UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

SABLE NETWORKS, INC. AND SABLE IP, LLC, ***Plaintiffs,*** v. **JUNIPER NETWORKS, INC.,** ***Defendant.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Sable Networks, Inc. and Sable IP, LLC (collectively, "Sable" or "Plaintiffs") bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 6,954,431 (the "'431 patent"); 6,977,932 (the "'932 patent"); 7,630,358 (the "'358 patent"); 8,085,775 (the "'775 patent"); 8,243,593 (the "'593 patent"); and 8,817,790 (the "'790 patent") (collectively, the "patents-in-suit"). Defendant Juniper Networks, Inc. ("Juniper" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.[1] The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the

[1] Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) ("Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.").

increasing amount of data sent over computer networks.

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.[2] Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.

Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router,* IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001)("Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency's Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.").

3. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a

[2] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

destination. "In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using those tiny data packets to send information from place to place."[3] Packet switching has become the primary technology for data communications over computer networks.

From Two Small Nodes, a Mighty Web Has Grown

By 1966, with these and other basic ideas in place, Lawrence Roberts, recruited by ARPA from the Massachusetts Institute of Technology, mapped out the plan. Two years after the first transmission, the number of host computers grew to 23. The @ symbol was invented in 1972, and a year later 75 percent of the Arpanet traffic was E-mail. It was starting to look like the Net.").

George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.[4] Dr. Roberts identified that as the "Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in."[5]

> ***The Internet is broken. I should know: I designed it***. In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic-I called them Interface Message Processors, or IMPs-evolved into today's

[3] Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) ("The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.").

[4] eWeek Editors, *Feeling A Little Congested,* EWEEK MAGAZINE (September 24, 2001) ("Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.").

[5] Michael Cooney, *Can ATM Save The Internet,* NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

> routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

5. In 1998, Dr. Roberts founded Caspian Networks.[6] At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network "gridlock." In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. "Roberts says the Apeiro will also create new revenue streams for the carriers by solving the 'voice and video problem.' IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient."[7]

Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

[6] Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

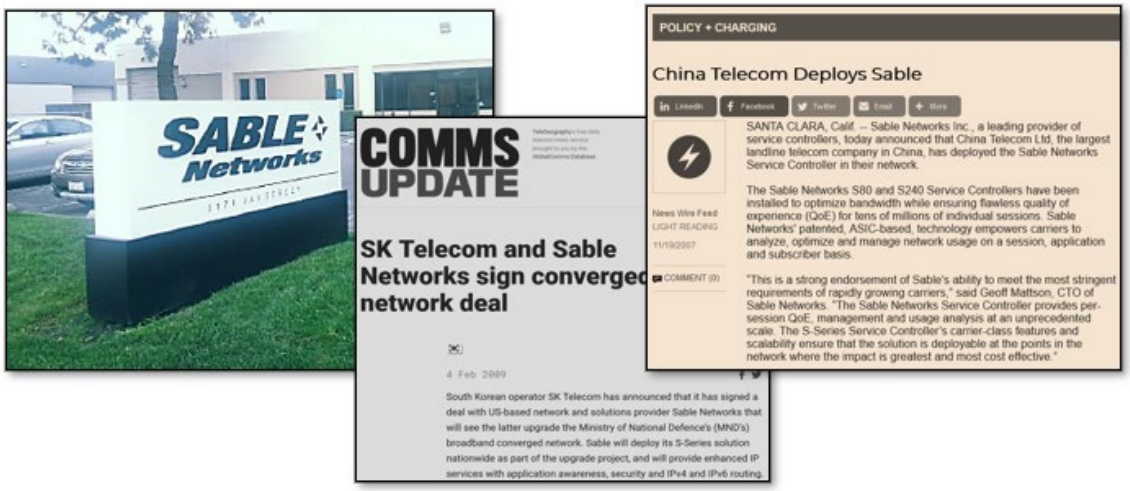
[7] John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included numerous technological advances including quality of service (QoS) routing and flow-based routing.

7. At its height, Caspian Networks Inc. raised more than $300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

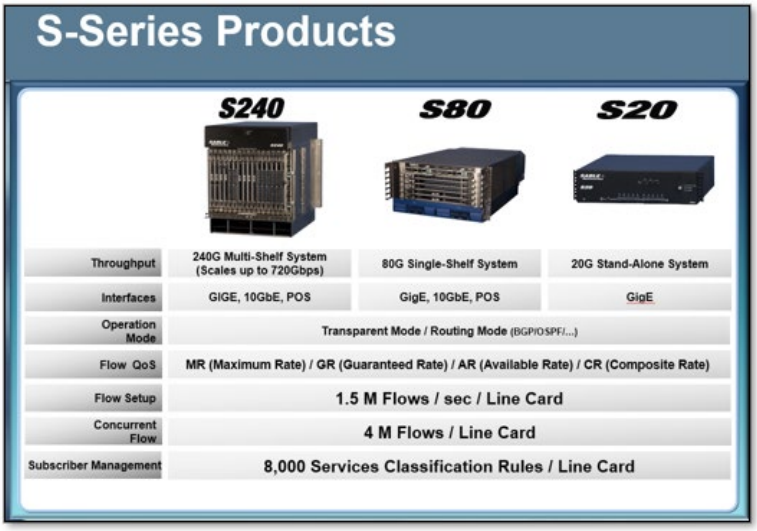
8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.[8] Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

[8] Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.



SK Telecom and Sable Networks Sign Convergence Network Deal, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) ("South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks."); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) ("Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.").

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks' technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts' flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits ("ASIC") designed for flow traffic management. Sable Network, Inc.'s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (*e.g.*, S80 and S240 Service Controller models) that contain Sable Networks' flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for Juniper's use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

SABLE'S PATENT PORTFOLIO

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.[9]

[9] *See, e.g.*, U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

- ***Juniper Networks, Inc.***[10]
- Broadcom Limited[11]
- EMC Corporation[12]
- F5 Networks, Inc.[13]
- Verizon Communications Inc.[14]
- Microsoft Corporation[15]
- Intel Corporation[16]
- Extreme Networks, Inc.[17]
- Huawei Technologies Co., Ltd.[18]

13. The Sable patent portfolio has been cited by Juniper in over 37 of its own patents and patent applications.

THE PARTIES

SABLE NETWORKS, INC.

14. Sable Networks, Inc. ("Sable Networks") is a corporation organized and existing under the laws of the State of California.

15. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts

[10] *See, e.g.*, U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

[11] *See, e.g.*, U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

[12] *See, e.g.*, U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

[13] *See, e.g.*, U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

[14] *See, e.g.*, U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

[15] *See, e.g.*, U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

[16] *See, e.g.*, U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

[17] *See, e.g.*, U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

[18] *See, e.g.*, U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.

to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

16. Sable Networks is the owner by assignment of all of the patents-in-suit.

SABLE IP, LLC

17. Sable IP, LLC ("Sable IP") is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

JUNIPER NETWORKS, INC.

18. Juniper Networks, Inc. ("Juniper"), is a Delaware corporation with its principal place of business at 1133 Innovation Way, Sunnyvale, California 94089. Juniper may be served through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, Juniper is registered to do business in the State of Texas and has been since at least April 27, 2017.

19. Juniper conducts business operations within the Western District of Texas in its facilities at 1120 South Capital of Texas Highway, Suite 120, First Floor, Building 2, Austin, Texas 78746. Juniper has offices in the Western District of Texas where it sells and/or markets its products, including an office in Austin, Texas.

JURISDICTION AND VENUE

20. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

21. This Court has personal jurisdiction over Juniper in this action because Juniper has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Juniper would not offend traditional notions of fair play and substantial justice. Defendant Juniper, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Juniper is registered to do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

22. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Juniper is registered to do business in the State of Texas, has offices in the State of Texas, and upon information and belief, has transacted business in the Western District of Texas and has committed acts of direct and indirect infringement in the Western District of Texas. Juniper maintains a regular and established place of business in the Western District of Texas, including an office in Austin, Texas.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,954,431

23. U.S. Patent No. 6,954,431 (the "'431 patent") entitled, *Micro-Flow Management*, was filed on December 6, 2001, and claims priority to April 19, 2000. The '431 patent is subject to a 35 U.S.C. § 154(b) term extension of 722 days. Sable Networks, Inc. is the owner by assignment of the '431 patent. Sable IP is the exclusive licensee of the '431 patent. A true and correct copy of the '431 patent is attached hereto as Exhibit A.

24. The '431 patent discloses novel methods and systems for managing data traffic comprising a plurality of micro-flows through a network.

25. The inventions disclosed in the '431 patent improve the quality of service in data transmissions over a computer network by relying on per micro-flow state information that enables rate and delay variation requirements to be within set quantified levels of service.

26. The '431 patent discloses technologies that speed the rate at which data can effectively travel over a computer network by optimizing packet discarding.

27. The '431 patent discloses the use of micro-flow state information to determine the rate of each flow, thus optimizing discards and optimizing the quality of service of data transmission.

28. The '431 patent discloses methods and systems that avoid networking system degradation by not overloading network switch buffers.

29. The '431 patent discloses a method for managing data traffic through a network that determines a capacity of a buffer containing a micro-flow based on a characteristic.

30. The '431 patent discloses a method for managing data traffic through a network that assigns an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

31. The '431 patent discloses a method for managing data traffic through a network that delegates a portion of available bandwidth in the network to the micro-flow.

32. The '431 patent discloses a method for managing data traffic through a network that uses the buffer for damping jitter associated with the micro-flow.

33. The '431 patent has been cited by 103 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '431 patent as relevant prior art:

- Cisco Systems, Inc.
- ***Juniper Networks, Inc.***

- Broadcom Limited
- Intel Corporation
- Sun Microsystems, Inc.
- Oracle Corporation
- Samsung Electronics Co., Ltd.
- Adtran, Inc.
- Time Warner Cable, Inc.
- FSA Technologies, Inc.
- Internap Corporation
- France Telecom
- The Boeing Company
- Wistaria Trading, Ltd.

U.S. PATENT NO. 6,977,932

34. U.S. Patent No. 6,977,932 (the "'932 patent") entitled, *System and Method for Network Tunneling Utilizing Micro-Flow State Information*, was filed on January 16, 2002. The '932 patent is subject to a 35 U.S.C. § 154(b) term extension of 815 days. Sable Networks, Inc. is the owner by assignment of the '932 patent. Sable IP is the exclusive licensee of the '932 patent. A true and correct copy of the '932 patent is attached hereto as Exhibit B.

35. The '932 patent discloses novel methods and apparatuses for utilizing a router capable of network tunneling utilizing flow state information.

36. The inventions disclosed in the '932 patent enable the use of micro-flow state information to improve network tunneling techniques.

37. The inventions disclosed in the '932 patent maintain flow state information for various quality of service characteristics by utilizing aggregate flow blocks.

38. The aggregate flow blocks disclosed in the '932 patent maintain micro-flow block information.

39. The technologies claimed in the '932 patent speed the flow of network traffic over computer networks by avoiding time consuming and processor intensive tasks by combining flow state information with other information such as label switched paths utilization information. This

permits the micro-flows associated with an aggregate flow block to all be processed in a similar manner.

40. The technologies disclosed in the '932 patent result in more efficient computer networks by avoiding the processor intensive tasks of searching millions of flow blocks to identify flow blocks having certain micro-flow characteristics in order to process large numbers of micro-flows.

41. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing an aggregate flow block having tunnel specific information for a particular network tunnel.

42. The '932 patent discloses a router capable of network tunneling utilizing flow state information containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block.

43. The '932 patent discloses a router capable of network tunneling utilizing flow state information wherein the aggregate flow block stores statistics for the particular network tunnel.

44. The '932 patent has been cited by 86 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '932 patent as relevant prior art:

- Cisco Systems, Inc.
- ***Juniper Networks, Inc.***
- Avaya, Inc.
- Fujitsu, Ltd.
- Intel Corporation
- Nokia Corporation
- Qualcomm, Inc.
- Sprint Communications Co.
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 7,630,358

45. U.S. Patent No. 7,630,358 ("the '358 patent") entitled, *Mechanism for Implementing Multiple Logical Routers Within A Single Physical Router*, was filed on July 9, 2002, and claims priority to July 9, 2001. The '358 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,136 days. Sable Networks, Inc. is the owner by assignment of the '358 patent. Sable IP is the exclusive licensee of the '358 patent. A true and correct copy of the '358 patent is attached hereto as Exhibit C.

46. The '358 patent claims specific methods and systems for implementing multiple logical routers within a single physical router.

47. The '358 patent discloses systems and methods that combine the benefits of multi-routers and virtual routers. The logical routers are included within the same physical router; however, internal links permit improved efficiency over virtual routers because the technologies claimed in the '358 patent can take advantage of the fact that the logical routers are not standalone routers bur are embodied in the same physical router.

48. The '358 patent discloses technology for implementing multiple logical routers within a single physical router.

49. The '358 patent discloses a router with a first set of one or more components capable of being figured to implement a first logical router within the router.

50. The '358 patent discloses a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

51. The '358 patent discloses a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

52. The '358 patent discloses a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

53. The '358 patent has been cited by 42 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the '358 patent as relevant prior art:

- Cisco Systems, Inc.
- Dell Technologies, Inc.
- ***Juniper Networks, Inc.***
- Nicira, Inc.
- International Business Machines Corporation
- NantWorks, LLC
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 8,085,775

54. U.S. Patent No. 8,085,775 (the "'775 patent") entitled, *Identifying Flows Based On Behavior Characteristics And Applying User-Defined Actions*, was filed on July 31, 2006. The '775 patent is subject to a 35 U.S.C. § 154(b) term extension of 467 days. Sable Networks, Inc. is the owner by assignment of the '775 patent. Sable IP is the exclusive licensee of the '775 patent. A true and correct copy of the '775 patent is attached hereto as Exhibit D.

55. The '775 patent discloses novel methods for identifying and handling a single application flow of a plurality of information packets.

56. The inventions disclosed in the '775 patent teach methods of identifying, classifying, and controlling information packet flows based on their observed behavior rather than the content of the data packets.

57. The '775 patent teaches technologies that can effectively identify and control specific types of data traffic despite attempts to conceal the content or type of traffic represented by the data packets.

58. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that creates a flow block as the first packet of a flow is processed by a router.

59. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that utilizes a flow block adapted to store payload-content agnostic behavioral statistics about the flow.

60. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that updates the flow block with the flow's payload-content agnostic behavioral statistics as packets belonging to the flow are processed by the router.

61. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that utilizes a flow incapable of being identified by header information alone.

62. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that heuristically determines whether at least one user-specified policy is satisfied by the payload-content agnostic behavioral statistics stored in the flow block.

63. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein the payload-content agnostic behavioral statistics for the flow are calculated by the router.

64. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein the payload-content agnostic behavioral statistics reflect the empirical behavior of the flow.

65. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein at least one of the payload-content agnostic behavioral statistics is one of the following characteristics: (1) total byte count accumulated for the flow, (2) flow life duration, (3) average rate of flow, (4) average packet size, (5) average packet rate, (6) average inter-packet gap, (7) instantaneous flow rate, and (8) moving average flow rate.

66. The '775 patent has been cited by 36 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the '775 patent as relevant prior art:

- Cisco Systems, Inc.
- Calix, Inc.
- British Telecommunications Public Limited Company
- Extreme Networks, Inc.
- Fujitsu Ltd.
- Level 3 Communications, Inc.
- Nokia Corporation
- Sprint Spectrum L.P.
- Solana Networks Inc.
- Taiwan Semiconductor Mfg. Co. Ltd.
- Verizon Communications, Inc.

U.S. PATENT NO. 8,243,593

67. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The '593 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit E.

68. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

69. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

70. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

71. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

72. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

73. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

74. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

75. The '593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

76. The '593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

77. The '593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

U.S. PATENT NO. 8,817,790

78. U.S. Patent No. 8,817,790 (the "'790 patent") entitled, *Identifying Flows Based on Behavior Characteristics and Applying User-Defined Actions*, was filed on September 23, 2011, and claims priority to July 31, 2006. Sable Networks, Inc. is the owner by assignment of the '790 patent. Sable IP is the exclusive licensee of the '790 patent. A true and correct copy of the '790 patent is attached hereto as Exhibit F.

79. The '790 patent claims specific methods and devices for handling a flow of information packets.

80. The '790 patent discloses methods and systems for efficiently identifying undesirable traffic over data networks.

81. The '790 patent teaches technologies that identify traffic not by inspecting the payload of each data packet, but rather by analyzing and classifying the behavior of the data flows to identify undesirable traffic.

82. The '790 patent discloses applying a user-specified action associated with a policy applicable to data flows that are designated undesirable.

83. The '790 patent discloses a method of handling a flow that processes a flow comprised of two or more information packets having header information in common.

84. The '790 patent discloses a method of handling a flow that stores header-independent statistics about the flow in a flow block associated with the flow.

85. The '790 patent discloses a method of handling a flow that updates the header-independent statistics in the flow block as each information packet belonging to the flow is processed.

86. The '790 patent discloses a method of handling a flow that categorizes the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

87. The '790 patent discloses a method of handling a flow that performs an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

88. The '790 patent family has been cited by 24 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '790 patent family as relevant prior art:

- Cisco Systems, Inc.
- Solana Networks, Inc.
- British Telecommunications Public Limited Company
- Level 3 Communications, LLC
- Calix, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Sprint Spectrum L.P.
- Hon Hai Precision Industry Co., Ltd.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,954,431

89. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

90. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing data traffic comprising a plurality of micro-flows through a network.

91. Juniper designs, makes, sells, offers to sell, imports, and/or uses Juniper devices that manage data traffic comprised of micro-flows, including the following router models: ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5448, ACX6160, and ACX6360 (collectively, the "'431 Product(s)").

92. One or more Juniper subsidiaries and/or affiliates use the Juniper '431 Products in regular business operations.

93. One or more of the Juniper '431 Products include technology for managing data traffic comprising a plurality of micro-flows through a network.

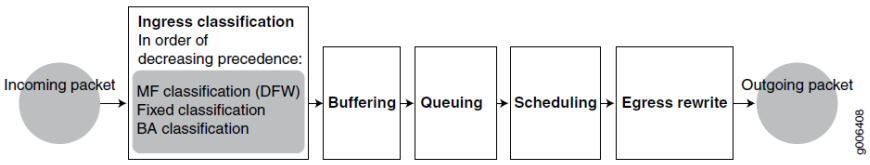
94. The following excerpt from Juniper documentation shows that the Juniper '431 Products support the buffering of micro-flows. Specifically, the Juniper '431 Products assign a class of service ("CoS") to each micro-flow. The CoS is the characteristic that then is used by the Juniper '431 Products to determine the appropriate size of the buffer (queue).

> All the child policers must be of single-rate, single-bucket, and two-color modes for bandwidth guarantee mode of hiearchical policer. This combination of attributes is also called floor mode. The micro-flow policer value specifies the minimum guaranteed bandwidth (CIR) for the micro-flow. The macro-flow policer value specifies the maximum allowed bandwidth (PIR) for all the flows. The sum or the cumulative value of all CIR values of the configured micro-flows must be less than or equal to the macro-flow PIR. The burst size of macro-flow must be greater than the sum of the aggregate of the burst size of all the child policers and the largest MTU of the physical interface among all the physical interfaces of the logical interfaces or interface families to which the child policers are attached.

Junos OS Routing Policies, *Firewall Filters, and Traffic Policers User Guide,* JUNIPER DOCUMENTATION at 1686 (April 6, 2020) (emphasis added).

95. One or more of the Juniper '431 Products determine the capacity of a buffer containing a micro-flow based on a characteristic. The following excerpt from Juniper's documentation of the Juniper '431 products shows that the ACX Series Routers take in a data packet and assign it to a micro-flow. The micro-flow is associated with a class of service that then determines the size of the buffer so that jitter can be minimized.

Figure 4: ACX Series Router Packet Forwarding and Data Flow

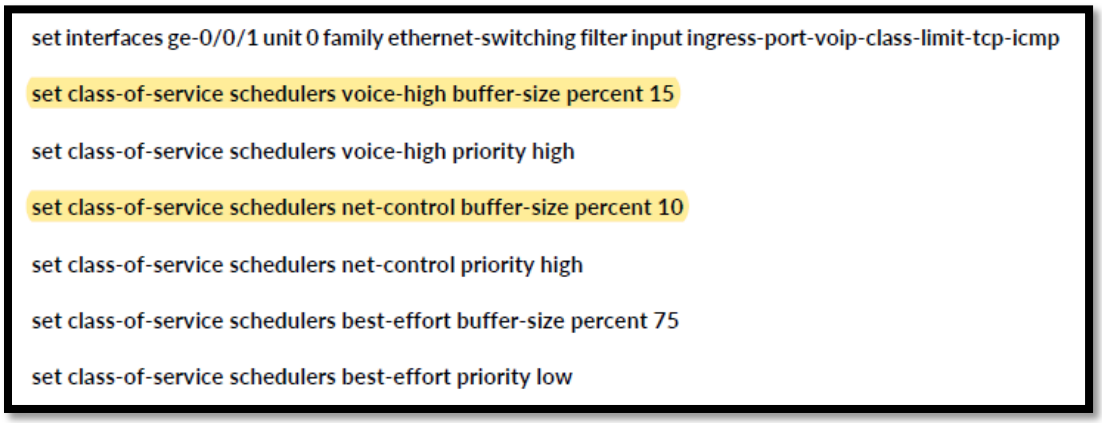


Based on the model, ACX Series routers contain a built-in Routing Engine and Packet Forwarding Engine and can contain both T1/E1 and Gigabit Ethernet Ports.

The Packet Forwarding Engine has one or two "pseudo" Flexible PIC Concentrators. Because there is no switching fabric, the single Packet Forwarding Engine takes care of both ingress and egress packet forwarding.

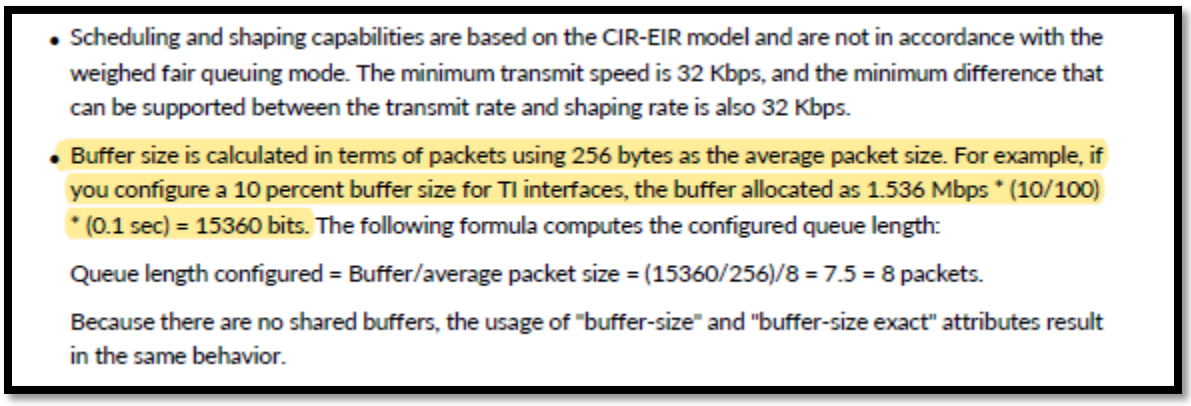
ACX4000 UNIVERSAL METRO ROUTER HARDWARE GUIDE at 23 (March 31, 2019).

96. One or more of the Juniper '431 Products assign an acceptable threshold value for the capacity of the buffer over a predetermined period of time. The following excerpt from Juniper documentation shows that for certain types of data such as "voice" the buffer size is assigned a threshold value of 15 percent.



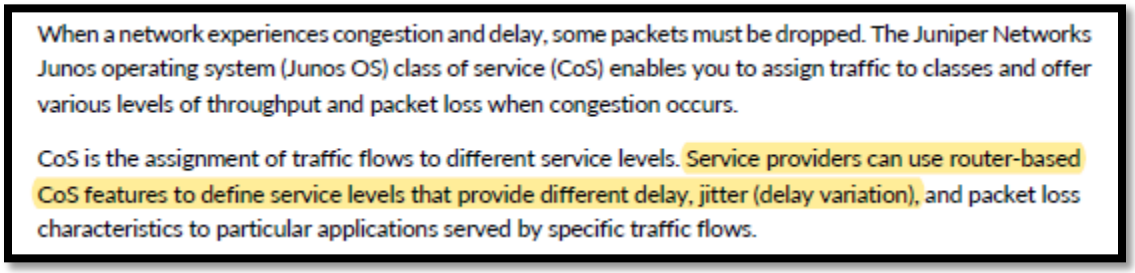
Junos OS Routing Policies, Firewall Filters, and Traffic Policers User Guide, JUNIPER DOCUMENTATION at 1454 (April 6, 2020) (emphasis added).

97. One or more of the Juniper '431 Products use the buffer for damping jitter associated with the micro-flow. The buffer size value is based on a specific time value. For example, the below excerpt from Juniper documentation shows how the buffer size is based on the number of bytes that can be stored in a buffer * 0.1 seconds.



Junos OS Class of Service User Guide (Routers and EX9200 Switches), JUNIPER DOCUMENTATION AT 609 (March 18, 2020) (emphasis added).

98. The Juniper '431 Products perform the step of using the buffer for damping jitter associated with the microflow. Juniper documentation describes that the assignment of buffer thresholds (sizing the queue associated with a micro-flow) is used by the Juniper '431 Products to reduce "jitter" for specific traffic flows.



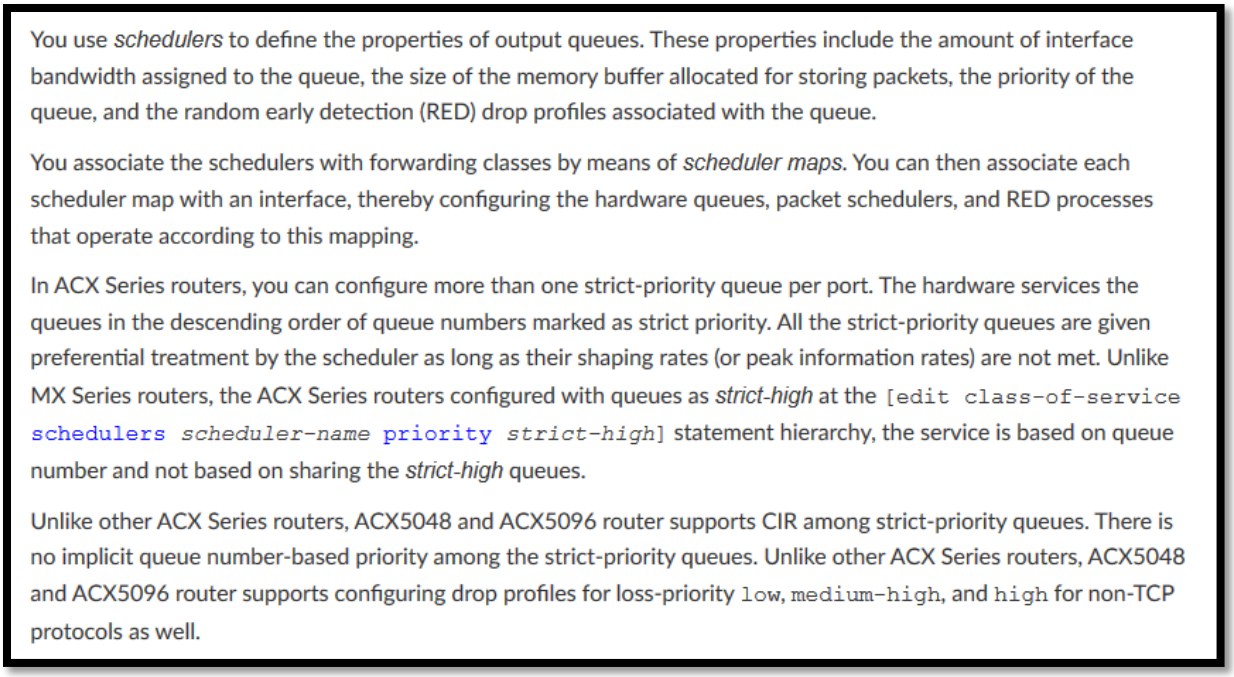
When a network experiences congestion and delay, some packets must be dropped. The Juniper Networks Junos operating system (Junos OS) class of service (CoS) enables you to assign traffic to classes and offer various levels of throughput and packet loss when congestion occurs.

CoS is the assignment of traffic flows to different service levels. Service providers can use router-based CoS features to define service levels that provide different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows.

Junos OS Class of Service User Guide (Routers and EX9200 Switches), JUNIPER DOCUMENTATION AT 3 (March 18, 2020) (emphasis added).

99. The Juniper '431 Products use buffers to limit jitter which is delay variance.

100. One or more of the Juniper '431 Products delegate a portion of available bandwidth in the network to the micro-flow. The following excerpt from Juniper's documentation describes the use of schedulers to "define" the "size of the memory buffer allocated for storing packets." The scheduler uses the CoS value to assign the size of the buffer.



You use *schedulers* to define the properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue.

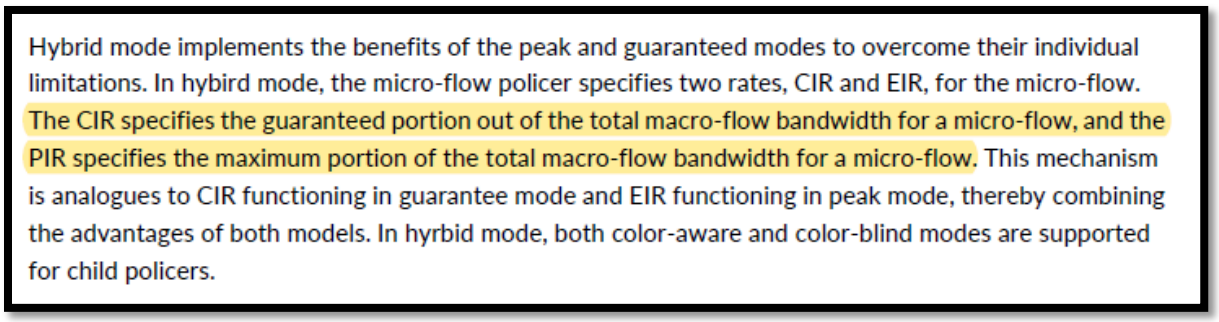
You associate the schedulers with forwarding classes by means of *scheduler maps*. You can then associate each scheduler map with an interface, thereby configuring the hardware queues, packet schedulers, and RED processes that operate according to this mapping.

In ACX Series routers, you can configure more than one strict-priority queue per port. The hardware services the queues in the descending order of queue numbers marked as strict priority. All the strict-priority queues are given preferential treatment by the scheduler as long as their shaping rates (or peak information rates) are not met. Unlike MX Series routers, the ACX Series routers configured with queues as *strict-high* at the `[edit class-of-service schedulers scheduler-name priority strict-high]` statement hierarchy, the service is based on queue number and not based on sharing the *strict-high* queues.

Unlike other ACX Series routers, ACX5048 and ACX5096 router supports CIR among strict-priority queues. There is no implicit queue number-based priority among the strict-priority queues. Unlike other ACX Series routers, ACX5048 and ACX5096 router supports configuring drop profiles for loss-priority `low`, `medium-high`, and `high` for non-TCP protocols as well.

Junos OS Class of Service User Guide (Routers and EX9200 Switches), JUNIPER DOCUMENTATION AT 604 (March 18, 2020).

101. The Juniper '431 Products enable the setting of thresholds for a buffer that include the ability to set a threshold as a percentage of the buffer. Specifically, the Juniper '431 Products assign to each micro-flow a class of service value that, through the scheduler, determines the capacity of the buffer.



Hybrid mode implements the benefits of the peak and guaranteed modes to overcome their individual limitations. In hybird mode, the micro-flow policer specifies two rates, CIR and EIR, for the micro-flow. The CIR specifies the guaranteed portion out of the total macro-flow bandwidth for a micro-flow, and the PIR specifies the maximum portion of the total macro-flow bandwidth for a micro-flow. This mechanism is analogues to CIR functioning in guarantee mode and EIR functioning in peak mode, thereby combining the advantages of both models. In hyrbid mode, both color-aware and color-blind modes are supported for child policers.

Junos OS Routing Policies, Firewall Filters, and Traffic Policers User Guide, JUNIPER DOCUMENTATION at 1689 (April 6, 2020) (emphasis added).

102. Juniper has directly infringed and continues to directly infringe the '431 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data

traffic comprising a plurality of micro-flows through a network, including but not limited to the Juniper '431 Products.

103. The Juniper '431 Products are available to businesses and individuals throughout the United States.

104. The Juniper '431 Products are provided to businesses and individuals located in the Western District of Texas.

105. By making, using, testing, offering for sale, and/or selling products and services for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Juniper '431 Products, Juniper has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '431 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

106. Juniper also indirectly infringes the '431 patent by actively inducing infringement under 35 USC § 271(b).

107. Juniper has had knowledge of the '431 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '431 patent and knew of its infringement, including by way of this lawsuit.

108. Alternatively, Juniper has had knowledge of the '431 patent since at least October 11, 2011, based on its citation of the '431 patent as relevant prior art in five patents and patent applications that are assigned to and owned by Juniper. These patents include:

- U.S. Patent No. 8,036,226 (assigned to Juniper and issued on October 11, 2011)
- U.S. Patent No. 9,258,228 (assigned to Juniper and issued on February 9, 2016)
- U.S. Patent No. 9,813,339 (assigned to Juniper and issued on November 7, 2017)
- U.S. Patent No. 10,193,807 (assigned to Juniper and issued on January 29, 2019)
- U.S. Patent Appl. 14/531,260 (assigned to Juniper and published on June 4, 2015)

109. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '431 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products would infringe the '431 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '431 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '431 Products that have the capability of operating in a manner that infringe one or more of the claims of the '431 patent, including at least claim 1, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '431 Products to utilize the products in a manner that directly infringe one or more claims of the '431 patent.[19] By providing instruction and training to customers and end-users on how to use the Juniper '431 Products in a manner that directly infringes one or more claims of the '431 patent, including at least claim 1, Juniper specifically intended to induce infringement of the '431 patent. Juniper engaged in such inducement to promote the sales of the Juniper '431 Products, e.g., through

[19] *See, e.g.*, *ACX6000 Line Of Universal Metro Routers,* JUNIPER DATA SHEET NO. 10006430004-EN (June 2019); *ACX500, ACX1000, ACX2000, and ACX4000 Universal Metro Routers,* JUNIPER DATA SHEET NO. 1000397-015-EN (January 20190); *ACX5000 Line Of Universal Metro Routers,* JUNIPER DATA SHEET NO. 1000644-005-EN (January 2020); *Junos OS Class of Service User Guide (Routers and EX9200 Switches)*, JUNIPER DOCUMENTATION (March 18, 2020); *Junos OS Routing Policies, Firewall Filters, and Traffic Policers User Guide,* JUNIPER DOCUMENTATION (April 6, 2020); *Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices*, JUNIPER DOCUMENTATION (March 25, 2020); *Application-Level Session Tracking and QoS Control,* JUNIPER DOCUMENTATION (June 21, 2019); Guy Davies, *Day One: Deploying Basic QoS*, JUNIPER FUNDAMENTALS SERIES (July 2011); Satish Surapaneni and Dmitry Shokarev, *Juniper 400G Portfolio,* JUNIPER PRESENTATION (2018); and Ragal Jan Szarecki, *Strategies of Packet Buffering Inside Routers*, JUNIPER SOLUTION ARCHITECT PRESENTATION (2015).

Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '431 patent. Accordingly, Juniper has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '431 patent, knowing that such use constitutes infringement of the '431 patent.

110. The '431 patent is well-known within the industry as demonstrated by multiple citations to the '431 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '431 patent without paying a reasonable royalty. Juniper is infringing the '431 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

111. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '431 patent.

112. As a result of Juniper's infringement of the '431 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,977,932

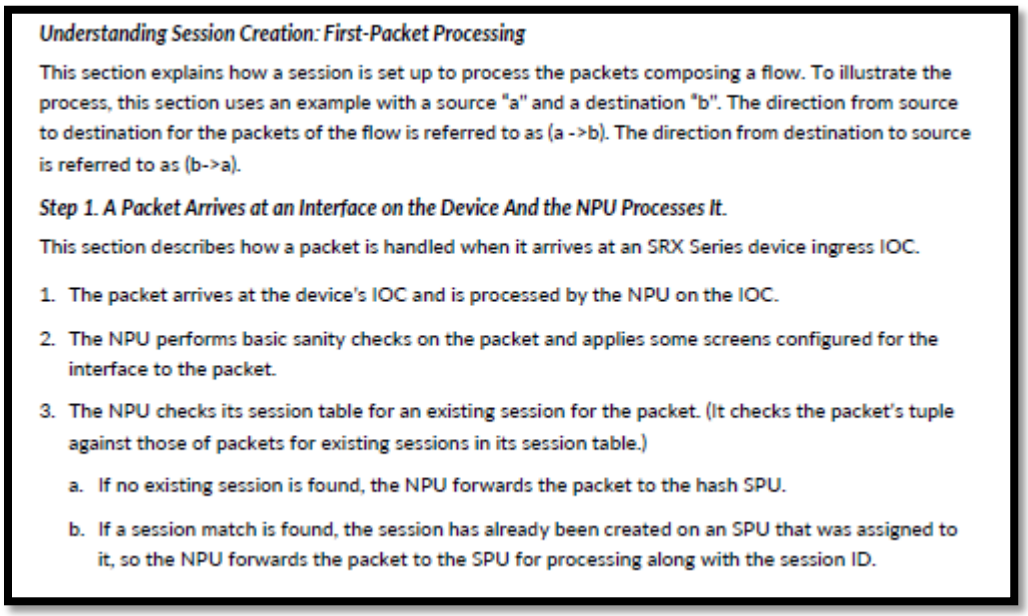
113. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

114. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services utilizing a router capable of network tunneling utilizing flow state information.

115. Juniper designs, makes, sells, offers to sell, imports, and/or uses Juniper devices for utilizing flow state information in network tunneling, including SRX Series devices running Junos OS version 15.1 and later, which include at least the following SRX Series device models: SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 (collectively, the "Juniper '932 Product(s)").

116. One or more Juniper subsidiaries and/or affiliates use the Juniper '932 Products in regular business operations.

117. One or more of the Juniper '932 Products perform the step of creating a flow block having flow state information for a receive first data packet on a micro-flow. Specifically, the flow block (session table) is created when a first packet is received by the Juniper '932 Products based on comparing a 5-tuple hash value against existing hash values that correspond to other micro-flows. The below excerpt from Juniper's documentation describes the creation of the flow block.



Understanding Session Creation: First-Packet Processing

This section explains how a session is set up to process the packets composing a flow. To illustrate the process, this section uses an example with a source "a" and a destination "b". The direction from source to destination for the packets of the flow is referred to as (a ->b). The direction from destination to source is referred to as (b->a).

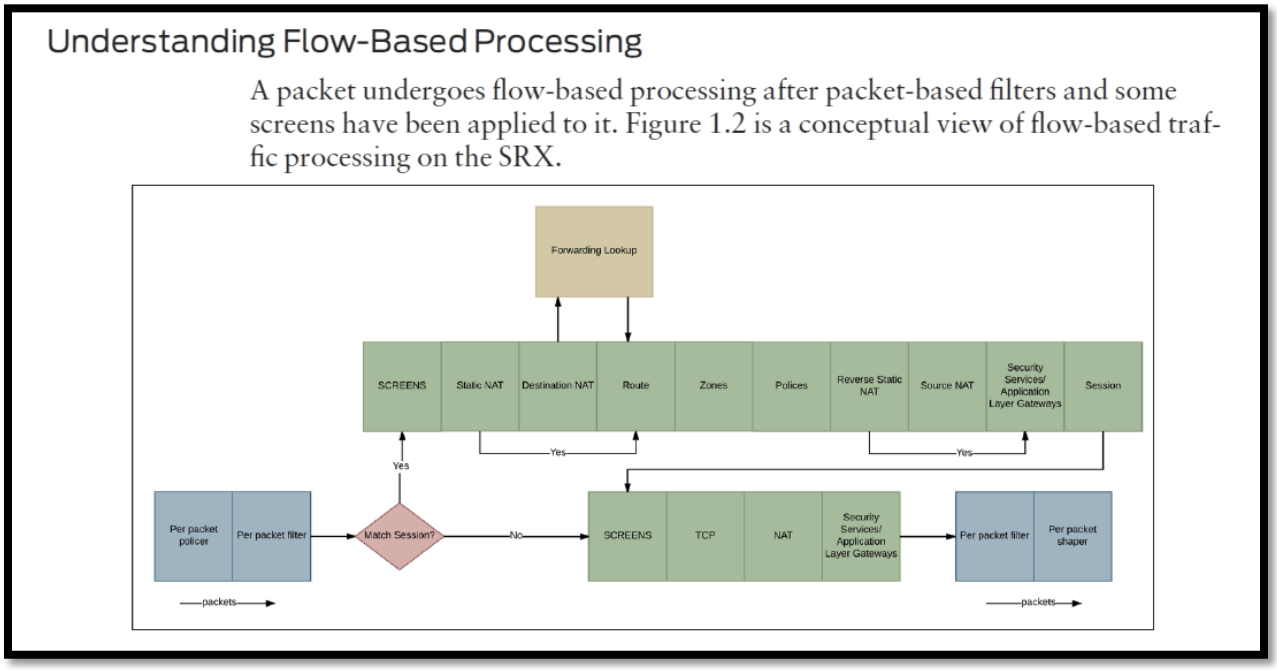
Step 1. A Packet Arrives at an Interface on the Device And the NPU Processes It.

This section describes how a packet is handled when it arrives at an SRX Series device ingress IOC.

1. The packet arrives at the device's IOC and is processed by the NPU on the IOC.
2. The NPU performs basic sanity checks on the packet and applies some screens configured for the interface to the packet.
3. The NPU checks its session table for an existing session for the packet. (It checks the packet's tuple against those of packets for existing sessions in its session table.)
   a. If no existing session is found, the NPU forwards the packet to the hash SPU.
   b. If a session match is found, the session has already been created on an SPU that was assigned to it, so the NPU forwards the packet to the SPU for processing along with the session ID.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 45 (March 25, 2020).

118. The Juniper '932 Products process packets of data that are received using flow-based processing. A flow is a stream of related packets that meet the same matching criteria and share the same characteristics. The Juniper '932 Products treat packets belonging to the same flow in the same manner. To determine if a flow exists for a packet, the Juniper '932 Products attempt to match the packet's information to that of an existing session based on criteria including "source address," "destination address," "source port," "destination port," "protocol," etc. The below excerpt from Juniper documentation shows "flow-based processing" conducted by the Juniper '932 Products.



Alexandre S. Cezar, DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES AT 13 (March 2018).

119. When a first packet is received by the Juniper '932 Products, a flow block is created that has flow state information (flow session entries). The below excerpt shows that the flow block has information including: "session-identifier, source-port, source-prefix and tunnel."

> You can display flow and session information about one or more sessions by specifying a filter as an argument to the **show security flow session** command. You can use the following filters: application, destination-port, destination-prefix, family, idp, interface, nat, protocol, resource-manager, session-identifier, source-port, source-prefix and tunnel. The device displays the information for each session followed by a line specifying the number of sessions reported on. Here is an example of the command using the source-prefix filter.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 191 (March 25, 2020) (emphasis added).

120. The Juniper '932 Products store a tunnel identifier in the session table. The tunnel associated with the micro-flow is associated with a "tunnel ID." The below excerpt from Juniper documentation shows the use of a Tunnel ID that is stored in the session table to identify the tunnel associated with the flow.

Field Name	Field Description
Timeout	Idle timeout after which the session expires.
In	For the input flow: • Source and destination addresses and protocol tuple for the input flow. • **Interface:** Input flow interface. • **Session token:** Internal token derived from the virtual routing instance. • **Flag:** Internal debugging flags. • **Route:** Internal next hop of the route to be used by the flow. • **Gateway:** Next-hop gateway of the flow. • **Tunnel:** If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero). • **Port Sequence, FIN sequence, FIN state, Cookie:** Internal TCP state tracking information.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 661 (March 25, 2020) (emphasis added).

121. The Juniper '932 Products transmit the data packet that is part of the flow using the network tunnel and the associated logical address that is identified in the routing table. The below excerpt from Juniper documentation describes that "packets for the same flow are forwarded onto the same interface" including "VPN tunnels."

multiple paths between routing devices. On Juniper Networks security devices, source and destination IP addresses and protocols are examined to determine individual traffic flows. Packets for the same flow are forwarded on the same interface; the interface does not change when there are additions or changes to the ECMP set. This is important for features such as source NAT, where the translation is performed only during the first path of session establishment for IDP, ALG, and route-based VPN tunnels. If a packet arrives on a given interface in an ECMP set, the security device ensures that reverse traffic is forwarded through the same interface.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 87 (March 25, 2020) (emphasis added).

122. Juniper has directly infringed and continues to directly infringe the '932 patent by, among other things, making, using, offering for sale, and/or selling technology utilizing flow state information to perform a method of network tunneling.

123. One or more of the Juniper '932 Products utilize an aggregate flow block having tunnel specific information for a particular network tunnel. For example, the "Route Table" contains the logical interface address as described in Juniper documentation describing the aggregated flow block.

Table 35: Aggregated Ethernet show interfaces Output Fields *(continued)*

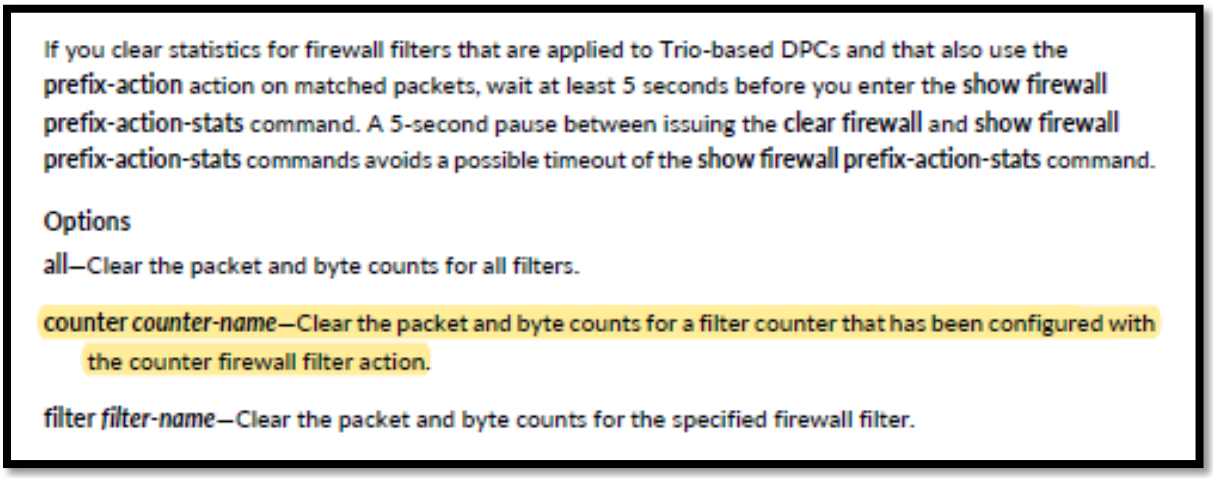
Field Name	Field Description	Level of Output
Protocol	Protocol family configured on the logical interface.	**detail extensive** none
MTU	Maximum transmission unit size on the logical interface.	**detail extensive** none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Route Table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	**detail extensive**

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 520 (March 25, 2020) (emphasis added).

124. One or more of the Juniper '932 Products store a tunnel identifier for the micro-flow in the flow block, the tunnel identifier identifying a selected network tunnel to be used to transmit the data packet.

125. One or more of the Juniper '932 Products index an aggregate flow block using the tunnel identifier.

126. One or more of the Juniper '932 Products utilize an aggregate flow block with tunnel specific information for the selected network tunnel and that stores statistics for the selected network tunnel.



If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the **prefix-action** action on matched packets, wait at least 5 seconds before you enter the **show firewall prefix-action-stats** command. A 5-second pause between issuing the **clear firewall** and **show firewall prefix-action-stats** commands avoids a possible timeout of the **show firewall prefix-action-stats** command.

Options

all—Clear the packet and byte counts for all filters.

counter *counter-name*—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.

filter *filter-name*—Clear the packet and byte counts for the specified firewall filter.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 399 (March 25, 2020) (emphasis added).

127. The Juniper '932 Products are available to businesses and individuals throughout the United States.

128. The Juniper '932 Products are provided to businesses and individuals located in the Western District of Texas.

129. By making, using, testing, offering for sale, and/or selling products utilizing a router capable of network tunneling utilizing flow state information, including but not limited to the Juniper '932 Products, Juniper has injured Plaintiffs and is liable to Plaintiffs for directly

infringing one or more claims of the '932 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

130. Juniper also indirectly infringes the '932 patent by actively inducing infringement under 35 USC § 271(b).

131. Juniper has had knowledge of the '932 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '932 patent and knew of its infringement, including by way of this lawsuit.

132. Alternatively, Juniper has had knowledge of the '932 patent since at least October 12, 2010, based on its citation of the '932 patent as relevant prior art in 17 patents that are assigned to and owned by Juniper. These patents include:

- U.S. Patent No. 7,813,346 (assigned to Juniper and issued on October 12, 2010)
- U.S. Patent No. 8,593,970 (assigned to Juniper and issued on November 26, 2013)
- U.S. Patent No. 8,717,889 (assigned to Juniper and issued on May 6, 2014)
- U.S. Patent No. 8,811,163 (assigned to Juniper and issued on August 19, 2014)
- U.S. Patent No. 8,811,183 (assigned to Juniper and issued on August 19, 2014)
- U.S. Patent No. 8,964,556 (assigned to Juniper and issued on February 24, 2015)
- U.S. Patent No. 9,032,089 (assigned to Juniper and issued on May 12, 2015)
- U.S. Patent No. 9,065,773 (assigned to Juniper and issued on June 23, 2015)
- U.S. Patent No. 9,106,506 (assigned to Juniper and issued on August 11, 2015)
- U.S. Patent No. 9,264,321 (assigned to Juniper and issued on February 16, 2016)
- U.S. Patent No. 9,426,085 (assigned to Juniper and issued on August 23, 2016)
- U.S. Patent No. 9,660,940 (assigned to Juniper and issued on May 23, 2017)
- U.S. Patent No. 9,705,827 (assigned to Juniper and issued on July 11, 2017)
- U.S. Patent No. 9,716,661 (assigned to Juniper and issued on July 25, 2017)
- U.S. Patent No. 9,876,725 (assigned to Juniper and issued on January 23, 2018)
- U.S. Patent No. 9,967,167 (assigned to Juniper and issued on May 8, 2018)
- U.S. Patent No. 10,554,528 (assigned to Juniper and issued on February 4, 2020)

133. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '932 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products

would infringe the '932 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '932 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '932 Products that have the capability of operating in a manner that infringe one or more of the claims of the '932 patent, including at least claim 1, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '932 Products to utilize the products in a manner that directly infringe one or more claims of the '932 patent.[20] By providing instruction and training to customers and end-users on how to use the Juniper '932 Products in a manner that directly infringes one or more claims of the '932 patent, including at least claim 1, Juniper specifically intended to induce infringement of the '932 patent. Juniper engaged in such inducement to promote the sales of the Juniper '932 Products, e.g., through Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '932 patent. Accordingly, Juniper has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '932 patent, knowing that such use constitutes infringement of the '932 patent.

134. The '932 patent is well-known within the industry as demonstrated by multiple citations to the '932 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '932 patent

[20] *See, e.g.*, *Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices*, JUNIPER DOCUMENTATION (March 25, 2020); *Junos OS Routing Policies, Firewall Filters, and Traffic Policers User Guide*, JUNIPER DOCUMENTATION (April 6, 2020); *Junos OS MPLA Applications User Guide,* JUNIPER DOCUMENTATION (March 30, 2020); Alexandre S. Cezar, DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES (Mar. 2018); *QoS Configuration for SRX Series for the Branch with Integrated Convergence Services*, JUNIPER NETWORKS APPLICATION NOTE (Nov. 2010); and JUNIPER ADVANCED THREAT PREVENTION APPLIANCE INTEGRATION WITH THE SRX SERIES DEVICE (Jan. 19, 2020).

without paying a reasonable royalty. Juniper is infringing the '932 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

135. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '932 patent.

136. As a result of Juniper's infringement of the '932 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,630,358

137. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

138. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing multiple logical routers within a single physical router.

139. Juniper designs, makes, sells, offers to sell, imports, and/or uses Junos OS Release 14.1 and later running on an MX Series Router and Junos OS Release 15.1 and later running on EX9200 switches (collectively, the "Juniper '358 Products").

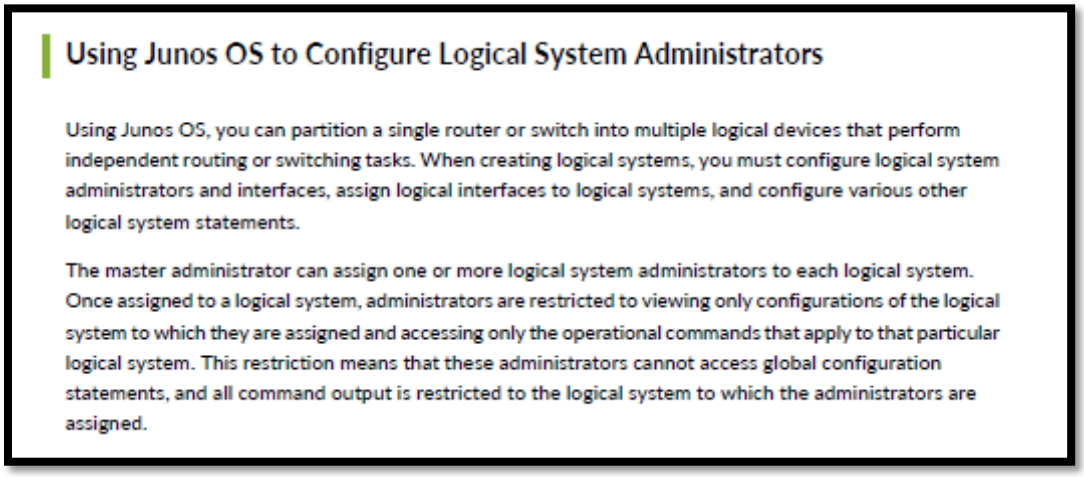
140. One or more Juniper subsidiaries and/or affiliates use the Juniper '358 Products in regular business operations.

141. One or more of the Juniper '358 Products include technology for implementing multiple logical routers within a single physical router. Specifically, the Juniper '358 Products are routers that contain the logical systems feature wherein one or more logical routers can be configured on the device.

System Virtualization	Enhanced SLA and queuing	✓
	Junos Fusion Edge (AD)	✓
	Logical systems	✓
	Virtual router/switch	✓
	Path Computation Element Protocol (PCEP)	✓
	OpenConfig	✓
	YANG data modeling	✓
	Juniper Extension Toolkit	✓

MX Series 5G Universal Routing Platforms, JUNIPER DOCUMENTATION AT 5 (February 2020) (emphasis added).

142. One or more of the Juniper '358 Products include a router with a first set of one or more components capable of being figured to implement a first logical router within the router. Specifically, Juniper documentation states, "using Junos OS, you can partition a single router or switch into multiple logical devices that perform independent routing or switching tasks."



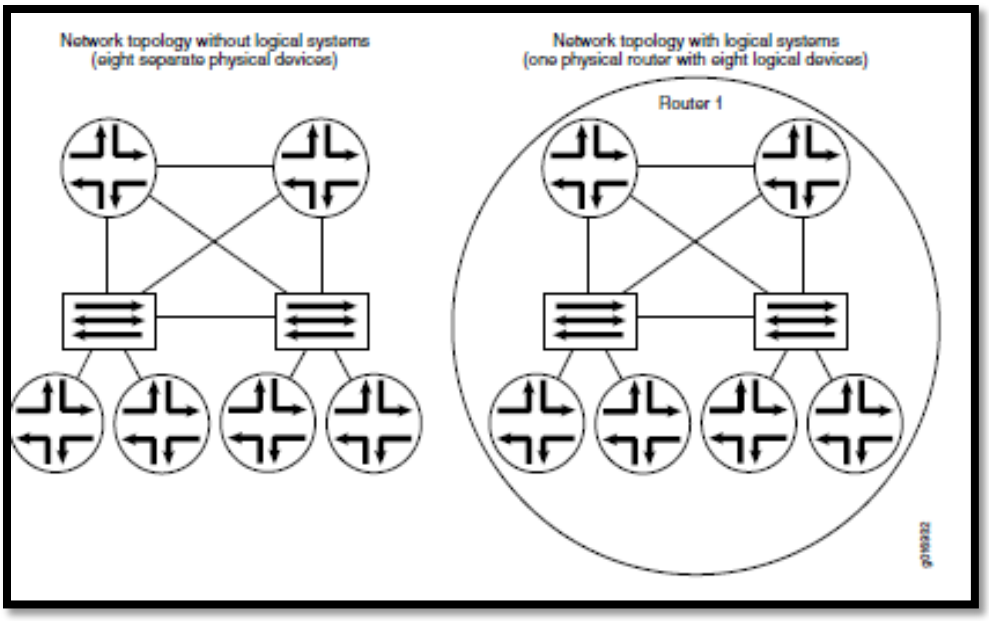
Using Junos OS to Configure Logical System Administrators

Using Junos OS, you can partition a single router or switch into multiple logical devices that perform independent routing or switching tasks. When creating logical systems, you must configure logical system administrators and interfaces, assign logical interfaces to logical systems, and configure various other logical system statements.

The master administrator can assign one or more logical system administrators to each logical system. Once assigned to a logical system, administrators are restricted to viewing only configurations of the logical system to which they are assigned and accessing only the operational commands that apply to that particular logical system. This restriction means that these administrators cannot access global configuration statements, and all command output is restricted to the logical system to which the administrators are assigned.

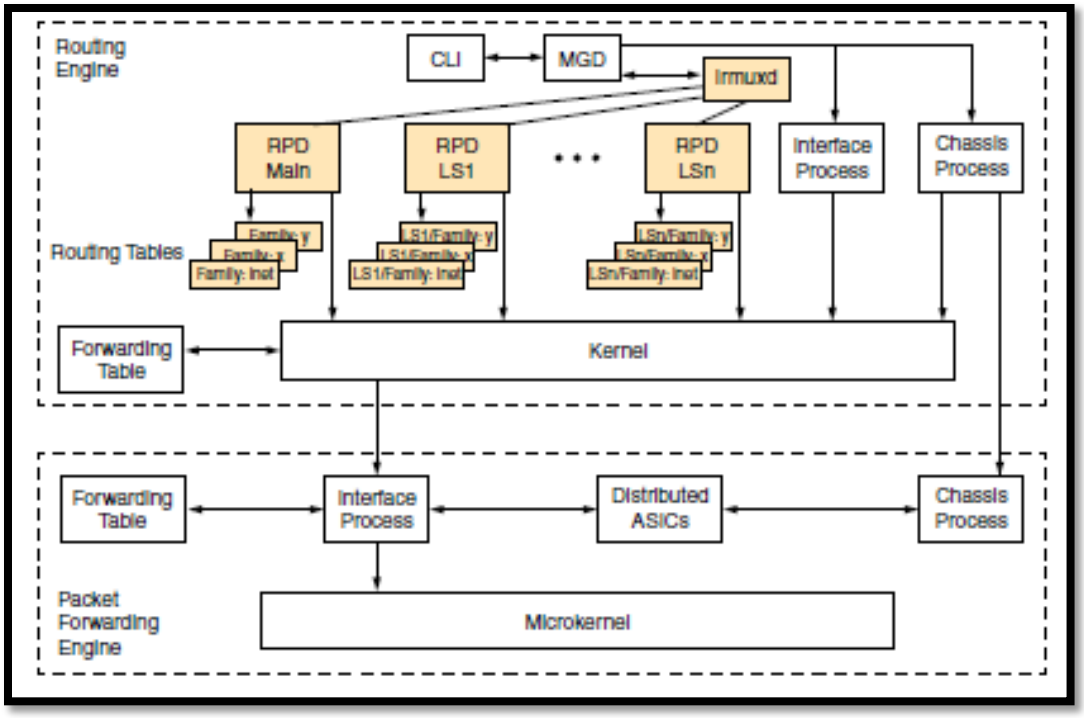
Junos OS Logical Systems User Guide for Routers and Switches, JUNIPER DOCUMENTATION AT 30 (March 27, 2020).

143. One or more of the Juniper '358 Products include a router with a second set of one or more components capable of being configured to implement a second logical router within the router. For example, the Juniper '358 Products enable the setting up of a second (or more) logical router that is located within the same physical device. The below excerpt shows a Juniper '358 Product where a first and second logical router can be setup within the same device.



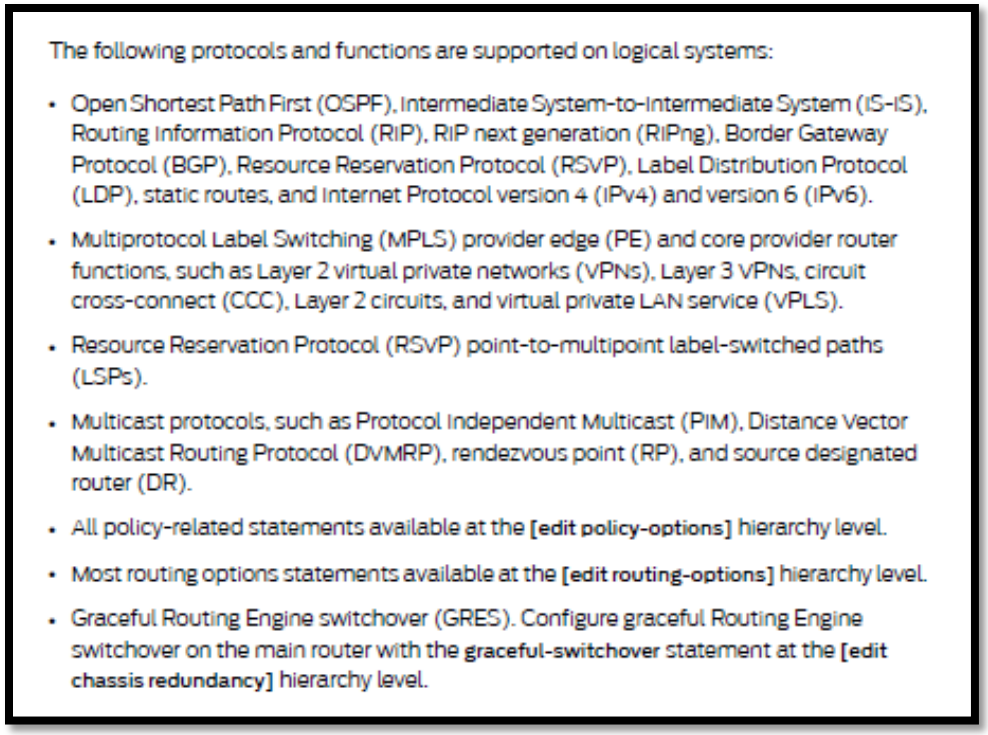
Junos OS Logical Systems User Guide for Routers and Switches, JUNIPER DOCUMENTATION AT 17 (March 27, 2020).

144. One or more of the Juniper '358 Products include a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link. The below excerpt from Juniper documentation shows the Forwarding Table for the Juniper '358 Products in which a forwarding table is created for the LS1 and LSN logical routers.



Junos OS Logical Systems Configuration Guide Release 12.3, JUNIPER DOCUMENTATION at 5 (2012).

145. The forwarding table in the Juniper '358 Products contains functionality wherein the links in the forwarding table are identified as being local links (links within the physical router to other logical routers) and external links that link to devices outside of the physical router containing the logical routers.



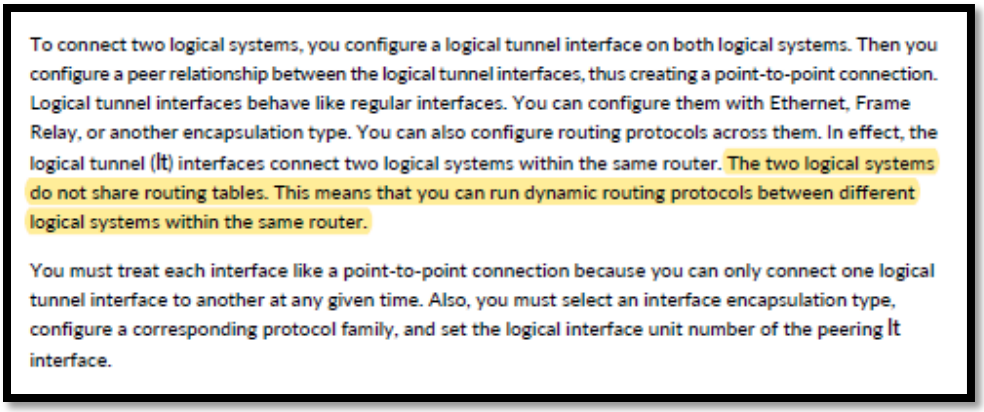
The following protocols and functions are supported on logical systems:

- Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), RIP next generation (RIPng), Border Gateway Protocol (BGP), Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP), static routes, and Internet Protocol version 4 (IPv4) and version 6 (IPv6).
- Multiprotocol Label Switching (MPLS) provider edge (PE) and core provider router functions, such as Layer 2 virtual private networks (VPNs), Layer 3 VPNs, circuit cross-connect (CCC), Layer 2 circuits, and virtual private LAN service (VPLS).
- Resource Reservation Protocol (RSVP) point-to-multipoint label-switched paths (LSPs).
- Multicast protocols, such as Protocol Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), rendezvous point (RP), and source designated router (DR).
- All policy-related statements available at the **[edit policy-options]** hierarchy level.
- Most routing options statements available at the **[edit routing-options]** hierarchy level.
- Graceful Routing Engine switchover (GRES). Configure graceful Routing Engine switchover on the main router with the **graceful-switchover** statement at the **[edit chassis redundancy]** hierarchy level.

Junos OS Logical Systems Configuration Guide Release 12.3, JUNIPER DOCUMENTATION at 5 (2012).

146. One or more of the Juniper '358 Products include a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

147. The Juniper '358 Products support creating a link between a first and second logical router and advertising the links to these interconnected routers as standalone routers.



To connect two logical systems, you configure a logical tunnel interface on both logical systems. Then you configure a peer relationship between the logical tunnel interfaces, thus creating a point-to-point connection. Logical tunnel interfaces behave like regular interfaces. You can configure them with Ethernet, Frame Relay, or another encapsulation type. You can also configure routing protocols across them. In effect, the logical tunnel (lt) interfaces connect two logical systems within the same router. The two logical systems do not share routing tables. This means that you can run dynamic routing protocols between different logical systems within the same router.

You must treat each interface like a point-to-point connection because you can only connect one logical tunnel interface to another at any given time. Also, you must select an interface encapsulation type, configure a corresponding protocol family, and set the logical interface unit number of the peering lt interface.

Junos OS Logical Systems User Guide for Routers and Switches, JUNIPER DOCUMENTATION AT 39 (March 27, 2020) (emphasis added).

148. The Juniper '358 Products are available to businesses and individuals throughout the United States.

149. The Juniper '358 Products are provided to businesses and individuals located in the Western District of Texas.

150. Juniper has directly infringed and continues to directly infringe the '358 patent by, among other things, making, using, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Juniper '358 Products.

151. By making, using, testing, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Juniper '358 Products, Juniper has injured Plaintiffs and is liable for directly infringing one or more claims of the '358 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

152. Juniper also indirectly infringes the '358 patent by actively inducing infringement under 35 USC § 271(b).

153. Juniper has had knowledge of the '358 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '358 patent and knew of its infringement, including by way of this lawsuit.

154. Alternatively, Juniper has had knowledge of the '358 patent since at least November 2, 2010, based on its citation of the '358 patent as relevant prior art in seven patents that are assigned to and owned by Juniper. These patents include:

- U.S. Patent No. 7,826,375 (assigned to Juniper and issued on November 2, 2010)
- U.S. Patent No. 8,069,023 (assigned to Juniper and issued on November 29, 2011)
- U.S. Patent No. 8,254,270 (assigned to Juniper and issued on August 28, 2012)
- U.S. Patent No. 8,867,408 (assigned to Juniper and issued on October 21, 2014)
- U.S. Patent No. 9,444,768 (assigned to Juniper and issued on September 13, 2016)
- U.S. Patent No. 9,485,149 (assigned to Juniper and issued on November 1, 2016)
- U.S. Patent No. 9,832,099 (assigned to Juniper and issued on November 28, 2017)

155. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '358 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products would infringe the '358 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '358 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '358 Products that have the capability of operating in a manner that infringe one or more of the claims of the '358 patent, including at least claim 1, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '358 Products to utilize the products in a manner that directly infringe one or more claims of the '358 patent.[21] By

[21] *See, e.g.*, *Junos OS Logical Systems and Tenant Systems User Guide for Security Devices*, JUNIPER DOCUMENTATION (March 24, 2020); *Junos OS Logical Systems Configuration Guide Release 12.3*, JUNIPER DOCUMENTATION (December 10, 2012); *Junos OS Logical Systems User Guide for Routers and Switches*, JUNIPER DOCUMENTATION (March 27, 2020); *EX9200 Ethernet*

providing instruction and training to customers and end-users on how to use the Juniper '358 Products in a manner that directly infringes one or more claims of the '358 patent, including at least claim 1, Juniper specifically intended to induce infringement of the '358 patent. Juniper engaged in such inducement to promote the sales of the Juniper '358 Products, e.g., through Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '358 patent. Accordingly, Juniper has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '358 patent, knowing that such use constitutes infringement of the '358 patent.

156. The '358 patent is well-known within the industry as demonstrated by multiple citations to the '358 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '358 patent without paying a reasonable royalty. Juniper is infringing the '358 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

157. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '358 patent.

Switch Data Sheet, JUNIPER DOCUMENTATION (December 2019); *MX2000 Universal Routing Platforms,* JUNIPER DOCUMENTATION (January 2020); *Junos OS Interfaces Fundamentals for Routing Devices,* JUNIPER DOCUMENTATION (March 23, 2020); Matt Dinham, *Day One: vMX Up and Running,* JUNIPER DOCUMENTATION (2016); and *MX Series 5G Universal Routing Platforms,* JUNIPER DOCUMENTATION (February 2020); Steven Wong, DDOS IMPLEMENTATION ON MX PLATFORM (May 2, 2014); Eric Sandoval, *MX Edge Security Solution for Cloud, Mobility & Wireline Providers*, NXTWORK 2017 JUNIPER CUSTOMER SUMMIT; *Frequently Asked Questions: MX Series 3D Universal Edge Routers Quality of Service*, JUNIPER NETWORKS TECHNOLOGY OVERVIEW RELEASE 11.2 (April 21, 2011); Pepe (Joseph) Garcia, *Juniper's MX 3D Product Overview Next Generation Access* (May 2010); *MX Series Overview and Roadmap* (April 1, 2014); Dmitry Shokarev, *MX Trio Load Balancing*, v. 1.4 (April 2014); *EX9200 Ethernet Switch*, JUNIPER NETWORKS DATASHEET, 1000430-017-EN (Dec. 2019); and *Junos OS Class of Service User Guide (Routers and EX9200 Switches)* (March 18, 2020).

158. As a result of Juniper's infringement of the '358 patent, Plaintiffs have suffered monetary damages, and seeks recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 8,085,775

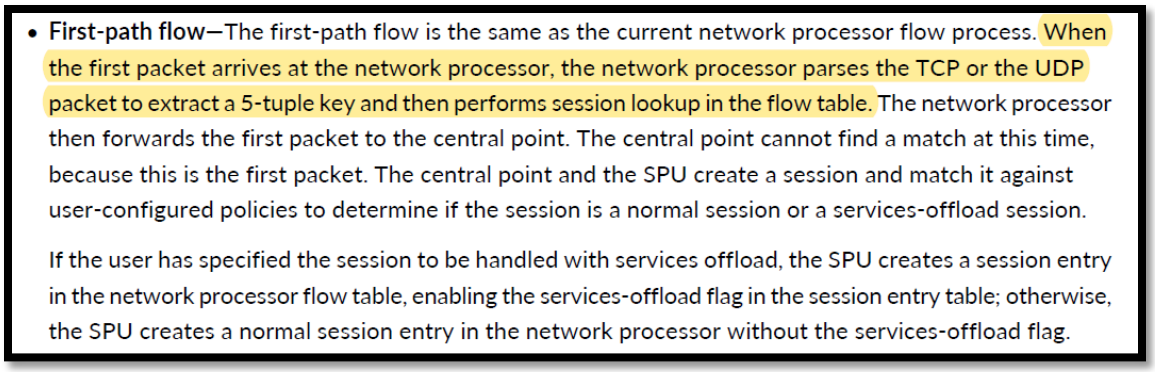
159. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

160. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for identifying and handling a single application flow of a plurality of information packets.

161. Juniper designs, makes, sells, offers to sell, imports, and/or uses Juniper devices that enable the identification of a flow based on the behavior of the flow, including the NFX150 and SRX300, SRX320, SRX340, SRX345, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices with Junos OS 18.2 Release 1 and later installed; SRX380 devices with Junos OS 20.1 Release 1 and later installed; and vSRX devices with vSRX 12.1X46-D10 and later installed (collectively, the "Juniper '775 Products(s)").

162. One or more Juniper subsidiaries and/or affiliates use the Juniper '775 Products in regular business operations.

163. One or more of the Juniper '775 Products include technology for identifying and handling a single application flow of a plurality of information packets. Specifically, the Juniper '775 Products perform the step of creating a flow block as the first packet of a flow is processed by a router.



- **First-path flow**—The first-path flow is the same as the current network processor flow process. When the first packet arrives at the network processor, the network processor parses the TCP or the UDP packet to extract a 5-tuple key and then performs session lookup in the flow table. The network processor then forwards the first packet to the central point. The central point cannot find a match at this time, because this is the first packet. The central point and the SPU create a session and match it against user-configured policies to determine if the session is a normal session or a services-offload session.

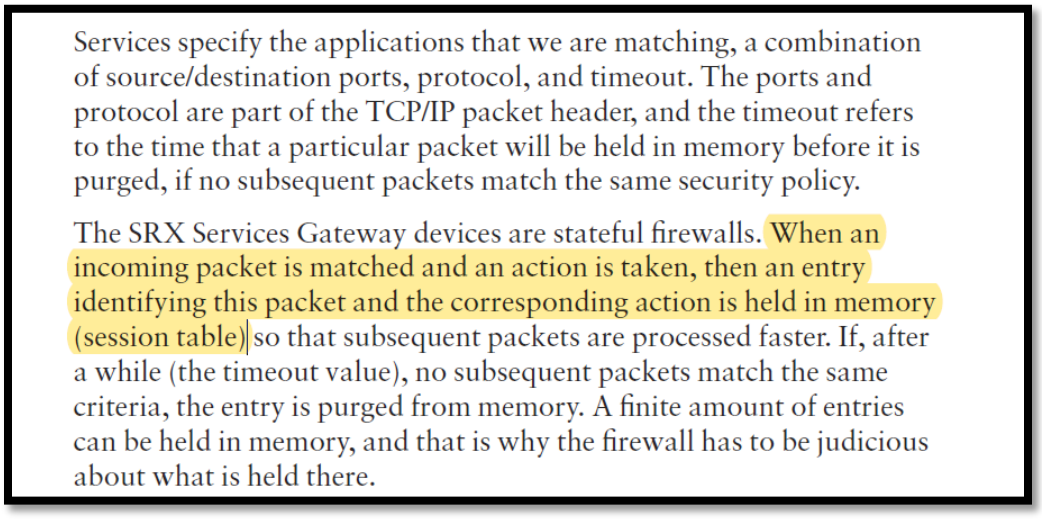
  If the user has specified the session to be handled with services offload, the SPU creates a session entry in the network processor flow table, enabling the services-offload flag in the session entry table; otherwise, the SPU creates a normal session entry in the network processor without the services-offload flag.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 265 (March 25, 2020) (emphasis added).

164. Juniper has directly infringed and continues to directly infringe the '775 patent by, among other things, making, using, offering for sale, and/or selling technology for identifying and handling a single application flow of a plurality of information packets, including but not limited to the Juniper '775 Products.

165. One or more of the Juniper '775 Products creates a flow block as the first packet of a flow is processed by a router.

166. The Flow information is stored in a flow block or session table that contains statistics about the flow that are updated as each packet in the flow is categorized.



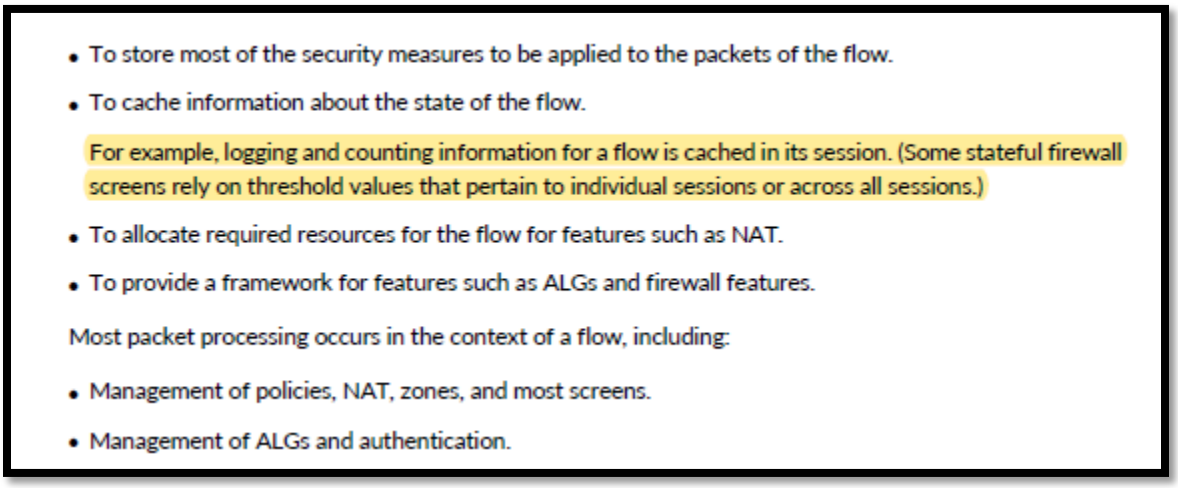
Services specify the applications that we are matching, a combination of source/destination ports, protocol, and timeout. The ports and protocol are part of the TCP/IP packet header, and the timeout refers to the time that a particular packet will be held in memory before it is purged, if no subsequent packets match the same security policy.

The SRX Services Gateway devices are stateful firewalls. When an incoming packet is matched and an action is taken, then an entry identifying this packet and the corresponding action is held in memory (session table) so that subsequent packets are processed faster. If, after a while (the timeout value), no subsequent packets match the same criteria, the entry is purged from memory. A finite amount of entries can be held in memory, and that is why the firewall has to be judicious about what is held there.

Barny Sanchez, *Day One: Deploying SRX Series Services Gateway*, JUNOS DYNAMIC SERVICES SERIES at 58 (2011) (emphasis added).

167. One or more of the Juniper '775 Products utilize a flow block adapted to store payload-content agnostic behavioral statistics about the flow.

168. One or more of the Juniper '775 Products update the flow block with the flow's payload-content agnostic behavioral statistics as packets belonging to the flow are processed by the router. This information includes the number of packets received, the size of the packet received for a flow, etc. Juniper documentation states that the Juniper '775 Products perform flow-based packet processing "which is stateful, requires the creation of Sessions" and includes logging and counting information (statistics) for each flow.



- To store most of the security measures to be applied to the packets of the flow.
- To cache information about the state of the flow.

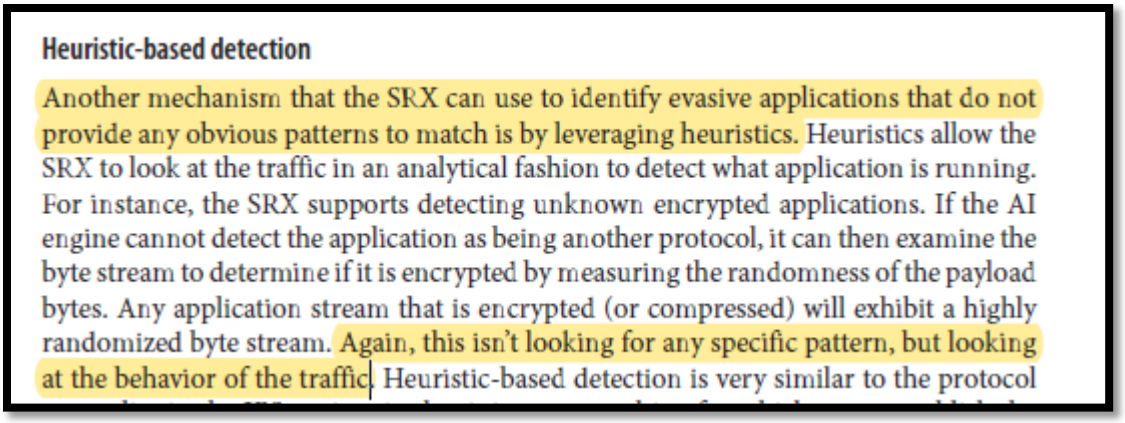
  For example, logging and counting information for a flow is cached in its session. (Some stateful firewall screens rely on threshold values that pertain to individual sessions or across all sessions.)
- To allocate required resources for the flow for features such as NAT.
- To provide a framework for features such as ALGs and firewall features.

Most packet processing occurs in the context of a flow, including:

- Management of policies, NAT, zones, and most screens.
- Management of ALGs and authentication.

Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 27 (March 25, 2020) (emphasis added).

169. One or more of the Juniper '775 Products utilize a flow incapable of being identified by header information alone. For example, the Juniper '775 Products support the creation of a flow block and tracking of statistics relating to a flow where the flow cannot be identified by the header data.

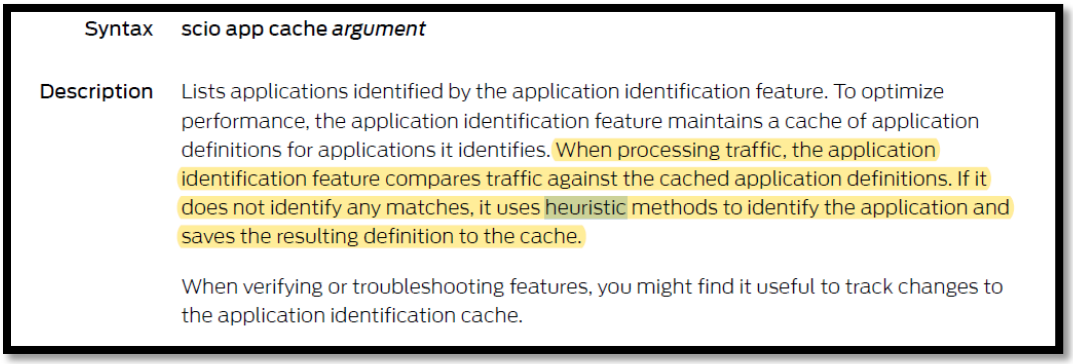


Heuristic-based detection

Another mechanism that the SRX can use to identify evasive applications that do not provide any obvious patterns to match is by leveraging heuristics. Heuristics allow the SRX to look at the traffic in an analytical fashion to detect what application is running. For instance, the SRX supports detecting unknown encrypted applications. If the AI engine cannot detect the application as being another protocol, it can then examine the byte stream to determine if it is encrypted by measuring the randomness of the payload bytes. Any application stream that is encrypted (or compressed) will exhibit a highly randomized byte stream. Again, this isn't looking for any specific pattern, but looking at the behavior of the traffic. Heuristic-based detection is very similar to the protocol

Brad Woodberg and Rob Cameron, JUNIPER SRX SERIES: A COMPREHENSIVE GUIDE TO SECURITY SERVICES ON SRX SERIES at 705 (2013) (emphasis added).

170. One or more of the Juniper '775 Products heuristically determine whether at least one user-specified policy is satisfied by the payload-content agnostic behavioral statistics stored in the flow block. For example, the following documentation from Juniper shows the use of heuristic methods to identify a flow based on the behavior of the flow.

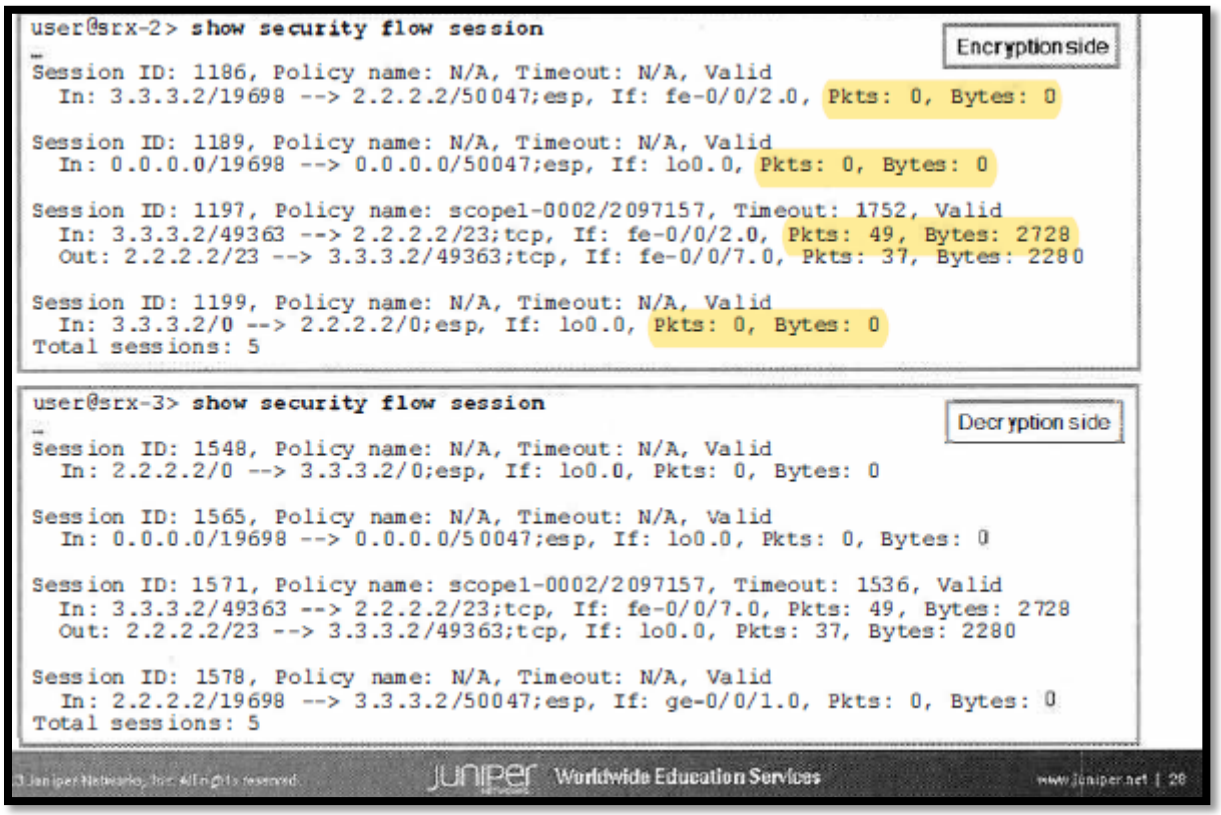


Syntax	scio app cache *argument*
Description	Lists applications identified by the application identification feature. To optimize performance, the application identification feature maintains a cache of application definitions for applications it identifies. When processing traffic, the application identification feature compares traffic against the cached application definitions. If it does not identify any matches, it uses heuristic methods to identify the application and saves the resulting definition to the cache. When verifying or troubleshooting features, you might find it useful to track changes to the application identification cache.

Juniper IDP Series Administration Guide Release 5.1rX, JUNIPER DOCUMENTATION at 327 (December 19, 2013) (emphasis added).

171. One or more of the Juniper '775 Products apply to at least one packet belonging to at least one user-specified action that is mapped to the user-specified policy that is satisfied by the payload-content agnostic behavioral statistics upon determining that the user-specified policy is satisfied by the payload-content agnostic behavioral statistics.

172. One or more of the Juniper '775 Products include functionality wherein the payload-content agnostic behavioral statistics for the flow are calculated by the router. For example, the payload content agnostic behavioral statistics that are calculated by the Juniper '775 Products when a packet is ingested include the total byte count accumulated for a flow as shown in the below excerpt from Juniper documentation.



Advanced Junos Security Version 12.b Student Guide Vol. 1, JUNIPER COURSE MATERIALS EDU-JUN-AJSEC at Chapter 7-28 (June 2013) (emphasis added).

173. One or more of the Juniper '775 Products include functionality wherein the payload-content agnostic behavioral statistics reflect the empirical behavior of the flow. For example, statistics calculated by the Juniper '775 Products include the duration of the flow as shown in the below excerpt from Juniper documentation.

```
user@host> show security flow session application-traffic-control extensive
  Session ID: 3729, Status: Normal, State: Active
  Flag: 0x40
  Policy name: p1
  Source NAT pool: Null
  Dynamic application: junos:FTP
  Application traffic control rule-set: ftp-test1, Rule: rule0
  Maximum timeout: 300, Current timeout: 276
  Session State: Valid
  Start time: 18292, Duration: 603536
     In: 192.0.2.1/1 --> 203.0.113.0/1;pim,
      Interface: reth1.0,
      Session token: 0x1c0, Flag: 0x0x21
      Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
      Port sequence: 0, FIN sequence: 0,
      FIN state: 0,
      Pkts: 21043, Bytes: 1136322
    Out: 203.0.113.0/1 --> 192.0.2.0/1;pim,
      Interface: .local..0,
      Session token: 0x80, Flag: 0x0x30
```

Junos OS Application Security User Guide For Security Devices, JUNIPER DOCUMENTATION at 194 (March 18, 2020) (emphasis added).

174. One or more of the Juniper '775 Products include functionality wherein at least one of the payload-content agnostic behavioral statistics is chosen from the group consisting of: (1) total byte count accumulated for the flow, (2) flow life duration, (3) average rate of flow, (4) average packet size, (5) average packet rate, (6) average inter-packet gap, (7) instantaneous flow rate, and (8) moving average flow rate.

175. The Juniper '775 Products are available to businesses and individuals throughout the United States.

176. The Juniper '775 Products are provided to businesses and individuals located in the Western District of Texas.

177. By making, using, testing, offering for sale, and/or selling products and services for identifying and handling a single application flow of a plurality of information packets, including

but not limited to the Juniper '775 Products, Juniper has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '775 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

178. Juniper also indirectly infringes the '775 patent by actively inducing infringement under 35 USC § 271(b).

179. Juniper has had knowledge of the '775 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '775 patent and knew of its infringement, including by way of this lawsuit.

180. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '775 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products would infringe the '775 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '775 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '775 Products that have the capability of operating in a manner that infringe one or more of the claims of the '775 patent, including at least claim 1, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '775 Products to utilize the products in a manner that directly infringe one or more claims of the '775 patent.[22] By

[22] *See, e.g.*, *Juniper vSRX – Technical Overview for X47D20*, JUNIPER PRESENTATION (2015); *Junos OS Application Security User Guide For Security Devices,* JUNIPER DOCUMENTATION (March 18, 2020); *Advanced Junos Security Version 12.b Student Guide Vol. 1*, JUNIPER COURSE MATERIALS EDU-JUN-AJSEC (June 2013); *Learn About Application Visibility and Control*, JUNIPER NETWORKS DOCUMENTATION (September 2016); *Juniper IDP Series Administration Guide Release 5.1rX*, JUNIPER DOCUMENTATION (December 19, 2013); *Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices,* JUNIPER DOCUMENTATION (March 25, 2020); Alexandre S. Cezar, DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES (Mar. 2018); *QoS Configuration for SRX Series*

providing instruction and training to customers and end-users on how to use the Juniper '775 Products in a manner that directly infringes one or more claims of the '775 patent, including at least claim 1, Juniper specifically intended to induce infringement of the '775 patent. Juniper engaged in such inducement to promote the sales of the Juniper '775 Products, e.g., through Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '775 patent. Accordingly, Juniper has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '775 patent, knowing that such use constitutes infringement of the '775 patent.

181. The '775 patent is well-known within the industry as demonstrated by multiple citations to the '775 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '775 patent without paying a reasonable royalty. Juniper is infringing the '775 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

182. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '775 patent.

183. As a result of Juniper's infringement of the '775 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

---

for the Branch with Integrated Convergence Services, JUNIPER NETWORKS APPLICATION NOTE (Nov. 2010); and JUNIPER ADVANCED THREAT PREVENTION APPLIANCE INTEGRATION WITH THE SRX SERIES DEVICE (Jan. 19, 2020).

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,243,593

184. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

185. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

186. Juniper designs, makes, sells, offers to sell, imports, and/or uses Juniper security devices that enable the identification and penalization of data flows based on the behavior of the data flow, including the Juniper SRX5400, SRX5600, and SRX5800 Series devices (collectively, the "Juniper '593 Products(s)").

187. One or more Juniper subsidiaries and/or affiliates use the Juniper '593 Products in regular business operations.

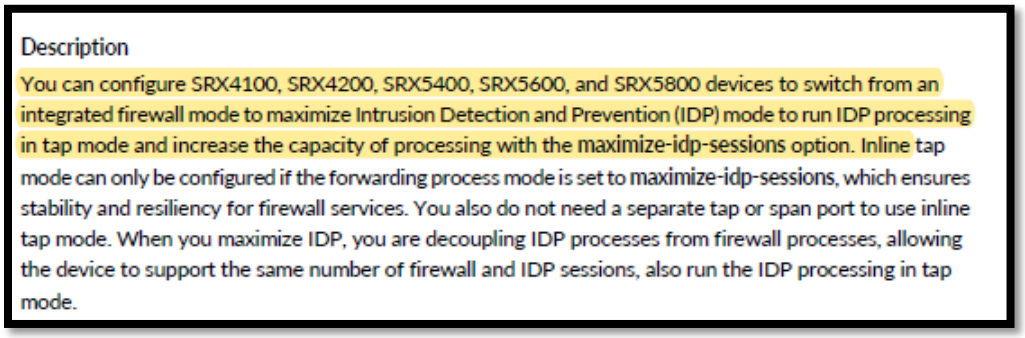
188. One or more of the Juniper '593 Products include technology for processing a flow of a series of information packets. Specifically, the Juniper '593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

189. The Juniper '593 Products are available to businesses and individuals throughout the United States.

190. The Juniper '593 Products are provided to businesses and individuals located in the Western District of Texas.

191. Juniper has directly infringed and continues to directly infringe the '593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

192. The Juniper '593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

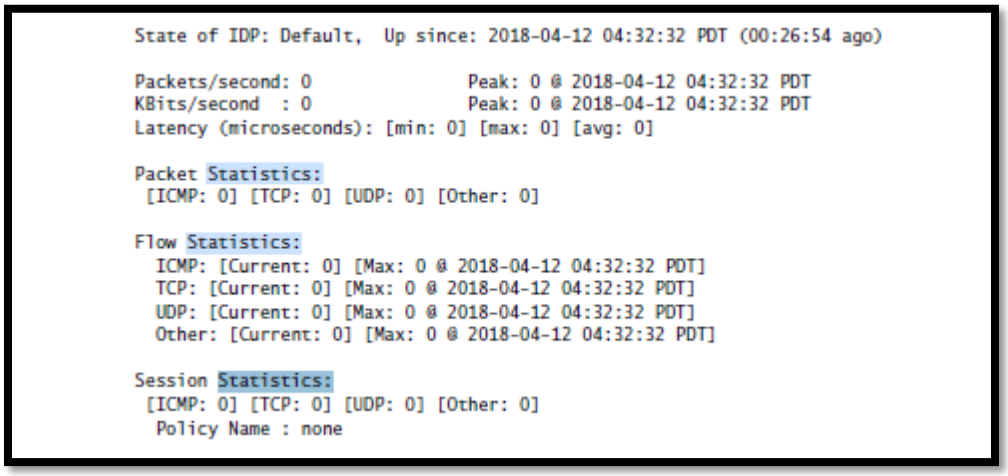


Description

You can configure SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices to switch from an integrated firewall mode to maximize Intrusion Detection and Prevention (IDP) mode to run IDP processing in tap mode and increase the capacity of processing with the maximize-idp-sessions option. Inline tap mode can only be configured if the forwarding process mode is set to maximize-idp-sessions, which ensures stability and resiliency for firewall services. You also do not need a separate tap or span port to use inline tap mode. When you maximize IDP, you are decoupling IDP processes from firewall processes, allowing the device to support the same number of firewall and IDP sessions, also run the IDP processing in tap mode.

Junos OS Flow-Based And Packet-Based Processing User Guide For Security Devices, JUNIPER DOCUMENTATION at 299 (March 25, 2020) (emphasis added).

193. The Juniper '593 Products enable the generation of behavioral statistics based on each packet that is processed.



```
State of IDP: Default,  Up since: 2018-04-12 04:32:32 PDT (00:26:54 ago)

Packets/second: 0               Peak: 0 @ 2018-04-12 04:32:32 PDT
KBits/second  : 0               Peak: 0 @ 2018-04-12 04:32:32 PDT
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2018-04-12 04:32:32 PDT]
  TCP: [Current: 0] [Max: 0 @ 2018-04-12 04:32:32 PDT]
  UDP: [Current: 0] [Max: 0 @ 2018-04-12 04:32:32 PDT]
  Other: [Current: 0] [Max: 0 @ 2018-04-12 04:32:32 PDT]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]
  Policy Name : none
```

Junos OS Intrusion Detection And Prevention Feature Guide For Security Devices, JUNIPER DOCUMENTATION at 208 (June 18, 2018) (emphasis added).

194. The Juniper '593 Products determine, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

Field Name	Field Description
State of IDP	Status of current IDP policy.
Packets/second	The aggregated throughput (packets per second) for the system.
KBits/second	The aggregated throughput (kilobits per second) for the system.
Latency	• min—Minimum delay for a packet to receive and return by a node in microseconds. • max—Maximum delay for a packet to receive and return by a node in microseconds. • ave—Average delay for a packet to receive and return by a node in microseconds.
Packet Statistics	Statistics for ICMP, TCP, and UDP packets.
Flow Statistics	Flow-related system statistics for ICMP, TCP, and UDP packets.
Session Statistics	Session-related system statistics for ICMP, TCP, and UDP packets.
Number of SSL Sessions	Number of current SSL sessions.
Policy Name	Name of the running policy. If IDP is configured for logical systems, idp-policy-combined is displayed.

Junos OS Intrusion Detection And Prevention Feature Guide For Security Devices, JUNIPER DOCUMENTATION at 594 (June 18, 2018) (emphasis added).

195. The Juniper '593 Products determine whether the flow is exhibiting undesirable behavior regardless of the presence or absence of congestion.

Understanding Predefined IDP Policy Templates

Predefined policy templates are available in the templates.xls file on a secured Juniper Networks website. To start using a template, you run a command from the CLI to download and copy this file to a /var/db/scripts/commit directory.

Each policy template contains rules that use the default actions associated with the attack objects. You should customize these templates to work on your network by selecting your own source and destination addresses and choosing IDP actions that reflect your security needs.

The client/server templates are designed for ease of use and provide balanced performance and coverage. The client/server templates include client protection, server protection, and client/server protection.

Juniper OS Intrusion Detection and Prevention User Guide, JUNIPER DOCUMENTATION AT 89 (April 24, 2020) (emphasis added).

196. The Juniper '593 Products enforce a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

197. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the Juniper '593 Products, Juniper has injured Plaintiffs and is liable for directly infringing one or more claims of the '593 patent, including at least claim 4, pursuant to 35 U.S.C. § 271(a).

198. Juniper also indirectly infringes the '593 patent by actively inducing infringement under 35 USC § 271(b).

199. Juniper has had knowledge of the '593 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '593 patent and knew of its infringement, including by way of this lawsuit.

200. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products would infringe the '593 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '593 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '593 Products that have the capability of operating in a manner that infringe one or more of the claims of the '593 patent, including at least claim 4, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '593 Products to utilize the products in a manner that directly infringe one or more claims of the '593 patent.[23] By

[23] *See, e.g.*, *Juniper OS Intrusion Detection and Prevention User Guide*, JUNIPER DOCUMENTATION (April 24, 2020); Keerthi Latha, *Learn About Intrusion Detection and Prevention,* JUNIPER DOCUMENTATION (2016); *Junos OS Flow-Based And Packet-Based Processing User Guide For Security Devices*, JUNIPER DOCUMENTATION (March 25, 2020); *Juniper Sky Advanced Threat Prevention CLI Reference Guide*, JUNIPER DOCUMENTATION (March 29, 2020); *Junos OS Intrusion Detection And Prevention Feature Guide For Security*

providing instruction and training to customers and end-users on how to use the Juniper '593 Products in a manner that directly infringes one or more claims of the '593 patent, including at least claim 4, Juniper specifically intended to induce infringement of the '593 patent. Juniper engaged in such inducement to promote the sales of the Juniper '593 Products, e.g., through Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '593 patent. Accordingly, Juniper has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '593 patent, knowing that such use constitutes infringement of the '593 patent.

201. The '593 patent is well-known within the industry as demonstrated by multiple citations to the '593 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '593 patent without paying a reasonable royalty. Juniper is infringing the '593 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

202. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '593 patent.

203. As a result of Juniper's infringement of the '593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Juniper's

Devices, JUNIPER DOCUMENTATION (June 18, 2018); *Juniper vSRX Technical Overview for X47D20 Release*, JUNIPER PRESENTATION at 23 (2015); Alexandre S. Cezar, DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES (March 2018); and JUNIPER ADVANCED THREAT PREVENTION APPLIANCE INTEGRATION WITH THE SRX SERIES DEVICE (January 19, 2020).

infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,817,790

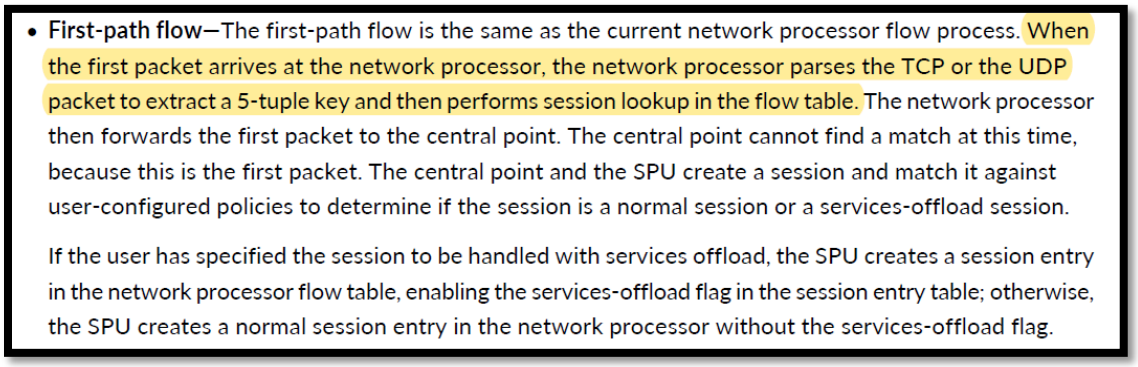
204. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

205. Juniper designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for handling a flow of information packets.

206. Juniper designs, makes, sells, offers to sell, imports, and/or uses Juniper devices that enable the identification of a flow based on the behavior of the flow, including the NFX150 SRX300, SRX320, SRX340, SRX345, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices with Junos OS 18.2 Release 1 and later installed; the SRX380 devices with Junos OS 20.1 Release 1 and later installed; and the vSRX devices with vSRX 12.1X46-D10 and later installed (collectively, the "Juniper '790 Products(s)").

207. One or more Juniper subsidiaries and/or affiliates use the Juniper '790 Products in regular business operations.

208. One or more of the Juniper '790 Products include technology for handling a flow of information packets. Specifically, the Juniper '790 Product process information packets that have the same header information. Specifically, the Juniper '790 Products perform the step of creating a flow block as the first packet of a flow is processed by a router.



- **First-path flow**—The first-path flow is the same as the current network processor flow process. When the first packet arrives at the network processor, the network processor parses the TCP or the UDP packet to extract a 5-tuple key and then performs session lookup in the flow table. The network processor then forwards the first packet to the central point. The central point cannot find a match at this time, because this is the first packet. The central point and the SPU create a session and match it against user-configured policies to determine if the session is a normal session or a services-offload session.

  If the user has specified the session to be handled with services offload, the SPU creates a session entry in the network processor flow table, enabling the services-offload flag in the session entry table; otherwise, the SPU creates a normal session entry in the network processor without the services-offload flag.

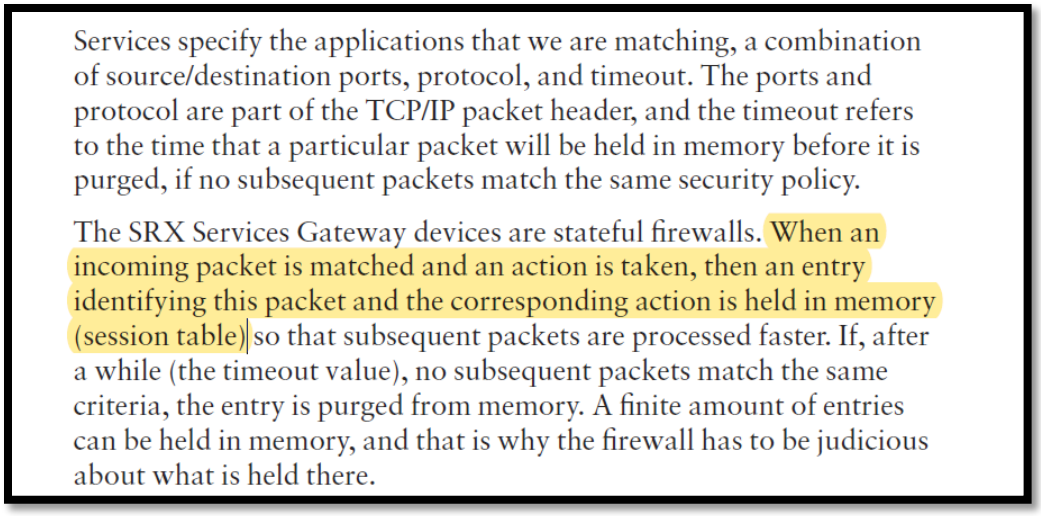
Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices, JUNIPER DOCUMENTATION at 265 (March 25, 2020) (emphasis added).

209. The Juniper '790 Products are available to businesses and individuals throughout the United States.

210. The Juniper '790 Products are provided to businesses and individuals located in the Western District of Texas.

211. Juniper has directly infringed and continues to directly infringe the '790 patent by, among other things, making, using, offering for sale, and/or selling technology for handling a flow of information packets, including but not limited to the Juniper '790 Products.

212. The Juniper '790 Products process a flow comprised of two or more information packets having header information in common. Further, the Juniper '790 Products use header-independent statistics for traffic classification. These statistics include bit rate, packet counts, and byte counts that are used to identify a particular traffic type. The flow information is stored in a flow block or session table that contains statistics about the flow that are updated as each packet in the flow is categorized.



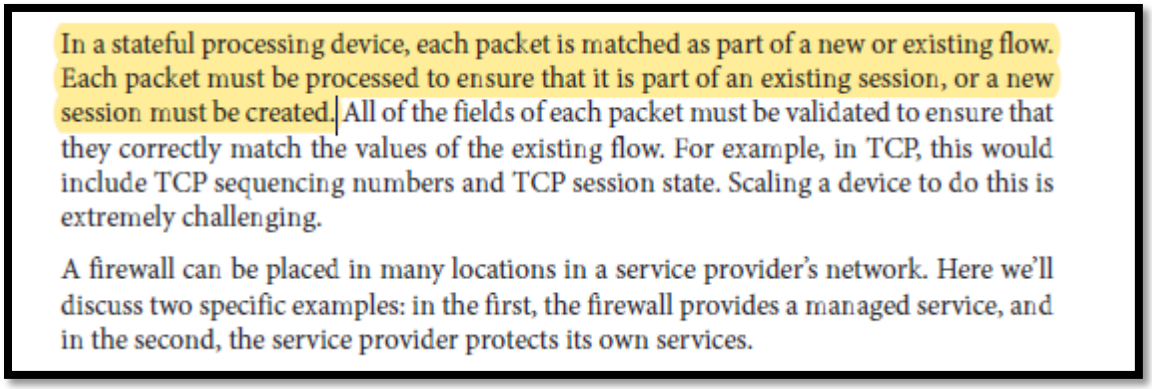
Services specify the applications that we are matching, a combination of source/destination ports, protocol, and timeout. The ports and protocol are part of the TCP/IP packet header, and the timeout refers to the time that a particular packet will be held in memory before it is purged, if no subsequent packets match the same security policy.

The SRX Services Gateway devices are stateful firewalls. When an incoming packet is matched and an action is taken, then an entry identifying this packet and the corresponding action is held in memory (session table) so that subsequent packets are processed faster. If, after a while (the timeout value), no subsequent packets match the same criteria, the entry is purged from memory. A finite amount of entries can be held in memory, and that is why the firewall has to be judicious about what is held there.

Barny Sanchez, *Day One: Deploying SRX Series Services Gateway*, JUNOS DYNAMIC SERVICES SERIES at 58 (2011) (emphasis added).

213. The Juniper '790 Products store header-independent statistics about the flow in a flow block associated with the flow.

214. The Juniper '790 Products perform traffic matching using header-independent statistics such as: total number of input packets, total number of output packets, input bit rates, and output bit rates.



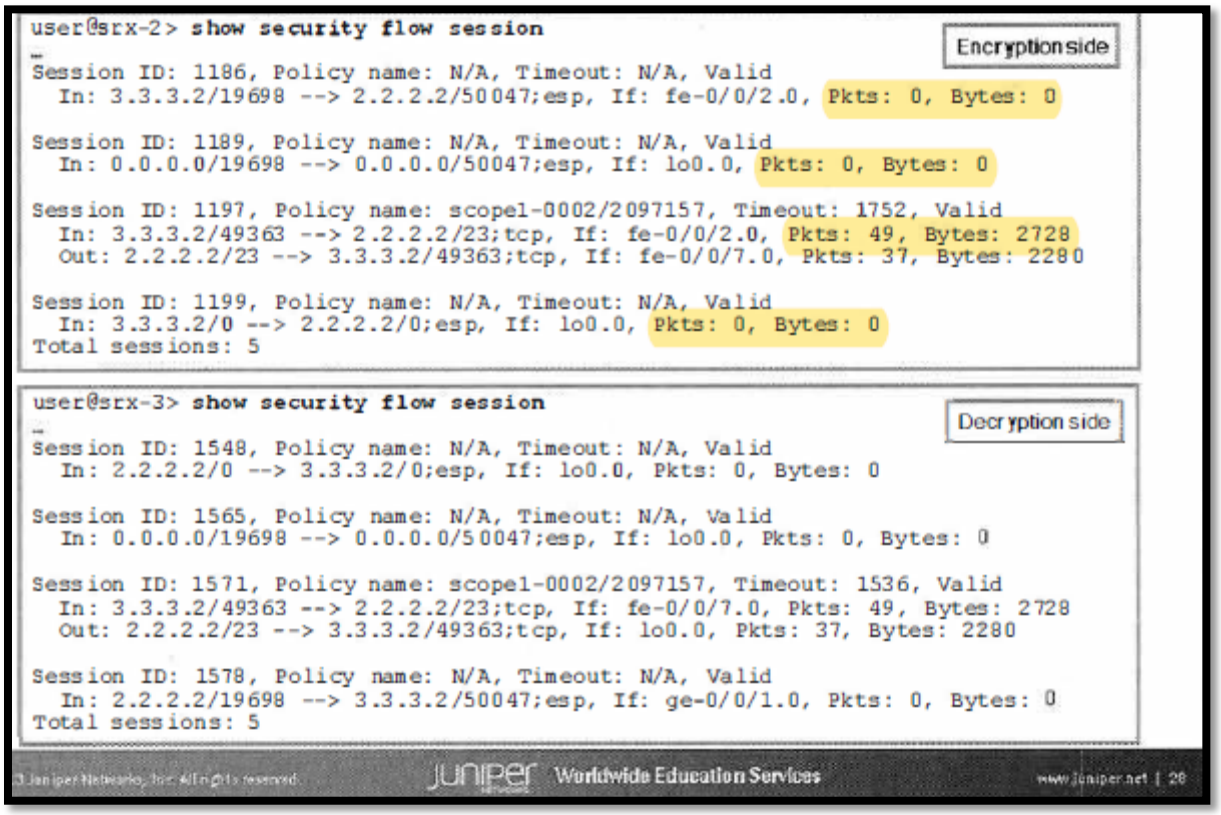
In a stateful processing device, each packet is matched as part of a new or existing flow. Each packet must be processed to ensure that it is part of an existing session, or a new session must be created. All of the fields of each packet must be validated to ensure that they correctly match the values of the existing flow. For example, in TCP, this would include TCP sequencing numbers and TCP session state. Scaling a device to do this is extremely challenging.

A firewall can be placed in many locations in a service provider's network. Here we'll discuss two specific examples: in the first, the firewall provides a managed service, and in the second, the service provider protects its own services.

Brad Woodberg & Rob Cameron, JUNIPER SRX SERIES: A COMPREHENSIVE GUIDE TO SECURITY SERVICES ON SRX SERIES at Chapter 1:16 (2013) (emphasis added).

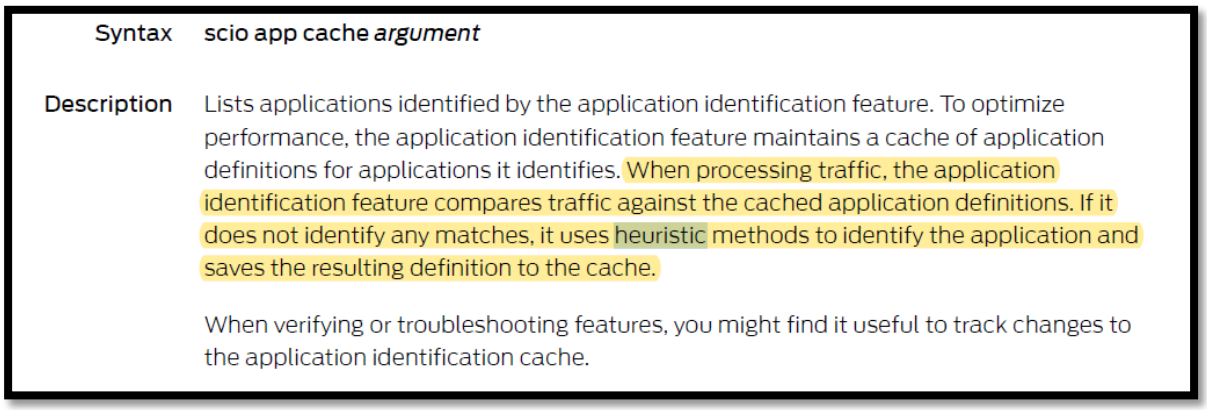
215. The Juniper '790 Products update the header-independent statistics in the flow block as each information packet belonging to the flow is processed. The header-independent

statistics are stored in a flow block associated with the flow. Specifically, the payload content agnostic behavioral statistics that are calculated by the Juniper '790 Products when a packet is ingested include the total byte count accumulated for a flow as shown in the below excerpt from Juniper documentation.



Advanced Junos Security Version 12.b Student Guide Vol. 1, JUNIPER COURSE MATERIALS EDU-JUN-AJSEC at Chapter 7-28 (June 2013) (emphasis added).

216. The Juniper '790 Products categorize the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.



Syntax	scio app cache *argument*
Description	Lists applications identified by the application identification feature. To optimize performance, the application identification feature maintains a cache of application definitions for applications it identifies. When processing traffic, the application identification feature compares traffic against the cached application definitions. If it does not identify any matches, it uses heuristic methods to identify the application and saves the resulting definition to the cache. When verifying or troubleshooting features, you might find it useful to track changes to the application identification cache.

Juniper IDP Series Administration Guide Release 5.1rX, JUNIPER DOCUMENTATION at 327 (December 19, 2013) (emphasis added).

217. The Juniper '790 Products perform an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

218. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Juniper '790 Products, Juniper has injured Plaintiffs and is liable for directly infringing one or more claims of the '790 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

219. Juniper also indirectly infringes the '790 patent by actively inducing infringement under 35 USC § 271(b).

220. Juniper has had knowledge of the '790 patent since at least service of this Complaint or shortly thereafter, and Juniper knew of the '790 patent and knew of its infringement, including by way of this lawsuit.

221. Alternatively, Juniper has had knowledge of the '790 patent since at least April 2, 2020, when U.S. Patent Appl. 16/145,682, which is owned by Juniper and cites the '790 patent as relevant prior art, was published.

222. Juniper intended to induce patent infringement by third-party customers and users of the Juniper '790 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Juniper specifically intended and was aware that the normal and customary use of the accused products would infringe the '790 patent. Juniper performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '790 patent and with the knowledge that the induced acts would constitute infringement. For example, Juniper provides the Juniper '790 Products that have the capability of operating in a manner that infringe one or more of the claims of the '790 patent, including at least claim 1, and Juniper further provides documentation and training materials that cause customers and end users of the Juniper '790 Products to utilize the products in a manner that directly infringe one or more claims of the '790 patent.[24] By providing instruction and training to customers and end-users on how to use the Juniper '790 Products in a manner that directly infringes one or more claims of the '790 patent, including at least claim 1, Juniper specifically intended to induce infringement of the '790 patent. Juniper engaged in such inducement to promote the sales of the Juniper '790 Products, e.g., through Juniper user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '790 patent. Accordingly, Juniper has

[24] *See, e.g.*, *See, e.g.*, *Juniper vSRX – Technical Overview for X47D20*, JUNIPER PRESENTATION (2015); *Junos OS Application Security User Guide For Security Devices,* JUNIPER DOCUMENTATION (March 18, 2020); *Advanced Junos Security Version 12.b Student Guide Vol. 1*, JUNIPER COURSE MATERIALS EDU-JUN-AJSEC (June 2013); *Learn About Application Visibility and Control*, JUNIPER NETWORKS DOCUMENTATION (September 2016); *Juniper IDP Series Administration Guide Release 5.1rX*, JUNIPER DOCUMENTATION (December 19, 2013); *Junos OS Flow-Based and Packet-Based Processing User Guide for Security Devices,* JUNIPER DOCUMENTATION (March 25, 2020); Alexandre S. Cezar, DAY ONE: SRX SERIES UP AND RUNNING WITH ADVANCED SECURITY SERVICES (Mar. 2018); *QoS Configuration for SRX Series for the Branch with Integrated Convergence Services*, JUNIPER NETWORKS APPLICATION NOTE (Nov. 2010); and JUNIPER ADVANCED THREAT PREVENTION APPLIANCE INTEGRATION WITH THE SRX SERIES DEVICE (Jan. 19, 2020).

induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '790 patent, knowing that such use constitutes infringement of the '790 patent.

223. The '790 patent is well-known within the industry as demonstrated by multiple citations to the '790 patent in published patents and patent applications assigned to technology companies and academic institutions. Juniper is utilizing the technology claimed in the '790 patent without paying a reasonable royalty. Juniper is infringing the '790 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

224. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '790 patent.

225. As a result of Juniper's infringement of the '790 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty for the use made of the invention by Juniper together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

A. A judgment in favor of Plaintiffs that Juniper has infringed, either literally and/or under the doctrine of equivalents, the '431, '932, '358, '775, '593, and '790 patents;

B. An award of damages resulting from Juniper's acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that Juniper's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Juniper.

E. Any and all other relief to which Plaintiffs may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: June 15, 2020

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for Sable Networks, Inc. and Sable IP, LLC