("LPTS"). CoPP/LPTS improve network stability, reliability, and packet delivery by managing the flow of certain types of network data (*e.g.*, control plane packets) to increase network stability, "reachability," and availability of network devices, and to protect devices' central processing units ("CPUs") against reconnaissance and denial-of-service ("DOS") attacks. The below figure depicts one example of Cisco's CoPP/LPTS architecture.



See Cisco QoS: Policing and Shaping Configuration Guide: IOS 15M&T, *available at* https://goo.gl/GDqsyJ.

24. The Accused Products also employ, among other infringing features and functions, infringing network event detection, monitoring, and response software called Embedded Event Management ("EEM"). EEM allows the Accused Products to, among other things, respond to network events in real time, automate or reduce the need for human involvement in certain tasks, and take actions based on conditions or triggers that the Cisco networking software system detects. The following illustration provides a matrix of at least some of the types of network events that various iterations of EEM are capable of monitoring and detecting, and at least some of the triggers that EEM uses to determine when to take action.



Event Detector	Description (ED Triggers, based on ...)	EEM Version in IOS 1.0	2.0	2.1	2.2	2.3	2.4	3.0	3.1	3.2	IOS XR 3.6	3.7	IOS XE 2.1	2.2	NX-OS 4.0	4.1
Syslog	RegExp match of local syslog message	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
SNMP Notif	SNMP MIB Variable Threshold	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
Watchdog	IOS process or subsystem activity events		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Interface Counter	(Interface) Counter Threshold		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
Timer	Designated Time or Interval		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Counter	Change of a designated counter value		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Application specific	An IOS subsystem or policy script		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
CLI	RegExp match of input via command line interface			✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
OIR	Hardware online insertion and removal OIR			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
none	No trigger, used in conjunction with exec command			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
ERM	Embedded Resource Manager (ERM) events				✓	✓	✓	✓	✓	✓						
EOT	Enhanced Object Tracking variable (EOT) events				✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
RF	IOS Redundancy Facility (switchover)				✓	✓	✓	✓	✓	✓			✓	✓		
GOLD	Generic Online Diagnostics (GOLD) events					✓	✓	✓	✓	✓					✓	✓
SNMP Proxy	Incoming remote SNMP Notification						✓	✓	✓	✓						
XML RPC	Incoming XML message						✓	✓	✓	✓						
Routing	State change of Routing Protocols							✓	✓	✓						
Netflow	Traffic Flow information from Netflow							✓	✓	✓						
IPSLA	IPSLA events (supersedes EOT for EEM / IPSLA)							✓	✓	✓						
CLI enhanced	Integrates CLI Ed with the XML PI							✓	✓	✓						
SNMP Object	Intercept SNMP GET/SET requests								✓	✓						
Neighbor Disco	CDP, LLPD, Link up/down events									✓						
Identity	802.1x and MAB authentication events									✓						
MAC	MAC Address Table entry changes									✓						
Hardware	Register for environmentla monitoring hardware										✓	✓				
Statistics	Threshold crossing of a statistical counter										✓	✓				
Fan (absent / bad)	Presence and State of a Fan														✓	✓
Module failure	Occurence of a Module Failure Event														✓	✓
Storm Control	Occurence of a Storm Control Event														✓	✓
Temperature	Temperature Sensor Thresholds														✓	✓

Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential 10

See Embedded Event Manager Presentation, *available at* https://goo.gl/n75rzx.

25. CoPP/LPTS and EEM are core technologies underpinning Cisco's family of networking software systems—*i.e.*, IOS, IOS XE, IOS XR, and NX-OS—

which are among the most widely deployed networking software systems in use today. Cisco has described the EEM and CoPP/LPTS features as, *inter alia*, "core," "essential," "critical," and "powerful" technologies embedded within its networking software system architecture. For instance, as depicted in the following graphic, Cisco describes EEM as providing a flexible, adaptable framework for automating many aspects of network administration, from troubleshooting and fault detection to device configuration.

> The Embedded Event Manager (EEM) also provides new components and methods to invoke customized local actions triggered by defined events such as a failure. EEM policies are created using a programmable scripting language founded in Tool Command Language (Tcl). This allows network operators to harness the vast network operational data and hardware and software diagnostics embedded within Cisco IOS Software, permitting them to monitor and proactively detect dangerous conditions that might affect network service. The EEM also includes methods to automate actions in response to those conditions. Tightly integrated with Cisco IOS Software, the EEM has intrinsic knowledge of the state of the network from the viewpoint of the device it is operating on. The ability to create programmable actions reduces reliance on a remote management system at headquarters and offers network managers far more detailed fault control. In the future, the EEM will be tightly integrated with the Enhanced Object Tracking feature, extending the range of monitoring and recovery capabilities.

See Cisco ISR White Paper, *available at* https://goo.gl/DkB19N. Cisco also describes CoPP/LPTS as providing essential security protections and reliability assurance functionality, as further explained by Cisco as follows:

> ## Benefits of Control Plane Policing
>
> Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:
>
> - Protection against DoS attacks at infrastructure routers and switches
> - QoS control for packets that are destined to the control plane of Cisco routers or switches
> - Ease of configuration for control plane policies
> - Better platform reliability and availability

See QoS: Policing and Shaping Configuration Guide, *available at* https://goo.gl/GDqsyJ.

26. These iterations of Cisco's networking software systems differ insofar as they are designed to support different types of operations: IOS supports general enterprise networking; IOS XR is designed for service-provider networks; IOS XE provides next-generation support for enterprise networks; and NX-OS is designed for data-center operations.

27. The networking software systems are similar in many ways—for instance, they share similar command-line interfaces (CLIs) for allowing system administrators to configure and monitor network operations. They also share many of the same features.

28. For example, CoPP and/or LPTS are included in all four iterations of Cisco's networking software systems running on Cisco devices. *See*, *e.g.*, Control Plane Policing Implementation Best Practices, *available at* https://goo.gl/HfpN4q (describing CoPP on IOS devices and describing LPTS on IOS XR devices as taking the "Cisco IOS CoPP concept to a new level"); Chapter: Configuring Control Plane, *available at* https://goo.gl/5mGmFM (describing CoPP on IOS XE devices); Cisco Nexus 7000 Series NX-OS Configuration Guide, *available at* https://goo.gl/K7ou84 (describing CoPP on NX-OS devices).

29. The Embedded Event Manager is similarly integrated into and across all four iterations of Cisco's networking software systems. *See* Embedded Event Manager Presentation, *available at* https://goo.gl/n75rzx.

COUNT I – CLAIM FOR INFRINGEMENT OF THE '730 PATENT

30. NetFuel incorporates and realleges Paragraphs 1 through 29 of this Complaint as if set forth fully herein.

31. Cisco directly infringes the '730 Patent pursuant to 35 U.S.C. § 271, either literally or under the doctrine of equivalents, by at least making, distributing, selling, offering for sale, and/or importing the Accused Products that are covered by one or more claims of the '730 Patent.

32. By way of a non-limiting example, each Accused Product constitutes a computer network disclosed in at least Claim 7 of the '730 patent, which includes a software agent with an assigned goal which is a programmatic expression of a predefined task for the software agent embodied in hardware; an agent support mechanism embodied in hardware that provides support to the agent; a modeler embodied in hardware to create test policy, model computer-network behavior based on the test policy, and determine an optimal policy; and a network control mechanism to dynamically modify the assigned goal of the software agent by replacing the assigned goal based on the optimal policy, wherein the software agent is operable to request further policy when it lacks an ability to perform the predefined task.

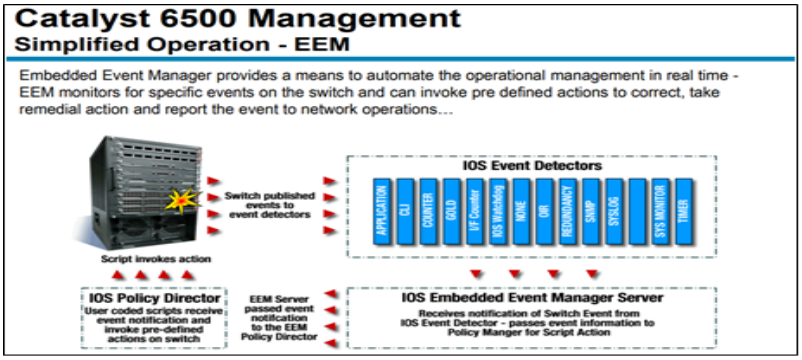
33. For example, Cisco makes and sells devices constituting a computer network, comprising a combination of connected router or switch components and interfaces, such as, *inter alia*, central processors, route processors, line cards, supervisors, forwarding engines, application-specific integrated circuits (ASICs), fabric modules, and physical and logical interfaces and sub-interfaces. Cisco also makes and sells network devices in packages so that one or more of the Accused Products will be connected.

34. By running Cisco's networking software systems—*e.g.*, an interation of IOS, IOS XR, IOS XE, or NX-OS—the Accused Products employ software agents, including, for example, CoPP/LPTS, which manage and control network traffic on and within Cisco network devices and have a variety of assigned goals, which may relate to, *inter alia*, improving network device stability, availability, or security. These goals take the form of a programmatic expression and are stored on the device. CoPP/LPTS has its own runtime environment provided by the networking software system; can communicate with other agents (as for example, through distributed and aggregate modes); can perceive its own state (*e.g.* disabled,

enabled, initialized); and can clone itself upon startup or when a network component is newly introduced into the network.

35. Cisco's networking software systems also provide an agent support mechanism embodied in hardware to the software agents operating on the Accused Products, as, for example, by providing state, access to processor resources, and memory.

36. The Accused Products also include a modeler embodied in hardware and a network control mechanism that create test policy, model computer-network behavior to determine an optimal policy, and replace the assigned goal with an optimal policy. By way of a non-limiting example, EEM's policy engines and managers contain and provision test policies that, based on events, trigger EEM to take action to instantiate the policies. EEM's test policies comprise specific requirements and are registered with EEM's policy engines and invoked when an EEM event detector has detected a triggering event (including events specific to the functions carried out by CoPP/LPTS). By using EEM event detectors in tandem with CoPP, the Accused Products predict a failure of a network component (for instance, a health score is an example of a policy that predicts failure of a network component), and dynamically replace the assigned goal at runtime with an optimal policy. The below figure provides a simplified illustration of how EEM monitors network events, invokes pre-defined corrective actions, and takes remedial action.



See Cisco Catalyst 6500 Bootcamp Presentation, *available at* https://goo.gl/TXLy22. CoPP/LPTS is also operable to request further policy when

it cannot perform a predefined task as, for example, by using APIs or network protocols (like Simple Network Management Protocol) to capture information at the control-plane interface and sending it to EEM, which can determine whether an action will be taken in response.

37. By way of another non-limiting example, each Accused Product and its users practice the inventions disclosed in at least Claim 1 of the '730 patent by assigning a goal to a software agent, monitoring the computer network, creating a test policy and modeling computer network behavior to determine an optimal computer network policy (including predicting failure of a network component), and dynamically modifying the software agent's assigned goal based on an optimal policy.

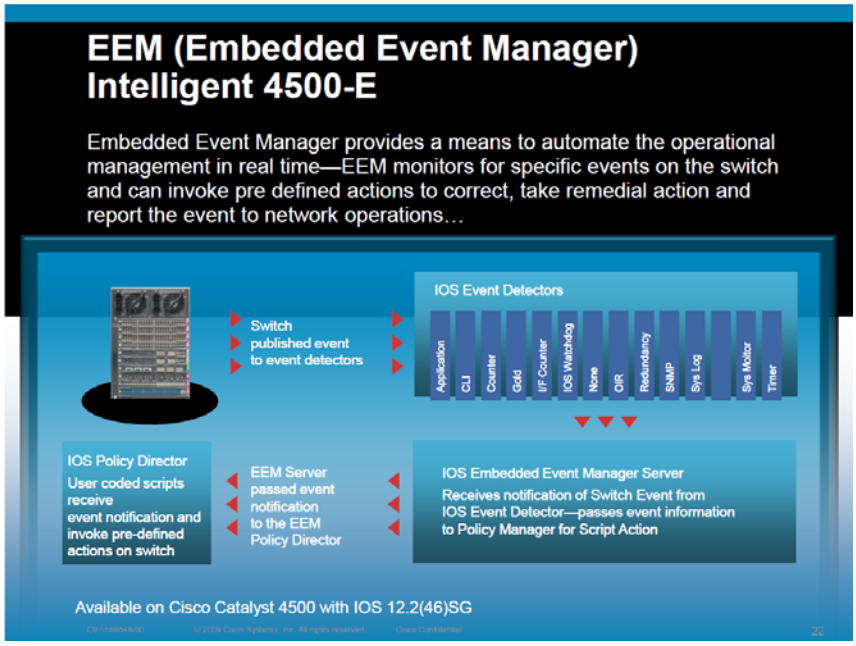
38. For example, Cisco makes and sells devices running IOS, IOS XR, IOS XE, and NX-OS networking software systems in which CoPP/LPTS is a software agent. CoPP/LPTS is provided a runtime environment by the networking software system; has the ability to communicate with other software agents in a computer network (as, for example, through distributed and aggregate modes); can perceive its own state (*e.g.*, disabled, enabled, initialized); and can clone itself upon startup or when a network component is newly introduced into the network.

39. Each goal assigned to CoPP, which may relate to, *inter alia*, improving network device stability, availability, or security, is a predefined task taking the form of a programmatic expression.

40. The Accused Products also perform monitoring of the network. For instance, CoPP/LPTS monitors network data traffic, and EEM monitors a range of network-related events, processes, and applications, including, *inter alia*, CoPP, using a variety of event detectors to trigger certain actions.

41. The Accused Products also create test policy, model computer-network behavior to determine an optimal policy, and replace the assigned goal with an optimal policy. By way of a non-limiting example, EEM's policy engines contain

test policies that, based on events, trigger the EEM to take action to instantiate the policies. EEM's test policies comprise specific requirements and are registered with EEM's policy engines and invoked when an EEM event detector has detected the triggering event (including events specific to the functions carried out by CoPP/LPTS). By using EEM event detectors in tandem with CoPP, the Accused Products predict a failure of a network component (for instance, a health score is an example of a policy that predicts failure of a network component), and dynamically replace the assigned goal at runtime with an optimal policy. The below figure provides a simplified illustration of how EEM monitors network events, invokes pre-defined corrective actions, and takes remedial action.

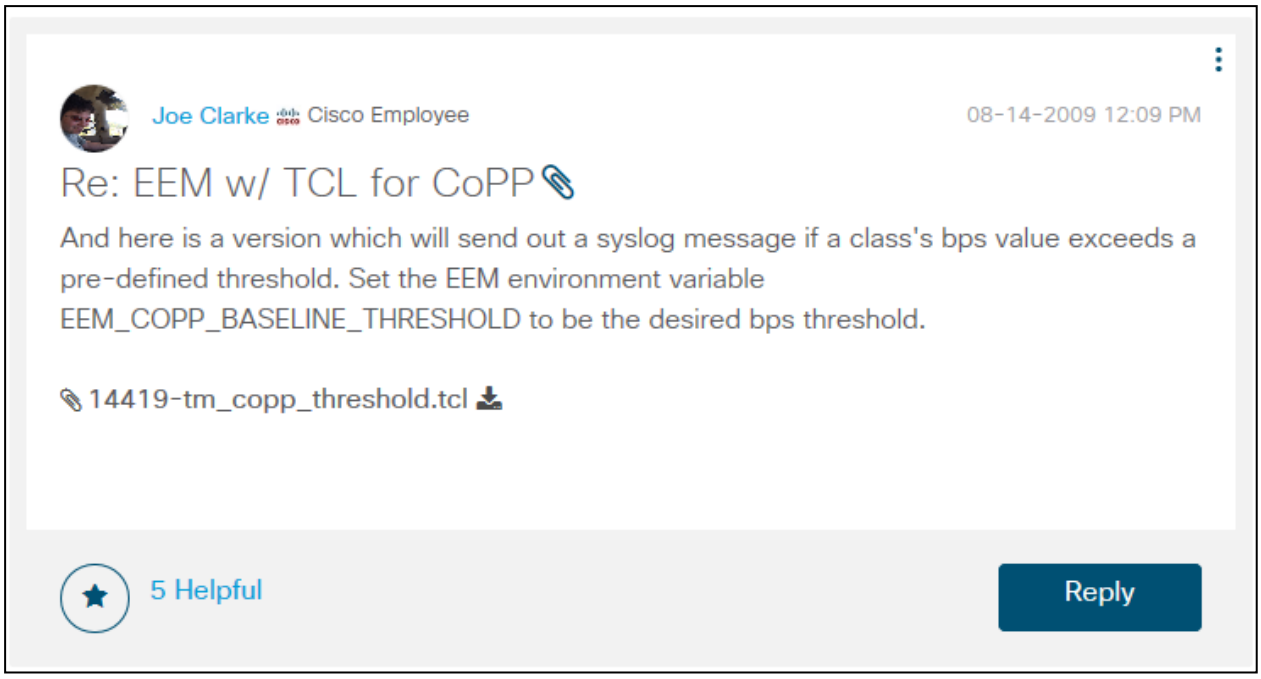


See Cisco Catalyst 4500-E Presentation, *available at* https://goo.gl/F2ejtY.

42. Cisco also actively induces infringement of the inventions disclosed in the '730 patent. Cisco's resellers, partners, third-party maintenance and service providers, instructors, students, customers, and end users directly infringe the Patents-in-Suit, including by performing the methods as described in paragraphs 37 through 41 using the Accused Products. Cisco knowingly induces that infringement by directing, instructing, and/or encouraging these resellers, partners, third-party

maintenance and service providers, instructors, students, customers, and end users to perform the infringing the methods.

43. Cisco provides to its customers and partners an extensive repository of user manuals, training material, books, reference guides, whitepapers, videos, user forums, and other information that Cisco intends to be used to instruct and direct users of the Accused Devices to configure the Accused Products and/or networks in such a way as to practice the Patents-in-Suit, or to put the Accused Products into use in such a way as to practice the Patents-in-Suit. As but one example, Cisco provides configuration guides and instructs its users to download and install scripts that, *inter alia*, learn from network data, generate alerts and trigger specific actions to take place when a particular event occurs.



See Cisco Support Community Forum, *available at*: https://goo.gl/JZvuR4. Cisco also publishes a large number of configuration guides that explain to users how to set up and configure EEM and CoPP/LPTS. See, e.g., Cisco Nexus 7000 Series NX-OS Security Configuration Guide Chapter: Configuring Control Plane Policing, available at: https://goo.gl/j47m6r; Cisco ASR 1000 Series Aggregation Services

Router Embedded Event Manager Configuration Guide, available at: https://goo.gl/ZxtYwL.

44. Cisco has had actual knowledge of the existence of the Patents-in-Suit's pending patent application since the early 2000s. In early 2003, Mr. Harlow and his business partner in NetFuel met with Dave Ward, then a Cisco Fellow and currently Cisco's current Senior Vice President, Chief Architect, and Chief Technology Officer for Engineering. At the time of the meeting, Mr. Ward was responsible for designing Cisco's IOS-XR operating system and various carrier, aggregation-services, and gigabit-switch routers and other line cards. The meeting with Mr. Ward was set up by Anson Chen, Cisco's then-head of Network Technology, who indicated that the purpose of the meeting was for Cisco to evaluate NetFuel's innovations and potential contribution to Cisco. During the meeting, Mr. Harlow presented NetFuel's innovations in software-defined networking, including the use of software agents to partially automate certain network-management functions. Mr. Harlow also disclosed that he was in the process of seeking patent protection for his technology, and showed a presentation he had made to the ACM OpenSig ("One-Pair Ether-Net Special Interest Group") alliance at the Imperial College of London in London, UK, which indicated Mr. Harlow was seeking patent protection for his invention.

45. Upon information and belief, Cisco remained aware of the pending patent application for the Patents-in-Suit when, in the mid-2000s, and over the course of several years, senior personnel from or closely affiliated with Cisco, including its then-Chief Technology Officer, Charles Giancarlo, the second in command to Cisco's then-head of network technology, Anson Chen, and Cisco's former outside director and board member, Bob Puette. These individuals approached Mr. Harlow at Mr. Puette's ranch and spoke with him about potential ways to license, fund, or otherwise work with NetFuel's technology. In a conversation with Mr. Giancarlo in or about July of 2007, Mr. Giancarlo inquired

about NetFuel's intellectual property protections, and Mr. Harlow indicated that his patent application had been pending for several years.

46. In addition, in late 2001, a significant amount of NetFuel's codebase and marketing presentations describing Mr. Harlow's invention were stolen by a then-NetFuel engineer, Jian "Jerry" Zhong, along with two other employees. Mr. Zhong stored copies of the stolen codebase and marketing presentations on his NetFuel-provided laptop. Upon information and belief, Mr. Zhong was aware of Harlow's draft patent application (which was filed with the U.S. PTO several months after the theft), and was married to Lan Zhang, then a senior operating-systems engineer for Cisco. The theft was reported to the local assistant district attorney and, as a result, the Santa Clara County's sheriff department conducted a raid on the engineers' homes, finding media and storage devices containing the stolen codebase and presentations. Upon information and belief, Mr. Zhong shared the stolen information with Ms. Zhang, who frequently used Mr. Zhong's NetFuel-provided laptop at home.

47. In addition, other Cisco personnel or affiliates were made aware of Mr. Harlow's technology in September 2001, when Mr. Harlow made the aforementioned presentation at the ACM OpenSig 2001 Program ("One-Pair Ether-Net Special Interest Group") alliance at Imperial College of London, in London, UK regarding the use of software agents in network operating systems. In attendance at the meeting were Dr. Morris Sloman, who, six months after the presentation, became a principal investigator for Cisco (for a two-year project), and Dr. Jon Crowcroft, a professor at Cambridge University who served on Cisco's editorial advisory board beginning in June 2001. The presentation made by Mr. Harlow indicated that he was in the process of seeking a patent on his technology.

48. At a minimum, Cisco has had actual knowledge of the existence of the Patents-in-Suit no later than the filing and service of this Complaint.

49. Cisco's acts of infringement have caused damage to Plaintiff, and Plaintiff is entitled to recover from Cisco (or any successor entity to Cisco) the damages sustained by Plaintiff as a result of Cisco's wrongful acts in an amount subject to proof at trial.

COUNT II – CLAIM FOR INFRINGEMENT OF THE '659 PATENT

50. Plaintiff incorporates by reference Paragraphs 1 through 49 above.

51. Cisco directly infringes the '659 Patent pursuant to 35 U.S.C. § 271, either literally or under the doctrine of equivalents, by at least making, distributing, selling, offering for sale, and/or importing the Accused Products that are covered by one or more claims of the '659 Patent.

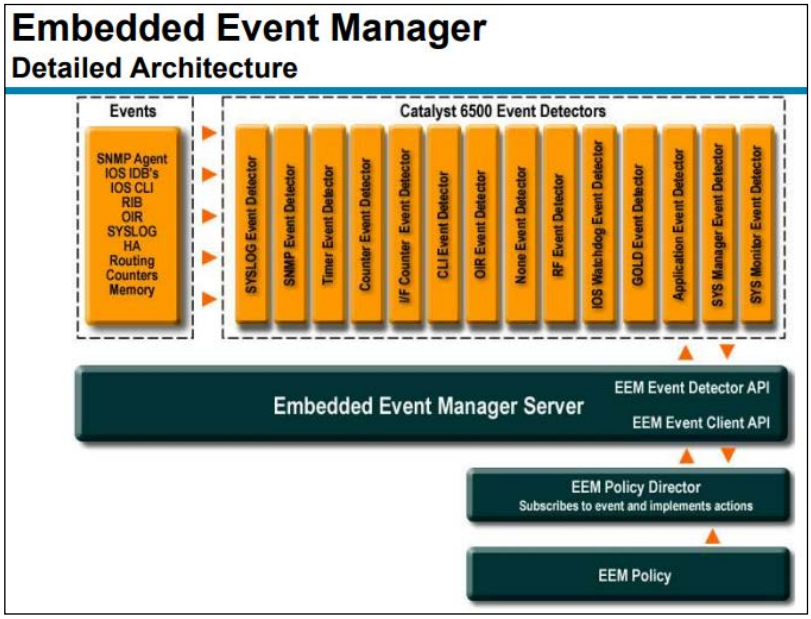
52. By way of a non-limiting example, Cisco directly infringes the inventions disclosed in the '659 patent, by making and selling devices comprising the system described in Claim 13.

53. For example, the Accused Products each constitute a system having a processor and a memory, the latter of which stores instructions for running Cisco's networking software systems (IOS, IOS XE, IOS XR, NX-OS) which, when executed, perform the method described in the invention.

54. The EEM and CoPP/LPTS software features—all of which run on the Accused Products' networking software systems—run at least one thread in a runtime environment.

55. The runtime environments made available by the Accused Products' operating systems provide each thread and each process state as well as access to system resources within each device.

56. The EEM software feature monitors a thread's operational parameters, including per-thread utilization for, *inter alia*, Cisco operating-system software processes, such as CoPP/LPTS and other applications or features running on the Accused Products. The graphic below provides a simplified illustration of EEM's monitoring and event-detection architecture.



See Catalyst 6500 Bootcamp Presentation, *available at*: https://goo.gl/TXLy22.

57. Among other infringing features, EEM's event detectors are configured to detect an operational abnormality in the monitored operational parameters, and can take corrective policy-implementation actions, which involves requesting a corrective policy from a global modeler external to the first runtime environment (for example, the EEM server), if the corrective policy is not first available to an agent operating in the first runtime environment.

58. Cisco also actively induces infringement of the inventions disclosed in the '659 patent. Cisco's resellers, partners, third-party maintenance and service providers, instructors, students, customers, and end users directly infringe the Patents-in-Suit, including by setting up and configuring the system as described in paragraphs 52 through 57 using the Accused Products. Cisco knowingly induces that infringement by directing, instructing, and/or encouraging these resellers, partners, third-party maintenance and service providers, instructors, students, customers, and end users to use the patent system.

59. Cisco provides to its customers and partners an extensive repository of user manuals, training material, books, reference guides, whitepapers, videos, and

other information that Cisco intends to be used to instruct and direct users to set up and configure the Accused Products and/or networks in such a way as to practice the Patents-in-Suit, or to put the Accused Products into use in such a way as to practice the Patents-in-Suit. As but one example, Cisco publishes a large number of configuration guides that explain to users how to set up and configure EEM and CoPP/LPTS. *See, e.g.*, Cisco Nexus 7000 Series NX-OS Security Configuration Guide Chapter: Configuring Control Plane Policing, *available at*: https://goo.gl/j47m6r; Cisco ASR 1000 Series Aggregation Services Router Embedded Event Manager Configuration Guide, *available at*: https://goo.gl/ZxtYwL.

60. As described in paragraphs 44 through 48, Cisco had knowledge of the patent application that led to the issuance of the '659 patent.

61. At a minimum, Cisco has had actual knowledge of the existence of the '659 patent no later than the filing and service of this Complaint.

62. Cisco's acts of infringement have caused damage to Plaintiff, and Plaintiff is entitled to recover from Cisco (or any successor entity to Cisco) the damages sustained by Plaintiff as a result of Cisco's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff NETFUEL, INC. requests entry of judgment in its favor and against Defendant CISCO SYSTEMS, INC. as follows:

a) A declaration that Cisco has infringed United States Patent Nos. 7,747,730 and 9,663,659;

b) An award of damages arising out of Cisco's infringement of U.S. Patent Nos. 7,747,730 and 9,663,659 to Plaintiff, together with prejudgment and post-judgment interest, in an amount according to proof;

c) An award of attorney's fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law; and

d) For such other costs and further relief as the Court may deem just and proper.

Dated: January 31, 2019

By: */s/ Floyd G. Short*

Floyd G. Short (*pro hac vice*)
Matthew R. Berry (*pro hac vice*)
Steven M. Seigel (*pro hac vice*)
P. Ryan Burningham (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101-3000
Telephone: (206) 516-3800
Facsimile: (206) 516-3883
fshort@susmangodfrey.com
mberry@susmangodfrey.com
sseigel@susmangodfrey.com
rburningham@susmangodfrey.com

Kalpana Srinivasan (237460)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100
Facsimile: (310) 789-3150
ksrinivasan@susmangodfrey.com

Attorneys for Plaintiff NetFuel, Inc.

DEMAND FOR JURY TRIAL

NetFuel, Inc. demands a trial by jury on all issues triable in this action pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: January 31, 2019

By: */s/ Floyd G. Short*

Floyd G. Short (*pro hac vice*)
Matthew R. Berry (*pro hac vice*)
Steven M. Seigel (*pro hac vice*)
P. Ryan Burningham (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101-3000
Telephone: (206) 516-3800
Facsimile: (206) 516-3883
fshort@susmangodfrey.com
mberry@susmangodfrey.com
sseigel@susmangodfrey.com
rburningham@susmangodfrey.com

Kalpana Srinivasan (237460)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100
Facsimile: (310) 789-3150
ksrinivasan@susmangodfrey.com

Attorneys for Plaintiff NetFuel, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on January 31, 2019, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ Floyd G. Short