UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

COMMSTECH LLC, Plaintiff, v. JUNIPER NETWORKS, INC., Defendant.	Case No. 4:19-cv-545 **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Commstech LLC ("Commstech" or "Plaintiff") hereby asserts the following claims for patent infringement against Defendant Juniper Networks, Inc. ("Juniper" or "Defendant"), and alleges as follows:

SUMMARY

1. Commstech owns United States Patent Nos. 6,349,340, 7,769,028, and 7,990,860 (collectively, the "Patents-in-Suit").

2. Juniper infringes the Patents-in-Suit by implementing, without authorization, Commstech's proprietary technologies in a number of its commercial networking products and related software (collectively referred to herein as the "Accused Products") including, *inter alia*, products that support the RFC 4607 specification related to "Source-Specific Multicast for IP" (e.g., Juniper's platform of switches and routers including the EX Series, the M Series, the MX Series, the T Series. the PTX Series, the SRX Series, the QFabric System, and the QFX Series), and products that operate with the Juniper Networks Session and Resource Control (SRC) software (e.g., C Series Controllers, including the C2000,

C3000, C4000, and C5000 systems). *See, e.g.,* https://www.juniper.net/documentation/en_US/junos/topics/reference/standards/multicast-ip.html; https://www.juniper.net/documentation/en_US/src4.7/topics/concept/src-description.html.

3. By this action, Commstech seeks to obtain compensation for the harm Commstech has suffered as a result of Juniper's infringement of the Patents-in-Suit.

NATURE OF THE ACTION

4. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

5. Juniper has infringed and continues to infringe, and at least as early as the filing and/or service of this Complaint, has induced and continues to induce infringement of, and has contributed to and continues to contribute to infringement of, at least one or more claims of Commstech's Patents-in-Suit at least by making, using, selling, and/or offering to sell its products and services in the United States, including in this District.

6. Commstech is the legal owner by assignment of the Patents-in-Suit, which were duly and legally issued by the United States Patent and Trademark Office ("USPTO"). Commstech seeks monetary damages for Juniper's infringement of the Patents-in-Suit.

THE PARTIES

7. Plaintiff Commstech LLC is a Texas limited liability company with its principal place of business at 1708 Harrington Dr., Plano, Texas 75075. Commstech is the owner of intellectual property rights at issue in this action.

8. On information and belief, Defendant Juniper Networks, Inc. is a Delaware corporation with a principal place of business at 1133 Innovation Way, Sunnyvale, California 94089.

On information and belief, Juniper maintains at least one office in this District at 5830 Granite Parkway, Suite 850, Plano, Texas 75024.

9. On information and belief, Juniper directly and/or indirectly develops, designs, manufactures, distributes, markets, offers to sell and/or sells infringing products and services in the United States, including in the Eastern District of Texas, and otherwise directs infringing activities to this District in connection with its products and services.

JURISDICTION AND VENUE

10. As this is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*., this Court has subject matter jurisdiction over the matters asserted herein under 28 U.S.C. §§ 1331 and 1338(a).

11. This Court has personal jurisdiction over Juniper because Juniper has (1) availed itself of the rights and benefits of the laws of the State of Texas, (2) transacted, conducted, and/or solicited business and engaged in a persistent course of conduct in the State of Texas (and in this District), (3) derived substantial revenue from the sales and/or use of products, such as the Accused Products, in the State of Texas (and in this District), (4) purposefully directed activities (directly and/or through intermediaries), such as shipping, distributing, offering for sale, selling, and/or advertising the Accused Products, at residents of the State of Texas (and residents in this District), (5) delivered Accused Products into the stream of commerce with the expectation that the Accused Products will be used and/or purchased by consumers in the State of Texas (and in this District), and (6) committed acts of patent infringement in the State of Texas (and in this District).

12. This Court also has personal jurisdiction over Juniper because it is registered to do business in Texas and has a regular and established place of business in the Eastern District of Texas.

13. Venue is proper in this District under 28 U.S.C. § 1400(b).

PATENTS-IN-SUIT

U.S. Patent No. 6,349,340

14. U.S. Patent No. 6,349,340 ("the '340 Patent") is entitled "Data multicast channelization," and was issued on February 19, 2002. A true and correct copy of the '340 Patent is attached as Exhibit A.

15. The '340 Patent was filed on January 13, 2000 as U.S. Patent Application No. 09/482,496.

16. Commstech is the owner of all rights, title, and interest in and to the '340 Patent, with the full and exclusive right to bring suit to enforce the '340 Patent, including the right to recover for past infringement.

17. The '340 Patent is valid and enforceable under United States Patent Laws.

18. The '340 Patent recognized several problems with existing high-speed network data distribution technology, such as multicast technology. Notably, the '340 Patent recognized that "[m]anagement of high-speed data across distributed data networks can involve two basic approaches," both of which have several drawbacks. Exhibit A at 1:32-33.

19. For instance, the '340 Patent recognized problems with a "more common approach" referred to as the "client-based" approach, where "client nodes notify server nodes of their interest in certain desired data," and the "servers can individually distribute data packets to each interested, subscribing client." *Id.* at 1:33-39. In this respect, the '340 Patent recognized that this "client-based" approach "tends to overburden the server as network demands grow." *Id.* at 1:30-41. In particular, the '340 Patent discloses that "as additional client nodes are added to the network, the server not only must individually distribute the data packets to each interested client node, but also the server must individually distribute

the data packets to each additional subscribing client node," and thus, "as the client node list grows, so does the server's workload." *Id.* at 1:41-47.

20. The '340 Patent also recognized problems with another approach referred to as the "server-based" approach that uses multicast technology, in which "the server transmits the data packet to a multicast destination address identifying a particular multicast session," and "[i]nterested client nodes merely subscribe to the multicast address, rather than the server, in order to receive the broadcast data." *Id.* at 1:48-58. However, the '340 Patent recognized that "because all client nodes receive each broadcast data packet, regardless of the content of the data packet, each client node must filter unwanted data upon receipt of each data packet," but "[c]lient nodes generally are uninterested in most of the broadcast data and, as a result, client nodes expend substantial processor resources identifying and discarding unwanted data packets." *Id.* at 1:54-2:4. Further, the '340 Patent recognized that, although these existing approaches "allow[ ] a server to provide data at high data transmission rates to more client[ ] nodes," these approaches can "limit the client node's ability to filter unwanted data packets" given the client node's "processor overhead." *Id.* at 2:7-11.

21. To address one or more shortcomings of existing high-speed network data distribution technology, such as existing multicast technology that "challeng[ed] the client node's ability to filter the unwanted data packets," the '340 Patent discloses, *inter alia*, a "method for efficient filtering of unwanted data in a multicast network environment" that "satisfies the long-felt need of the prior art by applying a combination hardware and software solution which selectively filters multicast data by selectively disabling channels containing unwanted data." *Id.* at 2:14-25. The '340 Patent's "inventive arrangements" have "advantages over all other data distribution methods" and provide "a novel and

nonobvious method for receiving the benefits of multicasting while avoiding the drawbacks associated with such systems." *Id.* at 2:26-30.

22. Indeed, the inventions of the '340 Patent improved the functionality of "client" computers operating in a multicast network environment by reducing the "substantial processor resources" expended by "client" computers using existing data filtering mechanisms, such as by reducing the resources expended by a "client" computer's "network applications software." Exhibit A at 6:9-47. In this respect, the inventions of the '340 Patent allow a "client" computer to "avoid excessive software filtering" that leads to "performance gain" that can be "significant." *Id.* at 10:21-31.

The Inventions Claimed in U.S. Patent No. 6,349,340 Improved Technology & Were Not Well-Understood, Routine, or Conventional

23. Given the state of the art at the time of the inventions of the '340 Patent, including the deficiencies in network data distribution systems of the time, the inventive concepts of the '340 Patent cannot be considered to be conventional, well-understood, or routine. *See, e.g.*, Exhibit A at 1:32-2:17. Indeed, there was a long-felt need in the art at the time of the inventions of the '340 Patent that the claimed inventions of the '340 Patent addressed. *See, e.g., id* at 2:20-26. In this respect, the '340 Patent discloses, among other things, an unconventional solution to problems arising in the context of network data distribution systems, namely, that "client" computers in such systems "expend[ed] substantial processor resources" filtering multicast data and this "processor overhead" inhibited the "client" computers' ability to handle the increasing user demands for network data distribution systems to broadcast more data. *See, e.g., id* at 2:1-17.

24. The inventions of the '340 Patent offered an unconventional, technological solution to such problems resulting in a "novel and nonobvious method for receiving the benefits of

multicasting while avoiding the drawbacks associated with such [existing] systems." Exhibit A at 2:25-30; *see also, e.g., id.* at 10:21-26 ("The inventive multicast channelization strategy can increase the bandwidth available to the expanding client node base by distributing the broadcast data across multiple channels," such that "client nodes can selectively filter unwanted broadcast data within the network interface circuitry of each client node."). In this respect, the inventions of the '340 Patent improved the functionality of "client" computers operating in a multicast network environment. *See, e.g.*, *id.* at 6:9-47, 10:21-31.

25. Indeed, it was not well-understood, routine, or conventional at the time of the inventions of the '340 Patent to perform the following functions, alone and/or in combination with one another: (i) selecting from among a plurality of multicast communications channels a source communications channel for receiving requested multicast data, (ii) enabling the selected source communications channel, (iii) receiving the requested multicast data through the enabled source communications channel, (iv) forwarding the requested multicast data to requesting processes, and (v) disabling the selected source communications channel when the requesting processes indicate that no further data is requested to be received over the selected source communications channel. *See, e.g.*, Exhibit A at Claims 1, 8, 14. Moreover, it was not well-understood, routine, or conventional at the time of the inventions of the '340 Patent to perform one or more of the following functions alone and/or in combination with one or more of the preceding functions: (i) receiving from one or more processes in a client node a request for multicast data, (ii) identifying a multicast data source for each requested data, and (iii) disabling an enabled selected source communications channel when the requesting client node process

indicates that no further data is requested to be received from the identified multicast data source over the selected source communications channel and no other requesting client node processes have indicated a continuing need for further data to be received from the identified multicast data source over the selected source communications channel. *See, e.g.*, *id.* at Claims 1, 8, 14.

26. Further, it was not well-understood, routine, or conventional at the time of the inventions of the '340 Patent to perform one or more of the following functions alone and/or in combination with one or more of the unconventional functions set forth in paragraph number 25: (i) filtering, from multicast data received through an enabled source communications channel, unwanted/unrequested multicast data, (ii) discarding the unwanted/unrequested multicast data, and (ii) forwarding the filtered multicast data to one or more requesting processes. *See, e.g.*, Exhibit A at Claims 3, 9, 15.

27. These are just exemplary reasons why the inventions claimed in the '340 Patent were not well-understood, routine, or conventional at the time of the invention of the '340 Patent.

28. Consistent with the problems addressed by the '340 Patent being rooted in network data distribution systems, the '340 Patent's inventions naturally are also rooted in that same technology that cannot be performed solely with pen and paper or in the human mind. Indeed, using pen and paper or a human mind would not only ignore, but would run counter to, the stated technical solution of the '340 Patent noted above and the technical problems that the '340 Patent was specifically designed to address. Likewise, at least because the '340 Patent's claimed inventions address problems rooted in network data distribution systems, these inventions are not merely drawn to longstanding human activities.

U.S. Patent No. 7,769,028

29. U.S. Patent No. 7,769,028 ("the '028 Patent") is entitled "Systems and methods for adaptive throughput management for event-driven message-based data," and was issued on August 3, 2010. A true and correct copy of the '028 Patent is attached as Exhibit B.

30. The '028 Patent was filed on June 21, 2006 as U.S. Patent Application No. 11/471,923.

31. Commstech is the owner of all rights, title, and interest in and to the '028 Patent, with the full and exclusive right to bring suit to enforce the '028 Patent, including the right to recover for past infringement.

32. The '028 Patent is valid and enforceable under United States Patent Laws.

33. The '028 Patent discloses, among other things, "a method for communicating data including prioritizing data by assigning a priority to the data, analyzing a network to determine a status of the network, and communicating data based at least in part on the priority of the data and the status of the network." Exhibit B at Abstract. The '028 Patent also discloses "Quality of Service (QoS)," which "refers to one or more capabilities of a network to provide various forms of guarantees with regard to data this is carried." *Id.* at 4:16-18. The '028 Patent states that "[t]he primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved [data] loss characteristics." *Id.* at 4:27-31.

34. In discussing QoS, the '028 Patent recognized various shortcomings of existing QoS systems. As one example, the '028 Patent states that "[e]xisting QoS systems cannot provide QoS based on message content at the transport layer" of the Open Systems Interconnection (OSI) seven-layer protocol model. Exhibit B at 5:1-2. Indeed, the '028 Patent explains that the "Transmission Control Protocol (TCP)," which is a protocol at the

transport layer, "requires several forms of handshaking and acknowledgements to occur in order to send data," and "[h]igh latency and [data] loss may result in TCP hitting time outs and not being able to send much, if any, meaningful data over [] a network." *Id.* at 1:57-60, 3:53-57. As another example, the '028 Patent states that "[c]urrent approaches to QoS often require every node in a network to support QoS, or at the very least, for every node in the network involved in a particular communication to support QoS," but such approaches to QoS "do[] not scale well because of the large amount of state information that must be maintained at every node and the overhead associated with setting up such connections." *Id.* at 4:35-39, 4:46-49. As yet another example, the '028 Patent states that "[d]ue to the mechanisms existing QoS solutions utilize, messages that look the same to current QoS systems may actually have different priorities based on message content," but "data consumers may require access to high-priority data without being flooded by lower-priority data." *Id.* at 4:61-67.

35. In discussing the shortcomings of the prior art, the '028 Patent recognized that "[t]here is a need for systems and methods for providing QoS on the edge of a [] data network," and "a need for adaptive, configurable QoS systems and methods in a [] data network." Exhibit B at 5:17-20. The claimed inventions of the '028 Patent provide such systems and methods.

The Inventions Claimed in U.S. Patent No. 7,769,028 Improved Technology & Were Not Well-Understood, Routine, or Conventional

36. Given the state of the art at the time of the inventions of the '028 Patent, including the deficiencies with existing QoS systems for computer networks, the inventive concepts of the '028 Patent cannot be considered to be conventional, well-understood, or routine. *See, e.g.*, Exhibit B at 1:57-60, 3:53-57, 4:35-39, 4:46-49, 4:61-67, 5:1-2, 5:17-20. The '028 Patent discloses, among other things, an unconventional solution to problems arising in the

context of communications networks that relied on existing QoS systems, namely, that such QoS systems did not scale, were not adaptive or configurable to different network types or architectures, and could not provide QoS based on message content at the transport layer, among other deficiencies. *See, e.g.*, *id.*

37. To address one or more deficiencies with existing QoS systems, the inventions of the '028 Patent offered a technological solution that facilitated providing an improved technique for communicating data over a network, which helped to control jitter and latency and improve data loss, among other benefits. In particular, the inventions of the '028 Patent provided a specific, unconventional solution for prioritizing data as part of and/or at the top of the transport layer, dynamically changing rules for assigning priority to data, and communicating data based at least in part on the priority of the data and the status of the network. *See, e.g.*, *id.* at Claims 1, 13, 17; 7:29-31. In this respect, the inventions of the '028 Patent improved the technical functioning of computers and computer networks by reciting a specific technique for prioritizing data communications over a network. *See, e.g.*, *id.* at 4:11-37, 4:57-5:9.

38. Indeed, it was not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication device to (i) prioritize data by assigning priority to data, where the prioritization occurs either as part of and/or at the top of the transport layer, (ii) analyze a network to determine a status of the network, (iii) select a mode based on the status of the network, (iv) change rules for assigning priority to the data based on the mode, and (v) communicate the data based at least in part on the priority of the data and the status of the network, where the data is communicated at a transmission rate metered based at least in part on the status of the network. *See, e.g.*, Exhibit B at Claim 1. Moreover, it was

not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication device to receive the data at a node on the edge of the network. *See, e.g.*, Exhibit B at Claim 5. It was also not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication device to receive the data at least in part from an application program and/or communicate the data to an application program. *See, e.g.*, *id.* at Claims 6, 12. Further, it was not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication device to assign the priority to the data based at least in part on message content of the data, protocol information of the data, or a user defined rule. *See, e.g.*, *id.* at Claims 7-9.

39. Additionally, it was not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication system to include (i) a data prioritize component adapted to assign a priority to data, where the prioritization occurs either as part of and/or at the top of the transport layer, (ii) a network analysis component adapted to determine a status of the network, (iii) a mode selection component adapted to select a mode based at least on the status of the network, and (iv) a data communications component adapted to communicate the data based at least in part on the priority of the data and the status of the network, where the data prioritization component is adapted to assign priority to the data based on prioritization rules that are selected based on a selected mode, and where the data is communicated at a transmission rate metered based at least in part on the status of the network. *See, e.g.*, Exhibit B at Claims 13, 17. It was also not well-understood, routine, or conventional at the time of the invention of the '028 Patent for a communication system to include a data organization component adapted to organize the data with respect to other data based at least in part on the priority of the data. *See, e.g.*,

id. at Claim 14.

40. These are just exemplary reasons why the inventions claimed in the '028 Patent were not well-understood, routine, or conventional at the time of the invention of the '028 Patent.

41. Consistent with the problems addressed being rooted in QoS systems for computer networks, the '028 Patent's inventions naturally are also rooted in that same technology that cannot be performed solely with pen and paper or in the human mind. Indeed, using pen and paper or a human mind would not only ignore, but would run counter to, the stated technical solution of the '028 Patent noted above and the technical problems that the '028 Patent was specifically designed to address. Likewise, at least because the '028 Patent's claimed inventions address problems rooted in QoS systems for computer networks, these inventions are not merely drawn to longstanding human activities.

U.S. Patent No. 7,990,860

42. U.S. Patent No. 7,990,860 ("the '860 Patent") is entitled "Method and system for rule-based sequencing for QoS," and was issued on August 2, 2011. A true and correct copy of the '860 Patent is attached as Exhibit C.

43. The '860 Patent was filed on June 16, 2006 as U.S. Patent Application No. 11/454,220.

44. Commstech is the owner of all rights, title, and interest in and to the '860 Patent, with the full and exclusive right to bring suit to enforce the '860 Patent, including the right to recover for past infringement.

45. The '860 Patent is valid and enforceable under United States Patent Laws.

46. The '860 Patent discloses, among other things, "a method for communicating data over a network to provide Quality of Service," including "prioritizing the data, and communicating the data based at least in part on the priority." Exhibit C at Abstract.

According to the '860 Patent, "Quality of Service (QoS)" "refers to one or more capabilities of a network to provide various forms of guarantees with regard to data that is carried." *Id.* at 4:16-18. The '860 Patent states that "[t]he primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved [data] loss characteristics." *Id.* at 4:27-32.

47. Like the '028 Patent, the '860 Patent recognized various shortcomings of existing QoS systems. As one example, the '860 Patent states that "[e]xisting QoS systems cannot provide QoS based on message content at the transport layer" of the Open Systems Interconnection (OSI) seven-layer protocol model. Exhibit C at 5:2-3. Indeed, the '860 Patent explains that the "Transmission Control Protocol (TCP)," which is a protocol at the transport layer, "requires several forms of handshaking and acknowledgements to occur in order to send data," and "[h]igh latency and [data] loss may result in TCP hitting time outs and not being able to send much, if any, meaningful data over [] a network." *Id.* at 1:57-60, 3:53-57. As another example, the '860 Patent states that "[c]urrent approaches to QoS often require every node in a network to support QoS, or at the very least, for every node in the network involved in a particular communication to support QoS," but such approaches to QoS "do[] not scale well because of the large amount of state information that must be maintained at every node and the overhead associated with setting up such connections." *Id.* at 4:36-39, 4:47-50. As yet another example, the '860 Patent states that "[d]ue to the mechanisms existing QoS solutions utilize, messages that look the same to current QoS systems may actually have different priorities based on message content," but "data consumers may require access to high-priority data without being flooded by lower-priority data." *Id.* at 4:64-5:1.

48. In discussing the shortcomings of the prior art, the '860 Patent recognized that "[t]here is a need for systems and methods for providing QoS on the edge of a [] data network," and "a need for adaptive, configurable QoS systems and methods in a [] data network." Exhibit C at 5:19-22. The claimed inventions of the '860 Patent provide such systems and methods.

The Inventions Claimed in U.S. Patent No. 7,990,860 Improved Technology & Were Not Well-Understood, Routine, or Conventional

49. Given the state of the art at the time of the inventions of the '860 Patent, including the deficiencies with existing QoS systems for computer networks, the inventive concepts of the '860 Patent cannot be considered to be conventional, well-understood, or routine. *See, e.g.*, Exhibit C at 1:57-60, 3:53-57, 4:36-39, 4:47-50, 4:64-5:2, 5:19-22. The '860 Patent discloses, among other things, an unconventional solution to problems arising in the context of communications networks that relied on existing QoS systems, namely, that such QoS systems did not scale, were not adaptive or configurable to different network types or architectures, and could not provide QoS based on message content at the transport layer, among other deficiencies. *See, e.g.*, *id.*

50. To address one or more deficiencies with existing QoS systems, the inventions of the '860 Patent offered a technological solution that facilitated providing an improved technique for communicating data over a network, which helped to control jitter and latency and improve data loss, among other benefits. In particular, the inventions of the '860 Patent provided a specific, unconventional solution for prioritizing data as part of and/or at the top of the transport layer by sequencing the data based at least in part on a user defined rule. *See, e.g.*, *id.* at Abstract, Claims 1, 13, 17. In this respect, the inventions of the '860 Patent improved the technical functioning of computers and computer networks by reciting a specific technique for prioritizing data communications over a network. *See, e.g.*, *id.* at

4:11-37, 4:57-5:9.

51. Indeed, it was not well-understood, routine, or conventional at the time of the invention of the '860 Patent for a communication device to include (i) a network analysis component configured to determine a network status from a plurality of network statuses based on analysis of network measurements, and determine at least one of an effective link speed and a link proportion for at least one link, (ii) a mode selection component configured to select a mode from a plurality of modes that corresponds with at least one of the plurality of network statuses based on the determined network status, where each of the plurality of modes comprises a user defined sequencing rule, (iii) a data prioritization component configured to operate at a transport layer of a protocol stack and prioritize the data by assigning a priority to the data, where the prioritization component includes a sequencing component configured to sequence the data based at least in part on the user defined sequencing rule of the selected mode, (iv) a data metering component configured to meter inbound data by shaping the inbound data at the data communications system for the at least one link, and meter outbound data by policing the outbound data at the data communications system for the at least one link, and (v) a data communication component configured to communicate the data based at least in part on the priority of the data, the effective link speed, and/or the link proportion. *See, e.g.*, Exhibit C at Claims 1, 15, 20.

52. Moreover, it was not well-understood, routine, or conventional at the time of the invention of the '860 Patent for the user defined sequencing rule mentioned above to be dynamically reconfigurable. *See, e.g.*, Exhibit C at Claim 5. It was also not well-understood, routine, or conventional at the time of the invention of the '860 Patent for a communication device to receive the data at least in part from an application program operating on the node, or

pass the data at least in part to an application program operating on the node. *See, e.g.*, *id.* at Claims 6, 12. Further, it was not well-understood, routine, or conventional at the time of the invention of the '860 Patent for a communication device to prioritize the data by differentiating the data based at least in part on message content, protocol information, or a user defined differentiation rule. *See, e.g.*, *id.* at Claims 8-11.

53. These are just exemplary reasons why the inventions claimed in the '860 Patent were not well-understood, routine, or conventional at the time of the invention of the '860 Patent.

54. Consistent with the problems addressed being rooted in QoS systems for computer networks, the '860 Patent's inventions naturally are also rooted in that same technology that cannot be performed solely with pen and paper or in the human mind. Indeed, using pen and paper or a human mind would not only ignore the stated technical solution of the '860 Patent noted above and the technical problem that the '860 Patent was specifically designed to address. Likewise, at least because the '860 Patent's claimed inventions address problems rooted in QoS systems for computer networks, these inventions are not merely drawn to longstanding human activities.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 6,349,340

55. Commstech incorporates by reference and re-alleges paragraphs 14-28 of this Complaint as if fully set forth herein.

56. Defendant Juniper has infringed and is infringing, either literally or under the doctrine of equivalents, the '340 Patent in violation of 35 U.S.C. § 271 *et seq.*, directly and/or indirectly, by making, using, offering for sale, or selling in the United States, and/or importing into the United States without authority or license, products that support the RFC 4607 specification related to "Source-Specific Multicast for IP" (e.g., Juniper's platform

of switches and routers including the EX Series, the M Series, the MX Series, the T Series. the PTX Series, the SRX Series, the QFabric System, and the QFX Series) (collectively referred to herein as the "Accused '340 Products"). *See, e.g.,* https://www.juniper.net/documentation/en_US/junos/topics/reference/standards/multicast-ip.html.

57. As just one non-limiting example, set forth below (with claim language in bold and italics) is exemplary evidence of infringement of Claim 1 of the '340 Patent in connection with the Accused '340 Products. This description is based on publicly available information. Commstech reserves the right to modify this description, including, for example, on the basis of information about the Accused '340 Products that it obtains during discovery.

1(a): A method for receiving requested multicast data over a plurality of multicast communications channels comprising:—Juniper makes, uses, sells, and/or offers to sell a device or system that practices the method of receiving requested multicast data over a plurality of multicast communications channels in accordance with Claim 1. For instance, the Accused '340 Products support the RFC 4607 specification related to "Source-Specific Multicast for IP" that discloses the method recited in Claim 1. *See, e.g.,* https://www.juniper.net/documentation/en_US/junos/topics/reference/standards/multicast-ip.html (disclosing "RFC 4607, Source-Specific Multicast for IP"); Multicast Protocols Feature Guide, p. 19, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf (same). In particular, RFC 4607 defines a "source-specific multicast service" ("SSM") as "[a] datagram sent with source IP address S and destination IP address G in the SSM range [that] is delivered to each host socket that has specifically requested delivery of datagrams sent by S to G, and only to those sockets." Holbrook, Source-specific

multicast for IP, RFC 4607 (2006), p. 5, *available at* https://tools.ietf.org/pdf/rfc4607.pdf; *see also* Multicast Protocols Feature Guide, p. 345, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf ("SSM builds shortest-path trees (SPTs) directly represented by (S,G) pairs[, where t]he 'S' refers to the source's unicast IP address, and the 'G' refers to the specific multicast group address."); *id.* at p. 343 ("Table 14" disclosing "Receiver operations"); https://www.juniper.net/documentation/en_US/junose10.3/information-products/topic-collections/swconfig-multicast-routing/id-66017.html ("Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications.").

1(b): selecting from among the plurality of multicast communications channels a source communications channel for receiving said requested multicast data;—Juniper makes, uses, sells, and/or offers to sell a device or system that selects from among the plurality of multicast communications channels a source communications channel for receiving said requested multicast data. For instance, the Accused '340 Products support the RFC 4607 specification, which discloses a plurality of multicast communication channels, where each "channel is identified (addressed) by the combination of a unicast source address and a multicast destination address in the SSM range" (e.g., "S, G = (192.0.2.1, 232.7.8.9)," "S, G = (192.0.2.2, 232.7.8.9)"). Holbrook, Source-specific multicast for IP, RFC 4607 (2006), p. 6, *available at* https://tools.ietf.org/pdf/rfc4607.pdf; *see also, e.g., id.* at pp. 3-4 ("The network service identified by (S,G), for SSM address G and source host address S, is referred to as a 'channel'"); *id.* at p. 6 ("We use the term 'channel' to refer to the service associated with an SSM address," and "[a] channel is identified by the combination of an

SSM destination address and a specific source, e.g., an (S,G) pair."). In particular RFC 4607 discloses that "[t]he IP module interface to upper-layer protocols is extended to allow a socket to 'Subscribe' to . . . a particular channel identified by an SSM destination address and a source IP address." *Id.* at p. 5; *see also, e.g., id.* at p. 6 ("The receiver operations allowed on a channel are called 'Subscribe (S,G)' and 'Unsubscribe (S,G)'"); *id.* at p. 7 ("If reception of the same channel is desired on multiple interfaces, Subscribe is invoked once for each"); *id.* at p. 8 ("An incoming datagram destined to an SSM address MUST be delivered by the IP module to all sockets that have indicated (via Subscribe) a desire to receive data that matches the datagram's source address, destination address, and arriving interface."). Moreover, Juniper explains that "[i]n a PIM SSM-configured network, a host subscribes to an SSM channel (by means of IGMPv3), announcing a desire to join group G and source S . . . ." Multicast Protocols Feature Guide, p. 339, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf; *see also id.* at p. 54 ("[T]he receiver specifies the source or sources it is interested in receiving the multicast group traffic from."); *id.* at p. 340 ("As sources become active and start sending multicast packets, interested receivers in the SSM group receive the multicast packets."); *id.* at p. 345 ("SSM builds shortest-path trees (SPTs) directly represented by (S,G) pairs[, where t]he 'S' refers to the source's unicast IP address, and the 'G' refers to the specific multicast group address.").

1(c): enabling said selected source communications channel;—Juniper makes, uses, sells, and/or offers to sell a device or system that enables the selected source communications channel. For instance, the Accused '340 Products support the RFC 4607 specification,

which discloses that "[t]he IP module interface to upper-layer protocols is extended to allow a socket to 'Subscribe' to . . . a particular channel identified by an SSM destination address and a source IP address," and subscribing to a particular channel comprises selecting a source communications channel and also enabling the selected source communications channel. Holbrook, Source-specific multicast for IP, RFC 4607 (2006), p. 5, *available at* https://tools.ietf.org/pdf/rfc4607.pdf; *see also, e.g., id.* at p. 6 ("The receiver operations allowed on a channel are called 'Subscribe (S,G)' and 'Unsubscribe (S,G)'"); *id.* at p. 7 ("If reception of the same channel is desired on multiple interfaces, Subscribe is invoked once for each"); *id.* at p. 8 ("An incoming datagram destined to an SSM address MUST be delivered by the IP module to all sockets that have indicated (via Subscribe) a desire to receive data that matches the datagram's source address, destination address, and arriving interface."). Indeed, RFC 4607 discloses that "'interface' is a local identifier of the network interface on which reception of the channel identified by the (source-address, group-address) pair is to be ***enabled*** [e.g., subscribed] or disabled [e.g., unsubscribed]." *Id.* at p. 7 (emphasis added). Moreover, Juniper explains that "[i]n a PIM SSM-configured network, a host subscribes to an SSM channel (by means of IGMPv3), announcing a desire to join group G and source S . . . ." Multicast Protocols Feature Guide, p. 339, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf; *see also id.* at p. 54 ("[T]he receiver specifies the source or sources it is interested in receiving the multicast group traffic from."); *id.* at p. 340 ("As sources become active and start sending multicast packets, interested receivers in the SSM group receive the multicast packets.").

1(d): receiving said requested multicast data through said enabled source

communications channel;—Juniper makes, uses, sells, and/or offers to sell a device or system that receives the requested multicast data through the enabled source communications channel. For instance, the Accused '340 Products support the RFC 4607 specification, which discloses that "[a]n incoming datagram destined to an SSM address MUST be delivered by the IP module to all sockets that have indicated (via Subscribe) a desire to receive data that matches the datagram's source address, destination address, and arriving interface." Holbrook, Source-specific multicast for IP, RFC 4607 (2006), p. 8, *available at* https://tools.ietf.org/pdf/rfc4607.pdf; *see also, e.g., id.* ("When the first socket on host H subscribes to a channel (S,G) on interface I, the host IP module on H sends a request on interface I to indicate to neighboring routers that the host wishes to receive traffic sent by source S to source-specific multicast destination G."). Moreover, Juniper explains that "[i]n a PIM SSM-configured network, a host subscribes to an SSM channel (by means of IGMPv3), announcing a desire to join group G and source S . . . ." Multicast Protocols Feature Guide, p. 339, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf. According to Juniper, "[a]s sources become active and start sending multicast packets, interested receivers in the SSM group receive the multicast packets.". *Id.* at p. 340; *see also id.* at p. 343 ("Table 14" disclosing "Receiver operations"); *id.* at p. 54 ("[T]he receiver specifies the source or sources it is interested in receiving the multicast group traffic from.").

1(e): forwarding said requested multicast data to requesting processes; and,—Juniper makes, uses, sells, and/or offers to sell a device or system that forwards the requested multicast data to requesting processes. For instance, as noted above, the Accused '340

Products support the RFC 4607 specification, which discloses that "[a]n incoming datagram destined to an SSM address MUST be delivered by the IP module to all ***sockets*** that have indicated (via Subscribe) a desire to receive data that matches the datagram's source address, destination address, and arriving interface." Holbrook, Source-specific multicast for IP, RFC 4607 (2006), p. 8, *available at* https://tools.ietf.org/pdf/rfc4607.pdf (emphasis added); *see also, e.g., id.* ("When the first socket on host H subscribes to a channel (S,G) on interface I, the host IP module on H sends a request on interface I to indicate to neighboring routers that the host wishes to receive traffic sent by source S to source-specific multicast destination G."). In particular, RFC 4607 defines a "socket" as "an implementation-specific parameter used to distinguish among different requesting entities (e.g., programs or processes or communication end-points within a program or process) within the requesting host." *Id.* at p. 5. Moreover, Juniper discloses that "[a]s sources become active and start sending multicast packets, interested receivers in the SSM group receive the multicast packets." Multicast Protocols Feature Guide at p. 340, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf; *see also id.* at p. 343 ("Table 14" disclosing "Receiver operations"); *id.* at p. 54 ("[T]he receiver specifies the source or sources it is interested in receiving the multicast group traffic from.").

1(f): disabling said selected source communications channel when said requesting processes indicate that no further data is requested to be received over said selected source communications channel.—Juniper makes, uses, sells, and/or offers to sell a device or system that disables the selected source communications channel when the requesting processes indicate that no further data is requested to be received over the selected source

communications channel. For instance, the Accused '340 Products support the RFC 4607 specification, which discloses that "[t]he IP module interface to upper-layer protocols is extended to allow a socket to . . . 'Unsubscribe' from a particular channel identified by an SSM destination address and a source IP address," and unsubscribing from a particular channel disables the particular channel to indicate that no further data is requested to be received over the particular channel. Holbrook, Source-specific multicast for IP, RFC 4607 (2006), p. 5, *available at* https://tools.ietf.org/pdf/rfc4607.pdf; *see also, e.g., id.* at p. 8 (disclosing that "[a]n incoming datagram destined to an SSM address MUST be delivered by the IP module to all sockets that have indicated (via Subscribe) a desire to receive data that matches the datagram's source address, destination address, and arriving interface," but "MUST NOT be delivered to other sockets" (e.g., sockets that have Unsubscribed)). Indeed, as noted above, RFC 4607 discloses that "'interface' is a local identifier of the network interface on which reception of the channel identified by the (source-address, group-address) pair is to be enabled [e.g., subscribed] or ***disabled*** [e.g., unsubscribed]." *Id.* at p. 7 (emphasis added). Moreover, Juniper discloses that "PIM SSM describes receiver operations as *subscribe* and ***unsubscribe*** . . ." Multicast Protocols Feature Guide, p. 339, *available at* https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-multicast/config-guide-multicast.pdf (emphasis added); *see also id.* at p. 339 ("Table 13" disclosing "subscribe, unsubscribe").

58. Additionally, Juniper has been and/or currently is an active inducer of infringement of the '340 Patent under 35 U.S.C. § 271(b) and a contributory infringer of the '340 Patent under 35 U.S.C. § 271(c).

59. Juniper knew of the '340 Patent, or at least should have known of the '340 Patent, but was

willfully blind to its existence. On information and belief, Juniper has had actual knowledge of the '340 Patent since at least as early as the filing and/or service of this Complaint.

60. Juniper has provided the Accused '340 Products to its customers and, on information and belief, instructions to use the Accused '340 Products in an infringing manner while being on notice of (or willfully blind to) the '340 Patent and Juniper's infringement. Therefore, on information and belief, Juniper knew or should have known of the '340 Patent and of its own infringing acts, or deliberately took steps to avoid learning of those facts.

61. Juniper knowingly and intentionally encourages and aids at least its end-user customers to directly infringe the '340 Patent.

62. Juniper's end-user customers directly infringe at least one or more claims of the '340 Patent by using the Accused '340 Products in their intended manner to infringe. Juniper induces such infringement by providing the Accused '340 Products and instructions to enable and facilitate infringement, knowing of, or being willfully blind to the existence of, the '340 Patent. On information and belief, Juniper specifically intends that its actions will result in infringement of one or more claims of the '340 Patent, or subjectively believe that their actions will result in infringement of the '340 Patent, but took deliberate actions to avoid learning of those facts, as set forth above.

63. Additionally, Juniper contributorily infringes at least one or more claims of the '340 Patent by providing the Accused '340 Products and/or software components thereof, that embody a material part of the claimed inventions of the '340 Patent, that are known by Juniper to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses. The Accused '340 Products are specially designed to

infringe at least one or more claims of the '340 Patent, and their accused components have no substantial non-infringing uses. In particular, on information and belief, the software modules and code that implement and perform the infringing functionalities identified above are specially made and adapted to carry out said functionality and do not have any substantial non-infringing uses.

64. At least as early as the filing and/or service of this Complaint, Juniper's infringement of the '340 Patent was and continues to be willful and deliberate, entitling Commstech to enhanced damages.

65. Additional allegations regarding Juniper's knowledge of the '340 Patent and willful infringement will likely have evidentiary support after a reasonable opportunity for discovery.

66. Juniper's infringement of the '340 Patent is exceptional and entitles Commstech to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

67. Commstech is in compliance with any applicable marking and/or notice provisions of 35 U.S.C. § 287 with respect to the '340 Patent.

68. Commstech is entitled to recover from Juniper all damages that Commstech has sustained as a result of Juniper's infringement of the '340 Patent, including, without limitation, a reasonable royalty.

COUNT II: INFRINGEMENT OF U.S. PATENT NO. 7,769,028

69. Commstech incorporates by reference and re-alleges paragraphs 29-41 of this Complaint as if fully set forth herein.

70. Defendant Juniper has infringed and is infringing, either literally or under the doctrine of equivalents, the '028 Patent in violation of 35 U.S.C. § 271 *et seq.*, directly and/or

indirectly, by making, using, offering for sale, or selling in the United States, and/or importing into the United States without authority or license, products that operate with the Juniper Networks Session and Resource Control (SRC) software (e.g., C Series Controllers, including the C2000, C3000, C4000, and C5000 systems) (collectively referred to herein as the "Accused '028 Products"), that infringe at least one or more claims of the '028 Patent. *See, e.g.,* https://www.juniper.net/documentation/en_US/src4.7/topics/concept/src-description.html.

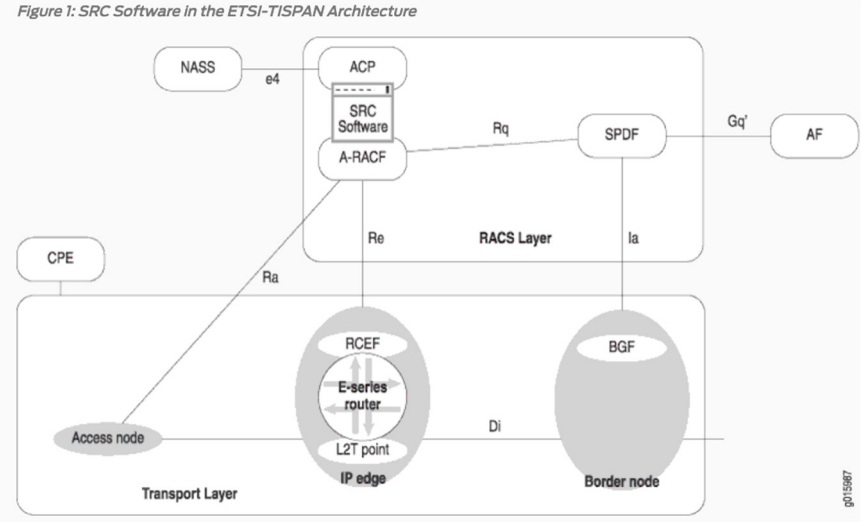
71. As just one non-limiting example, set forth below (with claim language in bold and italics) is exemplary evidence of infringement of Claim 17 of the '028 Patent in connection with the Accused '028 Products. This description is based on publicly available information. Commstech reserves the right to modify this description, including, for example, on the basis of information about the Accused '028 Products that it obtains during discovery.

17(a): A non-transitory computer-readable medium including a set of instructions for execution on a computer, the set of instructions including: —Juniper makes, uses, sells, and/or offers to sell a non-transitory computer-readable medium including a set of instructions for execution on a computer that include the functions recited below. For instance, according to Juniper, the Accused '028 Products that operate with the SRC software "can manage policies on Juniper Networks routers and cable modem termination system (CMTS) devices and can activate policies on other systems to provide end-to-end service quality." https://www.juniper.net/documentation/en_US/src4.7/topics/concept/src-description.html. Juniper also discloses that the SRC software can operate in the "ETSI-TISPAN Architecture." https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* https://www.jun

iper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture.html (disclosing "ETSI-TISPAN Architecture").

17(b): a data prioritization routine configured to assign a priority to data, wherein the prioritization occurs at least one of: in a transport layer of a network communications protocol stack of a data communication system, and at a top of the transport layer of the network communications protocol stack of the data communication system;—Juniper makes, uses, sells, and/or offers to sell a non-transitory computer-readable medium including a set of instructions comprising a data prioritization routine configured to assign a priority to data, where the prioritization occurs at least in a transport layer of a network communications protocol stack of a data communication system (e.g., the transport layer which includes TCP, and/or application layer). For instance, the Accused '028 Products that operate with the SRC software are configured to assign a priority to data. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf. In particular, Juniper discloses that "[g]lobal and local parameters are assigned a type," and lists various "parameter types, the predefined parameters for each type, the policy object in which you can use the parameter type, and how the type is used." *Id.* at p. 106. Specifically, Juniper discloses a "packetLossPriority" parameter type with three different predefined parameters: "any_priority," "high_priority," and "low_priority." *Id.* at p. 111; *see also id.* at p. 116 (disclosing that "any_priority" "[s]ets packet loss priority to 'any'"); *id.* at p. 118 (disclosing that "high_priority" "[s]ets packet loss priority (PLP) to high"); *id.* at p. 121 (disclosing that "low_priority" "[s]ets packet loss priority to low"); *id.* at p. 87 (disclosing

that a "Loss priority" action "[a]ssigns a packet loss priority to packets that match the classify-traffic condition."). In this respect, the Accused '028 Products that operate with the SRC software are configured to assign a priority to data such that users can then "configure hierarchical policies to dynamically share unused bandwidth from high-priority traffic with lower priority traffic." *Id.* at p. 89. Indeed, as one specific example, Juniper explains that "a traffic flow may include video traffic and Internet traffic," and in such traffic flow, "[t]he video traffic would have a high priority, but during times when not all bandwidth allocated to video is in use, the Internet traffic can access the unused bandwidth." *Id.* Furthermore, Juniper discloses that the prioritization of data may occur at least at the transport layer of the network communications protocol stack. *See, e.g., id.* at p. 78 ("You can configure rate-limit profiles to provide . . . [a] TCP-friendly rate-limiting service that works in conjunction with TCP's native flow-control functionality."); *id.* at p. 113 (disclosing "protocol" parameter types including "tcp, udp"); *see also* https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-gprs-sctp.html (disclosing that TCP and UDP provides "transport layer" functions). Moreover, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture" in which the SRC software can "integrate with services found on the ***application layer*** of IMS [IP Multimedia Subsystem]." https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html. An example of an ETSI-TISPAN Architecture is illustrated in the screenshot below, where the SRC software operates in the "RACS Layer":



Id. According to Juniper, "[t]he RACS layer is the TISPAN next-generation network subsystem that is responsible for elements of policing control, including resource reservation and admission control in the access and aggregation networks," and "provides policy-based transport control services to applications." https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("RACS shall be able to change the Upstream and Downstream bandwidth available to a particular subscriber. Such changes may apply to all traffic classes offered to the subscriber or a subset of those classes."); *id.* at p. 13 ("The number of queues varies from one level to another: a priority queue dedicated for Voice traffic is configured at the VC level but not at the VP level."); *id.* at p. 8 ("In order to achieve these requirements the RACS needs to have an accurate and current knowledge of the available network resources in the transport layer . . ."); *id.* at p. 10 ("The NGN shall support a mechanism to apply the end-to-end QoS requirements to the transport layer in each domain between

connectivity end points.").

17(c): a network analysis routine configured to determine a status of a network;— Juniper makes, uses, sells, and/or offers to sell a non-transitory computer-readable medium including a set of instructions comprising a network analysis routine configured to determine a status of a network. For instance, the Accused '028 Products that operate with the SRC software include a network analysis routine configured to determine a status of a network at various times. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 88, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf (disclosing that a "Policer . . . [s]pecifies rate and burst size limits and the action taken if a packet exceeds those limits)"); *id.* at p. 89 ("The video traffic would have a high priority, but during times when not all bandwidth allocated to video is in use, the Internet traffic can access the unused bandwidth."), ("A rate-limit hierarchy is a defined series of rate limits that a packet traverses within a policy list. At each level in the hierarchy, the packet is evaluated and processed as configured."). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally comprises a network analysis routine configured to determine a status of a network. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("The NGN shall support resource monitoring mechanisms in order to determine the available network

resources (e.g. link bandwidth, port utilization, queue depth)."); *id.* at p. 8 ("The RACS needs also to have knowledge of the status of each network component (nodes and links) under its control."); *id.* at pp. 8-9 (disclosing "Resource monitoring information").

17(d): a mode selection routine configured to select at least one mode based at least in part on the status of the network; and;—Juniper makes, uses, sells, and/or offers to sell a non-transitory computer-readable medium including a set of instructions comprising a mode selection routine configured to select at least one mode based at least in part on the status of the network. For instance, the Accused '028 Products that operate with the SRC software include a mode selection routine configured to select at least one mode based at least in part on the status of the network. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 77, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("Policy management enables network service providers to configure services that customize the treatment of individual packet flows received on a subscriber's interface."); *id.* at p. 78 ("To configure rate limiting, you first create a rate-limit profile, which is a set of bandwidth attributes and associated actions. You next create a policy list with a rule that has rate limit as the action and associate a rate-limit profile with this rule."); *id.* at p. 80 ("Policies are made up of conditions and actions that cause the router to handle packets in a certain way."); *id.* at p. 89 ("SRC support for JunosE rate-limit hierarchies lets you configure hierarchical policies to dynamically share unused bandwidth from high-priority traffic with lower priority traffic."); *see also id.* at pp. 77-249 (disclosing policies to manage traffic). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally

requires a mode selection routine configured to select at least one mode based at least in part on the status of the network. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf at p. 6 ("The NGN shall support dynamic policy provisioning mechanisms in order to allow the change on demand of the policies applied to a single user access (e.g. change the maximum bandwidth of an ADSL access)."); *id.* at p. 10 ("RACS shall be able to activate and enforce existing policies governing the bandwidth available to a particular User. In addition to this, RACS shall also be able to dynamically define new policies based on information from a number of sources, including network devices and management systems, and implement these policies.").

17(e): a data communications routine configured to communicate the data based at least in part on the priority of the data and the status of the network, the data prioritization routine being configured to assign priority to the data based on prioritization rules, wherein the prioritization rules are selected based upon the selected mode, wherein the data is communicated at a transmission rate metered based at least in part on the status of the network.—Juniper makes, uses, sells, and/or offers to sell a non-transitory computer-readable medium including a set of instructions comprising a data communications routine configured to communicate the data based at least in part on the priority of the data and the status of the network, and where the data prioritization routine described above is configured to assign priority to the data based on prioritization rules that are selected based

upon the selected at least one mode, and where the data is communicated at a transmission rate metered based at least in part on the status of the network. For instance, the Accused '028 Products that operate with the SRC software includes a data communications routine and data prioritization routine configured with such capabilities. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf at p. 78 ("You can configure rate-limit profiles to provide: A variety of services, including tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values and hard-limit service where a fixed bandwidth limit is applied to a traffic flow"); *id.* at p. 80 ("Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next interface, apply rate and burst size limits, assign a forwarding class"); *id.* at pp. 82-83 ("Policing applies two types of rate limits on the traffic: Bandwidth—Number of bps permitted, on average," and "Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit."); *id.* at p. 90 ("Traffic is transmitted depending on the rate limit set for the traffic flow. Preferred, high-priority traffic packets are dropped only as configured by the rate limit for that traffic flow. Lower priority traffic, however, can be dropped to keep the total traffic flow below a configured maximum limit."). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires a data communications routine and data prioritization routine configured with capabilities recited above. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-

mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 10, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("As a key part of an NGN's ability to offer QoS, RACS shall be able to activate and enforce existing policies governing the bandwidth available to a particular User."), ("RACS shall be able to change the Upstream and Downstream bandwidth available to a particular subscriber. Such changes may apply to all traffic classes offered to the subscriber or a subset of those classes."); *id.* at p. 8 ("Management of application QoS requirements where a number of services are being provided over individual links requires knowledge of the available bandwidth on the link."); *id.* at p. 9 ("In addition RACS may be able to derive some information by processing the available data (e.g. to calculate the current available link bandwidth from the total link bandwidth figure by maintaining knowledge of the current utilization of resources).").

72. Additionally, Defendant Juniper has been and/or currently is an active inducer of infringement of the '028 Patent under 35 U.S.C. § 271(b) and a contributory infringer of the '028 Patent under 35 U.S.C. § 271(c).

73. Juniper knew of the '028 Patent, or at least should have known of the '028 Patent, but was willfully blind to its existence. On information and belief, Juniper has had actual knowledge of the '028 Patent since at least as early as the filing and/or service of this Complaint.

74. Juniper has provided the Accused '028 Products to its customers and, on information and belief, instructions to (i) use the Accused '028 Products in an infringing manner and/or (ii)

make an infringing device, while being on notice of (or willfully blind to) the '028 Patent and Juniper's infringement. Therefore, on information and belief, Juniper knew or should have known of the '028 Patent and of its own infringing acts, or deliberately took steps to avoid learning of those facts.

75. Juniper knowingly and intentionally encourages and aids at least its end-user customers to directly infringe the '028 Patent.

76. Juniper's end-user customers directly infringe at least one or more claims of the '028 Patent by using the Accused '028 Products in their intended manner to infringe. Juniper induces such infringement by providing the Accused '028 Products and instructions to enable and facilitate infringement, knowing of, or being willfully blind to the existence of, the '028 Patent. On information and belief, Juniper specifically intends that its actions will result in infringement of one or more claims of the '028 Patent, or subjectively believe that their actions will result in infringement of the '028 Patent, but took deliberate actions to avoid learning of those facts, as set forth above.

77. Additionally, Juniper contributorily infringes at least one or more claims of the '028 Patent by providing the Accused '028 Products and/or software components thereof, that embody a material part of the claimed inventions of the '028 Patent, that are known by Juniper to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses. The Accused '028 Products are specially designed to infringe at least one or more claims of the '028 Patent, and their accused components have no substantial non-infringing uses. In particular, on information and belief, the software modules and code that implement and perform the infringing functionalities identified above are specially made and adapted to carry out said functionality and do not have any

substantial non-infringing uses.

78. At least as early as the filing and/or service of this Complaint, Juniper's infringement of the '028 Patent was and continues to be willful and deliberate, entitling Commstech to enhanced damages.

79. Additional allegations regarding Juniper's knowledge of the '028 Patent and willful infringement will likely have evidentiary support after a reasonable opportunity for discovery.

80. Juniper's infringement of the '028 Patent is exceptional and entitles Commstech to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

81. Commstech is in compliance with any applicable marking and/or notice provisions of 35 U.S.C. § 287 with respect to the '028 Patent.

82. Commstech is entitled to recover from Juniper all damages that Commstech has sustained as a result of Juniper's infringement of the '028 Patent, including, without limitation, a reasonable royalty.

COUNT III: INFRINGEMENT OF U.S. PATENT NO. 7,990,860

83. Commstech incorporates by reference and re-alleges paragraphs 42-54 of this Complaint as if fully set forth herein.

84. Defendant Juniper has infringed and is infringing, either literally or under the doctrine of equivalents, the '860 Patent in violation of 35 U.S.C. § 271 *et seq.*, directly and/or indirectly, by making, using, offering for sale, or selling in the United States, and/or importing into the United States without authority or license, products that operate with the Juniper Networks Session and Resource Control (SRC) software (e.g., C Series Controllers, including the C2000, C3000, C4000, and C5000 systems) (collectively

referred to herein as the "Accused '028 Products"), that infringe at least one or more claims of the '028 Patent. *See, e.g.,* https://www.juniper.net/documentation/en_US/src4.7/topics/concept/src-description.html.

85. As just one non-limiting example, set forth below (with claim language in bold and italics) is exemplary evidence of infringement of Claim 15 of the '860 Patent in connection with the Accused '860 Products. This description is based on publicly available information. Commstech reserves the right to modify this description, including, for example, on the basis of information about the Accused '860 Products that it obtains during discovery.

15(a): A processing device for communicating data, the processing device including:— Juniper makes, uses, sells, and/or offers to sell a processing device for communicating data in accordance with Claim 15. For instance, the Accused '860 Products that operate with the SRC software "can manage policies on Juniper Networks routers and cable modem termination system (CMTS) devices and can activate policies on other systems to provide end-to-end service quality." https://www.juniper.net/documentation/en_US/src4.7/topics/concept/src-description.html. Juniper also discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires a processing device for communicating data. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture.html.

15(b): a network analysis component of the processing device configured to: determine a network status from a plurality of network statuses based on analysis of network measurements, and—Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a network analysis component configured to determine a network status

from a plurality of network statuses based on analysis of network measurements. For instance, the Accused '860 Products that operate with the SRC software includes a network analysis component configured to determine a network status from a plurality of network statuses at various times. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 89, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("A rate-limit hierarchy is a defined series of rate limits that a packet traverses within a policy list. At each level in the hierarchy, the packet is evaluated and processed as configured."); *see also id.* at p. 88 (disclosing that a "Policer . . . [s]pecifies rate and burst size limits and the action taken if a packet exceeds those limits)"); *id.* at p. 89 ("The video traffic would have a high priority, but during times when not all bandwidth allocated to video is in use, the Internet traffic can access the unused bandwidth."). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires a network analysis component configured to determine a network status based on analysis of network measurements. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("The NGN shall support resource monitoring mechanisms in order to determine the available network resources (e.g. link bandwidth, port utilization, queue depth)."); *id.* at p. 8 ("Management of application QoS requirements where a number of services are being provided over

individual links requires knowledge of the available bandwidth on the link. . . . The RACS needs also to have knowledge of the status of each network component (nodes and links) under its control."); *id.* at pp. 8-9 (disclosing "Resource monitoring information").

15(c): a network analysis component of the processing device configured to: determine at least one of an effective link speed and a link proportion for at least one link;—Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a network analysis component configured to determine at least one of an effective link speed and a link proportion for at least one link. For instance, the Accused '860 Products that operate with the SRC software includes a network analysis component configured to determine either an effective link speed or a link proportion for at least on link. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf at pp. 82-83 ("Policing applies two types of rate limits on the traffic: Bandwidth—Number of bps permitted, on average," and "Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit."); *id.* at p. 80 ("Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next interface, apply rate and burst size limits, assign a forwarding class"); *id.* at p. 90 ("Traffic is transmitted depending on the rate limit set for the traffic flow. Preferred, high-priority traffic packets are dropped only as configured by the rate limit for that traffic flow. Lower priority traffic, however, can be dropped to keep the total traffic flow below a configured maximum limit."); *id.* at p. 78 ("You can configure rate-limit profiles to provide: A variety of services, including tiered bandwidth service where traffic conforming to configured

bandwidth levels is treated differently than traffic that exceeds the configured values and hard-limit service where a fixed bandwidth limit is applied to a traffic flow"). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires a network analysis component configured to determine at least one of an effective link speed and a link proportion for at least one link. *See, e.g.,* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 9, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("In addition RACS may be able to derive some information by processing the available data (e.g. to calculate the current available link bandwidth from the total link bandwidth figure by maintaining knowledge of the current utilization of resources).").

15(d): a mode selection component of the processing device configured to select a mode from a plurality of modes based on the determined network status, wherein each of the plurality of modes corresponds with at least one of the plurality of network statuses, wherein each of the plurality of modes comprises a user defined sequencing rule,— Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a mode selection component configured to select a mode from a plurality of modes based on the determined network status, where each of the plurality of modes corresponds with at least one of the plurality of network statuses, and where each of the plurality of modes comprises a user defined sequencing rule. For instance, the Accused '860 Products operate with the SRC software includes a mode selection component configured to select at least one mode

from a plurality of modes based at least in part on the network status, where each of the plurality of modes corresponds with at least one of a plurality of network statuses, and where each of the plurality of modes comprises a user defined sequencing rule. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf at p. 77 ("Policy management enables network service providers to configure services that customize the treatment of individual packet flows received on a subscriber's interface."); *id.* at p. 78 ("To configure rate limiting, you first create a rate-limit profile, which is a set of bandwidth attributes and associated actions. You next create a policy list with a rule that has rate limit as the action and associate a rate-limit profile with this rule."); *id.* at p. 80 ("Policies are made up of conditions and actions that cause the router to handle packets in a certain way."); *id.* at p. 89 ("SRC support for JunosE rate-limit hierarchies lets you configure hierarchical policies to dynamically share unused bandwidth from high-priority traffic with lower priority traffic."); *see also id.* at pp. 77-249 (disclosing policies to manage traffic). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which requires such a mode selection component recited above. *See* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("The NGN shall support dynamic policy provisioning mechanisms in order to allow the change on demand of the

policies applied to a single user access (e.g. change the maximum bandwidth of an ADSL access)."); *id.* at p. 10 ("RACS shall be able to activate and enforce existing policies governing the bandwidth available to a particular User. In addition to this, RACS shall also be able to dynamically define new policies based on information from a number of sources, including network devices and management systems, and implement these policies."); *id.* at p. 7 ("The policies to be changed are an operator choice . . .").

15(e): a data prioritization component of the processing device configured to prioritize data by assigning a priority to the data, wherein the prioritization component includes a sequencing component configured to sequence the data based at least in part on the user defined sequencing rule of the selected mode;—Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a data prioritization component configured to prioritize data by assigning a priority to the data, where the prioritization component includes a sequencing component configured to sequence the data based at least in part on the user defined sequencing rule of the selected mode. For instance, the Accused '860 Products that operate with the SRC software include such a data prioritization component. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 78, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("You can configure rate-limit profiles to provide: A variety of services, including tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values and hard-limit service where a fixed bandwidth limit is applied to a traffic flow"); *id.* at p. 80 ("Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next

interface, apply rate and burst size limits, assign a forwarding class"); *id.* at pp. 82-83 ("Policing applies two types of rate limits on the traffic: Bandwidth—Number of bps permitted, on average," and "Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit."); *id.* at p. 90 ("Traffic is transmitted depending on the rate limit set for the traffic flow. Preferred, high-priority traffic packets are dropped only as configured by the rate limit for that traffic flow. Lower priority traffic, however, can be dropped to keep the total traffic flow below a configured maximum limit."). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires such a data prioritization component recited above. *See, e.g.,* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Tele communications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 10, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("As a key part of an NGN's ability to offer QoS, RACS shall be able to activate and enforce existing policies governing the bandwidth available to a particular User."), ("RACS shall be able to change the Upstream and Downstream bandwidth available to a particular subscriber. Such changes may apply to all traffic classes offered to the subscriber or a subset of those classes."); *id.* at p. 8 ("Management of application QoS requirements where a number of services are being provided over individual links requires knowledge of the available bandwidth on the link."); *id.* at p. 9 ("In addition RACS may be able to derive some information by processing the available data (e.g. to calculate the current available link bandwidth from the total link bandwidth figure by maintaining knowledge

of the current utilization of resources)."); *id.* at p. 13 ("The number of queues varies from one level to another: a priority queue dedicated for Voice traffic is configured at the VC level but not at the VP level.").

15(f): a data metering component of the processing device configured to: meter inbound data by shaping the inbound data for the at least one link, and meter outbound data by policing the outbound data for the at least one link; and —Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a data metering component configured to meter inbound data by shaping the inbound data for the at least one link, and meter outbound data by policing the outbound data for the at least one link. For instance, the Accused '860 Products that operate with the SRC software include a data metering component configured to shape data packets. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 245, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("Traffic-shape actions specify the maximum rate of traffic transmitted on an interface. You can create traffic-shape actions in Junos OS shaping policy rules."); *id.* at p. 88 (disclosing the same). In this respect, the Accused '860 Products are configured to meter inbound data by shaping the inbound data. The Accused '860 Products that operate with the SRC software also include a data metering component configured to police data packets. *See e.g., id.* at p. 221 ("The policer action specifies rate and burst size limits and the action taken if a packet exceeds those limits."); *id.* at p. 88 (disclosing the same). In this respect, the Accused '860 Products are configured to meter outbound data by policing the outbound data. Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which

generally requires a data metering component configured to meter inbound data by shaping the inbound data for the at least one link, and meter outbound data by policing the outbound data for the at least one link. https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 12, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("In fact such mechanisms impact on the quality of the bearer flows received no matter which traffic conditioning policies you enforce both on the IP edge an access node."); *id.* p. 13 ("According to this scenario, QoS Reporting mechanism could help RACS to be informed of the un-managed traffic entering the network under its control and accordingly react. As soon as QoS reports degrade, RACS shall for example lower the available bandwidth."); *id.* at p. 10 ("RACS shall support provisioning and configuration of policies to be used to guarantee the requested QoS level. This includes to dynamically create/update/remove/query/activate/de-activate policies.").

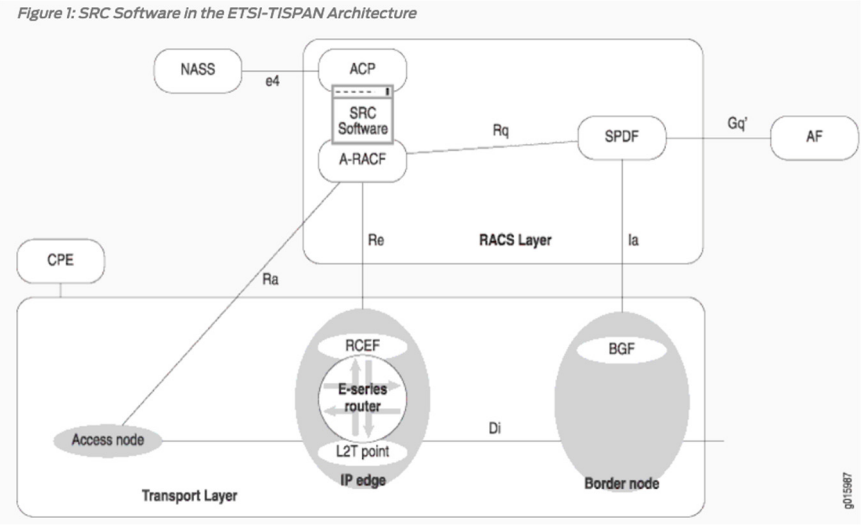
15(g): a data communication component of the processing device configured to communicate the data based at least in part on at least one of: the priority of the data, the effective link speed, and the link proportion;—Juniper makes, uses, sells, and/or offers to sell a processing device that comprises a data communication component configured to communicate the data based at least in part on the priority of the data, the effective link speed, and/or the link proportion. For instance, the Accused '860 Products that operate with the SRC software include such a data communications component. *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 78, *available at*

https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("You can configure rate-limit profiles to provide: A variety of services, including tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values and hard-limit service where a fixed bandwidth limit is applied to a traffic flow"); *id.* at p. 80 ("Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next interface, apply rate and burst size limits, assign a forwarding class"); *id.* at pp. 82-83 ("Policing applies two types of rate limits on the traffic: Bandwidth—Number of bps permitted, on average," and "Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit."); *id.* at p. 90 ("Traffic is transmitted depending on the rate limit set for the traffic flow. Preferred, high-priority traffic packets are dropped only as configured by the rate limit for that traffic flow. Lower priority traffic, however, can be dropped to keep the total traffic flow below a configured maximum limit."). Moreover, as noted above, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture," which generally requires a data communication component configured to communicate the data based at least in part on the priority of the data, the effective link speed, and/or the link proportion. *See, e.g.,* https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 10, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("RACS shall support provisioning and configuration of policies to be used to

guarantee the requested QoS level."), ("RACS shall be able to change the Upstream and Downstream bandwidth available to a particular subscriber. Such changes may apply to all traffic classes offered to the subscriber or a subset of those classes."); *id.* at p. 8 ("Management of application QoS requirements where a number of services are being provided over individual links requires knowledge of the available bandwidth on the link."); *id.* at p. 9 ("In addition RACS may be able to derive some information by processing the available data (e.g. to calculate the current available link bandwidth from the total link bandwidth figure by maintaining knowledge of the current utilization of resources).").

15(h): wherein at least the data prioritization component is configured to operate at a transport layer of a protocol stack.—Juniper discloses that the data prioritization component is configured to operate at transport layer of a protocol stack (e.g., the transport layer which includes TCP, and/or application layer). *See, e.g.,* SRC PE Software Services and Policies Guide, Release 4.12.x (Oct. 2018), p. 78, *available at* https://www.juniper.net/documentation/en_US/src4.12/information-products/topic-collections/services-policies/book-services-policies.pdf ("You can configure rate-limit profiles to provide . . . [a] TCP-friendly rate-limiting service that works in conjunction with TCP's native flow-control functionality."); *id.* at p. 113 (disclosing "protocol" parameter types including "tcp, udp"); *see also* https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-gprs-sctp.html (disclosing that TCP and UDP provides "transport layer" functions). Moreover, Juniper discloses that the SRC software can operate in the "ETSI-TISPAN Architecture" in which the SRC software can "integrate with services found on the ***application layer*** of IMS [IP Multimedia Subsystem]." https://www.juniper.net/

documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture-src.html. An example of an ETSI-TISPAN Architecture is illustrated in the screenshot below, where the SRC software operates in the "RACS Layer":



Id. According to Juniper, "[t]he RACS layer is the TISPAN next-generation network subsystem that is responsible for elements of policing control, including resource reservation and admission control in the access and aggregation networks," and "provides policy-based transport control services to applications." https://www.juniper.net/documentation/en_US/src4.8/topics/reference/general/service-mgm-ims-architecture.html; *see also* Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN, ETSI TS 181 018 V2.0.0, p. 6, *available at* https://www.etsi.org/deliver/etsi_ts/181000_181099/181018/02.00.00_60/ts_181018v020000p.pdf ("RACS shall be able to change the Upstream and Downstream bandwidth available to a particular subscriber. Such changes may apply to all traffic classes offered to the subscriber or a subset of those classes."); *id.* at p. 13 ("The number of queues varies from one level to another: a priority queue dedicated for Voice traffic is configured at the VC level but not at the VP level."); *id.* at p. 8 ("In

order to achieve these requirements the RACS needs to have an accurate and current knowledge of the available network resources in the transport layer . . ."); *id.* at p. 10 ("The NGN shall support a mechanism to apply the end-to-end QoS requirements to the transport layer in each domain between connectivity end points.").

86. Additionally, Defendant Juniper has been and/or currently is an active inducer of infringement of the '860 Patent under 35 U.S.C. § 271(b) and a contributory infringer of the '860 Patent under 35 U.S.C. § 271(c).

87. Juniper knew of the '860 Patent, or at least should have known of the '860 Patent, but was willfully blind to its existence. On information and belief, Juniper has had actual knowledge of the '860 Patent since at least as early as the filing and/or service of this Complaint.

88. Juniper has provided the Accused '860 Products to its customers and, on information and belief, instructions to use the Accused '860 Products in an infringing manner while being on notice of (or willfully blind to) the '860 Patent and Juniper's infringement. Therefore, on information and belief, Juniper knew or should have known of the '860 Patent and of its own infringing acts, or deliberately took steps to avoid learning of those facts.

89. Juniper knowingly and intentionally encourages and aids at least its end-user customers to directly infringe the '860 Patent.

90. Juniper's end-user customers directly infringe at least one or more claims of the '860 Patent by using the Accused '860 Products in their intended manner to infringe. Juniper induces such infringement by providing the Accused '860 Products and instructions to enable and facilitate infringement, knowing of, or being willfully blind to the existence of, the '860 Patent. On information and belief, Juniper specifically intends that its actions will result

in infringement of at least one or more claims of the '860 Patent, or subjectively believe that their actions will result in infringement of the '860 Patent, but took deliberate actions to avoid learning of those facts, as set forth above.

91. Additionally, Juniper contributorily infringes at least one or more claims of the '860 Patent by providing the Accused '860 Products and/or software components thereof, that embody a material part of the claimed inventions of the '860 Patent, that are known by Juniper to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses. The Accused '860 Products are specially designed to infringe at least one or more claims of the '860 Patent, and their accused components have no substantial non-infringing uses. In particular, on information and belief, the software modules and code that implement and perform the infringing functionalities identified above are specially made and adapted to carry out said functionality and do not have any substantial non-infringing uses.

92. At least as early as the filing and/or service of this Complaint, Juniper's infringement of the '860 Patent was and continues to be willful and deliberate, entitling Commstech to enhanced damages.

93. Additional allegations regarding Juniper's knowledge of the '860 Patent and willful infringement will likely have evidentiary support after a reasonable opportunity for discovery.

94. Juniper's infringement of the '860 Patent is exceptional and entitles Commstech to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

95. Commstech is in compliance with any applicable marking and/or notice provisions of 35 U.S.C. § 287 with respect to the '860 Patent.

96. Commstech is entitled to recover from Juniper all damages that Commstech has sustained as a result of Juniper's infringement of the '860 Patent, including, without limitation, a reasonable royalty.

PRAYER FOR RELIEF

WHEREFORE, Commstech respectfully requests:

A. That Judgment be entered that Juniper has infringed at least one or more claims of the Patents-in-Suit, directly and/or indirectly, literally and/or under the doctrine of equivalents;

B. An award of damages sufficient to compensate Commstech for Juniper's infringement under 35 U.S.C. § 284, including an enhancement of damages on account of Juniper's willful infringement;

C. That the case be found exceptional under 35 U.S.C. § 285 and that Commstech be awarded its reasonable attorneys' fees;

D. Costs and expenses in this action;

E. An award of prejudgment and post-judgment interest; and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Commstech respectfully demands a trial by jury on all issues triable by jury.

Respectfully submitted,

Dated: July 23, 2019

LEE SULLIVAN SHEA & SMITH LLP
and
TOLER LAW GROUP, PC

By: */s/ Aakash S. Parekh*

Aakash S. Parekh, Texas Bar No. 24059133
aparekh@tlgiplaw.com
TOLER LAW GROUP PC
8500 Bluffstone Cove, Suite A201
Austin, TX 78759

George I. Lee (pro hac vice)
lee@ls3ip.com
Sean M. Sullivan (pro hac vice)
sullivan@ls3ip.com
Michael P. Boyea (pro hac vice)
boyea@ls3ip.com
Cole B. Richter (pro hac vice)
richter@ls3ip.com
Jae Y. Pak (pro hac vice)
pak@ls3ip.com
LEE SULLIVAN SHEA & SMITH LLP
656 West Randolph Street, Floor 5W
Chicago, IL 60661
Tel: (312) 754-0002
Fax: (312) 754-0003

Attorneys for Plaintiff
Commstech Holdings LLC