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

HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD., and HUAWEI DIGITAL TECHNOLOGIES (CHENGDU) CO., LTD. Plaintiffs, vs. **VERIZON COMMUNICATIONS, INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS, and VERIZON BUSINESS NETWORK SERVICES, INC.** Defendants.	**Civil Action No. 6:20-cv-00090** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Huawei Technologies Co. Ltd., Huawei Device Co., Ltd., and Huawei Digital Technologies (Chengdu) Co., Ltd. (collectively, "Huawei" or "Plaintiffs") hereby allege as follows against Verizon Communications, Inc., Cellco Partnership d/b/a Verizon Wireless, and Verizon Business Network Services, Inc. (collectively "Verizon" or "Defendants"):

THE PARTIES

1. Plaintiff Huawei Technologies Co., Ltd. ("Huawei Technologies") is a Chinese corporation with its principal place of business at Bantian, Longgang District, Shenzhen, People's Republic of China.

2. Plaintiff Huawei Device Co., Ltd. ("Huawei Device") is a Chinese corporation with its principal place of business at Songshan Lake Science and Technology Industrial Zone, Dongguan, Guangdong, People's Republic of China.

3. Plaintiff Huawei Digital Technologies (Chengdu) Co., Ltd. ("Huawei Digital") is a Chinese corporation with its principal place of business at No.1899 Xiyuan Avenue, High-tech Zone, Chengdu, Sichuan, People's Republic of China.

4. Defendant Verizon Communications Inc. ("Verizon Communications") is a Delaware corporation with a principal place of business at 1095 Avenue of the Americas, New York, New York 10036. Verizon Communications may be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

5. Defendant Cellco Partnership d/b/a Verizon Wireless ("Cellco Partnership") is a Delaware partnership with its principal place of business at 1 Verizon Way, Basking Ridge, New Jersey 07920. Cellco Partnership is wholly owned by its corporate parent, Verizon Communications, and together with Verizon Communications is collectively referred to as "Verizon Wireless." Cellco Partnership may be served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

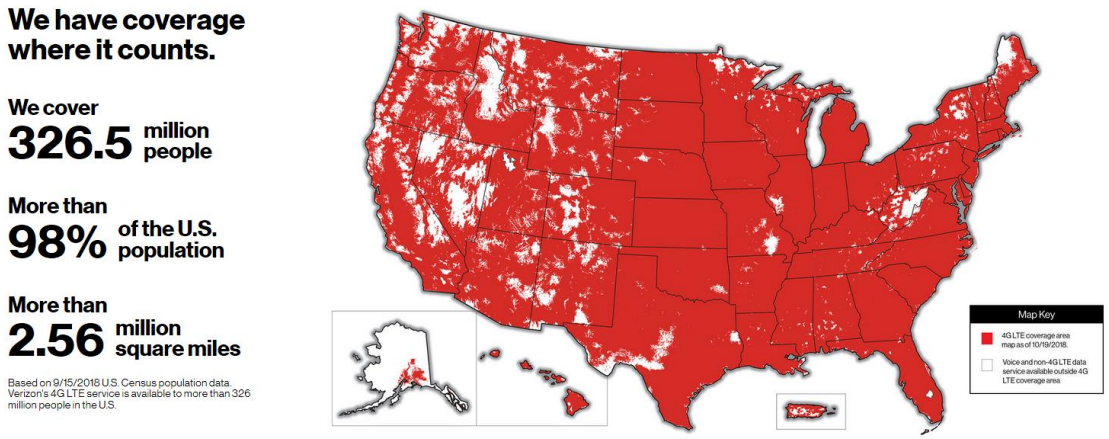
6. Defendant Verizon Business Network Services, Inc. ("Verizon Business") is a Delaware corporation with a place of business in at least San Antonio, Texas. Verizon Business may be served through its registered agent for service of process in Texas at CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

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

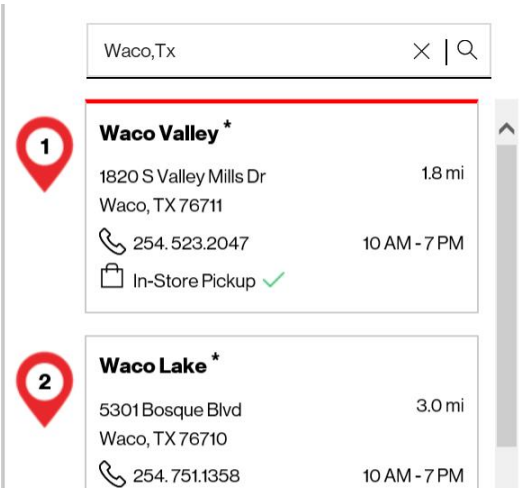
8. The patents-at-issue in this action are U.S. Patent Nos. 7,965,709 ("the '709 Patent"), 8,154,986 ("the '986 Patent"), 10,027,693 ("the '693 Patent"), 7,609,288 ("the '288 Patent"), 9,521,366 ("the '366 Patent"), 7,715,832 ("the '832 Patent"), and 8,761,839 ("the '839 Patent") (collectively, the "Asserted Patents").

9. The Court has personal jurisdiction over Verizon at least because it has continuous business contacts in the State of Texas and in this District. Verizon has engaged in business activities including transacting business in this District and purposefully directing its business activities, including the provision of infringing communications networks and services, and the use, marketing, sale or offer for sale of mobile devices and services, such as Verizon's Smart Family Service and One Talk Service and Cisco's Webex service in this District, and the sale or offer for sale of services and goods to this District to aid, abet, or contribute to the infringement of third parties in this District. For example, Verizon—either directly or through those acting on its behalf—offers infringing communications networks and services in this District, as shown, e.g., at https://www.verizonwireless.com/featured/better-matters/:



As another example, Verizon—either directly or through those acting on its behalf—has stores and/or authorized retailers in this District in which infringing communications networks and services are offered for sale. *See* https://www.verizonwireless.com/stores/texas/. For example,

Verizon through each of the named parties has various places of business within this District, including data centers at 222 Rotary, San Antonio, TX, 78202 and 2525 Ridgepoint Drive, Austin TX, 78754, and numerous retail stores including the following examples in Waco:



https://www.verizonwireless.com/stores/storesearchresults/?lat=31.549333&long=-97.14666950000003&q=waco%2Ctx#/Search. Verizon also has a call center in El Paso. *See* https://www.verizon.com/about/careers/we-are-global#featured-region-6753. Verizon also offers enterprise products and services to Texas "[s]tate agencies, cities, counties, public school districts, and universities" through the Texas Department of Information Resources in Austin. *See, e.g.*, https://enterprise.verizon.com/solutions/public-sector/state-local/contracts/texas/; https://dir.texas.gov/; *see also* https://www.marketwatch.com/press-release/verizon-invested-more-than-348-million-in-texas-wireline-telecommunications-infrastructure-in-2013-2014-03-31 ("Verizon Enterprise Solutions oversees all of Verizon's solutions for large-business and government customers in Texas and globally . . .").

10. Venue is proper in this judicial district under 28 U.S.C. §§ 1391 and 1400(b). As shown above, Verizon has multiple regular and established place of business in this District and is engaged in activities including: transacting business in this district and purposefully directing

its business activities, including the installation, maintenance, and use of infringing communications networks, services, and other technologies in this District, and the sale or offer for sale of services and goods to this District to aid, abet, or contribute to the infringement of third parties in this District.

HUAWEI'S INNOVATION AND RESEARCH

11. Founded in 1987, Huawei is a global leader of information and communication technology ("ICT") solutions. Continuously innovating to meet customer needs, Huawei is committed to enhancing customer experience and creating maximum value for telecommunications carriers, enterprises, and consumers. Huawei's telecom network equipment, IT products and solutions, and smart devices, such as telepresence products, transport and core network equipment, fixed and radio access products, and fiber infrastructure products are deployed and used in 170 countries and regions and serve over one-third of the world's population. Huawei is also a leader in research, innovation, and implementation of future networks.

12. Indeed, R&D has been at the core of Huawei's business. Huawei started its business reselling third-party telecommunication products, but shortly thereafter Huawei chose to shift its focus by expanding its own R&D and developing its own products. Since then, Huawei has heavily invested in R&D and routinely spends no less than 10% of its annual revenue on innovation. For example, Huawei ranks fifth globally in *The 2019 European Union Industrial R&D Investment Scoreboard*, a report published by the European Commission.

13. Over the past decade through 2018, Huawei has invested nearly $73 billion in research and development in total. In the next five years, Huawei plans to invest $100 billion. Huawei's R&D efforts are now focused on addressing customer needs, as well as long-term technology research and standardization. In pursuit of these goals, Huawei has assembled a

global team with thousands of scientists and top engineers in the United States, Europe, and Japan, to staff its R&D department. Globally, Huawei has 14 R&D Institutes and Centers, 36 joint innovation centers and 45 training centers. Indeed, about 45% of Huawei's global workforce – over 80,000 employees in 2018 – works in the Research and Development Department. Huawei's innovations are central to important cutting-edge technologies, including ultra-broadband solutions, such as 100G super-fast data transmission, LTE, and WiMAX wireless networks.

14. As a result of Huawei's substantial dedication to R&D in the telecommunications industry over the past three decades, Huawei has contributed to the evolution of telecommunication networks from the Wired Communication Age, into the Wireless Age, and from 2G, 3G, and 4G to advanced 5G networks.

15. Over the course of this evolution, Huawei has been responsible for several of the industry's notable achievements and milestones. In the Wired Communication Age, due to its heavy investment in R&D in its early years, Huawei successfully launched a new line of fixed network switch products in 1993, the centerpiece of which was the C&C 08 switching product, which proved to be a tremendous success in rural areas of China, with a rapid coverage of over 300 regional networks.

16. Entering the Wireless Age, Huawei launched the first-ever Global System for Mobile Communications ("GSM") infrastructure products engineered solely by a Chinese company in 1997. Three years later, Huawei's revenue had reached $1.9 billion, including $100 million from overseas sales. Along with great market success, Huawei has been significantly ahead of its competitors in bringing major innovations in cellular technology to market. Shortly after its success with distributed base stations, recognized as customer-centric innovations,

Huawei was the first infrastructure supplier to launch the unique SingleRAN technology in 2008, which is now the industry norm. The SingleRAN solution supports GSM, universal mobile telecommunications system ("UMTS"), code division multiple access ("CDMA"), WiMAX, and Long-Term Evolution ("LTE"), i.e., all relevant 2G, 3G, and 4G standards, and all in a common platform. In 2009, Huawei deployed the world's first commercial 4G LTE network in Oslo, Norway, sharing the first commercial 4G LTE network with Ericsson in TeliaSonera. In 2010, Huawei achieved the world's fastest LTE-A downlink speed, up to 1.2 Gbps at CTIA Wireless 2010 in Las Vegas, Nevada, and successfully demonstrated simultaneous voice calling and high definition video streaming over LTE and LTE-A networks for Cox Communications, the third-largest cable provider in the United States.

17. The above accomplishments and others earned Huawei the awards for "Best Contribution to R&D for LTE" and "Best Contribution to LTE Standards" at the LTE North America Awards in 2011. Huawei also won the "Most innovative service launch enabled by IMS" with its "Convergent Conference" solution at the 2012 IP Multimedia Subsystem ("IMS") World Forum, the "Best Integrated IMS Solution" award at the 2013 IMS World Forum, and the "Best VoLTE Product" for its end-to-end ("E2E") voice and video over LTE ("V2oLTE") solution and "Most Innovative Virtualized IMS Solution" for its Cloud IMS solution at the 2014 IMS World Forum in Barcelona, Spain.

18. At the LTE World Summit, Huawei also won numerous awards, such as the "Best LTE traffic management product" and "Innovation in HetNet development" awards in 2014, and the "Best NFV Innovation of the Year" and "Biggest Contribution to 5G Development" awards in 2015. Huawei was the only company that won two awards in both years.

19. After winning the "Best Managed Services Innovation Award" at Managed Services World Congress 2016, Huawei won the "Wireless Infrastructure Innovation" award and the "Cloud Innovation of the Year" award at the 2016 Telecoms Awards Ceremony in London for Operation Web Services ("OWS") due to Huawei's achievements in software defined operation research to enable ICT Managed Services. In 2017, Huawei won the Network Functions Virtualization ("NFV") Innovation Award for its NFV Integration Service at the World Communication Awards organized by Total Telecom.

20. In 2018, Huawei's RuralStar, WTTx, and PoleStar solutions respectively won the GSM Association's ("GSMA's") Best Mobile Innovation for Emerging Markets award, the International Telecommunication Union's ("ITU's") Global Corporate Award for Sustainable Development, and the GSMA's Outstanding Mobile Contribution to the United Nation Sustainable Development Goals in Asia award. Huawei's prefabricated modular data center solution and modular Uninterruptable Power Supply ("UPS") continue to hold the largest market share globally. Huawei also won Datacenter Dynamics' ("DCD's") global annual Living at the Edge award.

21. At Internet of Things ("IoT") Solutions World Congress 2018, Huawei's OceanConnect Internet of Vehicles ("IoV") Platform, which helped Groupe PSA become a leader in mobility services, won the award for Business Transformation.

22. Huawei was also awarded a First Class Progress in Science and Technology Prize for 2018 for unveiling the blade base station. Among other awards, Huawei has also been repeatedly named one of the Most Innovative Companies by Fast Company, and one of the World's 50 Most Innovative Firms by BCG.

23. Huawei has also won numerous awards and substantial industry recognition for its infrastructure and enterprise products, such as video conferencing and data communication products. As an example, Huawei was awarded the Frost & Sullivan Asia-Pacific Video Conferencing Endpoints Market Leadership Award at the 2018 Asia-Pacific Information and Communication Technologies ("ICT") awards ceremony. The award recognized Huawei's market leadership, technology and solution innovation, and customer value proposition in the video conference industry. As another example, Huawei's data communication products such as data center products including CloudEngine switches and controller were awarded Gartner Peer Insights Customers' Choice in 2019 and the "Best of Show Award" at Interop Tokyo in 2016, 2017, and 2018. And Huawei's Wi-Fi 6 products AirEngine AP, Router NetEngine 8000 and NetEngine 9000 400G were awarded the "Best of Show Award" grand prize at Interop Tokyo 2019.

24. Huawei has also won numerous awards and substantial industry recognition for its smartphones and other mobile devices. As an example, Huawei received the European Image and Sound Association ("EISA") Best Smartphone 2019-2020 award for Huawei's P30 Pro. The EISA recognized the P30 Pro's camera as being far beyond any of its competitors, including its low-light capabilities, portrait mode, and its ultra-wide and periscopic 5x telephoto lenses. Huawei also received the Technical Image Press Association ("TIPA") Best Photo Smartphone 2019 award for the P30 Pro. In December 2019, independent benchmark organization DxoMark Image Labs gave Huawei's Mate 30 Pro 5G the highest DXOMARK Camera score ever awarded, praising its image quality, autofocus, and zoom performance. Huawei smartphones received two awards from the GSMA at Mobile World Congress 2019: Huawei's Mate 20 Pro

won Best Smartphone and Huawei's Mate X foldable 5G smartphone won Best Connected Mobile Device.

25. During the past 20 years, Huawei has also endeavored to drive the mobile industry forward through collaborations on commercialization, innovation, and standardization. According to Current Analysis, Huawei is the clear overall leader in such efforts, due to the strength of its IT product portfolio, its broad variety of network solution options including high- and low-capacity offerings, and its range of power output levels and architectures. Huawei also invests in open source communities and partners with major industry players to innovate in emerging domains, such as cloud computing and the Internet of Things.

26. As a result of Huawei's commitment to innovation and significant long-term investment in R&D, Huawei has become one of the world's largest patent holders. As of December 31, 2019, Huawei holds more than 85,000 issued patents, covering all major jurisdictions of the world, including 40,000 Patents granted in the United States and Europe. Huawei's significant efforts in research and development demonstrate the value that Huawei places on innovation, and on sharing its efforts with the public, in return for a limited right to use its own inventions exclusively and/or to license its inventions to other companies willing to pay a reasonable royalty for their use.

VERIZON'S USE OF HUAWEI'S INNOVATIONS

27. Verizon has knowingly used, and is using, Huawei's patented technology without a license.

28. Verizon creates, promotes, uses, maintains, and provides access to infringing technologies and services ("Infringing Technologies & Services") that incorporate and/or utilize Huawei's patented technology, including through the utilization and incorporation of network infrastructure such as Cisco Integrated Service Routers, Aggregation Services Routers, Network

Convergence Systems, Nexus Switches, Catalyst Switches, and Clouds Services Router 1000v series, which facilitate communications throughout Verizon's networks. For example, Verizon's "Enterprise Solutions offers traditional circuit-based network services, and advanced networking solutions including Private IP, Ethernet, and Software-Defined Wide Area Network, along with our traditional voice services and advanced workforce productivity and customer contact center solutions." Verizon's 2019 Annual Report at 88.

29. Verizon also creates, promotes, uses, maintains, and provides access to its Infringing Technologies & Services that incorporate and/or utilize Huawei's patented technology through the utilization and incorporation of network infrastructure and services such as Juniper MX series routers and T series routers, SRX Series and/or virtualized SRX (vSRX) Services Gateways, which support Verizon's Infringing Technologies & Services.

30. Verizon also creates, promotes, uses, maintains, and provides access to its Infringing Technologies & Services that incorporate and/or utilize Huawei's patented technology through its distribution and/or reselling of services such as Cisco Webex, and distribution of applications such as the Smart Family application and the One Talk application.

31. Verizon has profited greatly from the Infringing Technologies & Services. *See* Verizon 2019 Annual Report at p. 12 ("Total Wireline segment operating revenues for the year ended December 31, 2018 totaled $29.8 billion . . . In 2018, Enterprise Solutions revenues were $8.8 billion, representing approximately 30% of Wireline's aggregate revenues.").

LICENSING NEGOTIATIONS

32. To protect its intellectual property rights, Huawei contacted Verizon on February 7, 2019 to discuss Verizon's need for a license to Huawei's patents. Huawei specifically identified patents from its portfolio and specific services offered by Verizon that infringed Huawei's patents, such as those at issue here.

33. Because of Huawei's notice, Verizon has known about at least the '709 Patent, the '986 Patent, and the '693 Patent at least as early as February 7, 2019.

34. Huawei then traveled from China and met in person with Verizon – in New York near Verizon's headquarters – on March 28, 2019 to discuss Verizon's need for a license to Huawei's patents. Huawei identified additional patents from its portfolio and services offered by Verizon that require a license to Huawei's patents.

35. On March 29, 2019, Huawei tried to move the licensing discussions forward in a cooperative manner by providing claim charts to Verizon. Those claim charts included the '709 Patent, the '986 Patent, the '693 Patent, the '288 Patent, the '366 Patent, and the '832 Patent.

36. Because of Huawei's notice, Verizon has known about the '288 Patent, the '366 Patent, and the '832 Patent at least as early as March 29, 2019. And Huawei provided additional notice of the '709 Patent, the '986 Patent, and the '693 Patent at least as early as March 29, 2019.

37. On June 4th and 5th, 2019, Huawei representatives from China again met in-person with representatives from Verizon in New York and discussed claim charts selected by Verizon concerning a wide variety of technologies.

38. On June 18, 2019, Huawei representatives spoke with Verizon representatives via telephone. Verizon committed to identifying issues and concerns regarding the claim charts discussed during the June 4th and 5th meeting. Huawei agreed to travel for yet another in-person meeting in New York, and Verizon advised it would identify more Huawei claim charts to be discussed at their next meeting.

39. On July 30-31, 2019, September 3-4, 2019, and November 21-22, 2019, Huawei representatives from China met in-person with representatives from Verizon in New York and

discussed the additional claim charts. Those claim charts included the '709 Patent, discussed on July 31, and the '832 Patent, discussed on September 4.

40. On January 21, 2020, Huawei representatives from China again met in-person with representatives from Verizon in New York, but there was no substantial progress and thus no licensing agreement was reached.

41. Because Verizon has not accepted Huawei's numerous flexible approaches during the year-long negotiations, Huawei is compelled to now enforce its patent rights through this lawsuit.

COUNT I: INFRINGEMENT OF PATENT NO. 7,965,709

42. Huawei realleges and incorporates by reference Paragraphs 1-41 above, as if fully set forth herein.

43. The U.S. Patent Office duly and properly issued the '709 Patent, entitled "Bridge Forwarding Method and Apparatus," on June 21, 2011. Huawei Technologies is the assignee of all right, title, and interest in and to the '709 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the '709 Patent is valid and enforceable. A true and correct copy of the '709 Patent is attached hereto as Exhibit A.

44. The '709 Patent provides novel, useful and more effective and efficient techniques for bridge forwarding between multiple Virtual Local Area Networks ("VLANs") that overcome the problems of the prior art and thereby improve the functioning of computer and network equipment.

45. The '709 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problem of "bridge forwarding of [] Ethernet frames between multiple VLANs." The '709 Patent at Abstract. The background section of the '709 Patent explains in reference to prior art bridge

forwarding that there are "two approaches for forwarding the frames of the Ethernet at present: Layer 2 Ethernet bridge and Layer 3 IP route." *Id.* at 1:13-15. "FIG. 1 is a flow chart illustrating the bridge forwarding within one VLAN in the prior art." *Id.* at 1:32-33. Figure 1 is shown below:

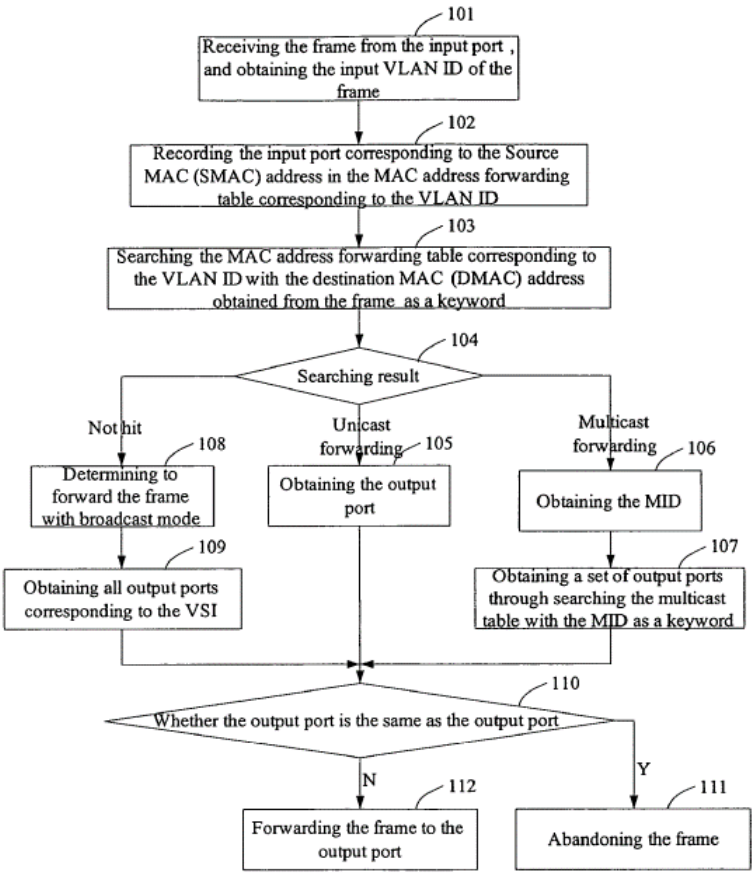


Fig.1

46. In reference to the prior art, the '709 Patent explains that "the relationship between the VLAN and the Virtual Switching Instance ("VSI") is [a] one-to-one relationship," which means "the multiple-to-one relationship between multiple VLANs with one VSI is not supported, the Ethernet frames can only be forwarded within one VLAN by means of Layer 2 Ethernet bridge forwarding." *Id.* at 2:7-12. In reference to prior art methods for bridge forwarding across VLANs, the '709 discloses that "[i]f the frames need to be forwarded across

VLANs, the Layer 3 IP routing must be adopted." *Id.* at 2:12-13. The '709 Patent further explains that in the prior art, "the Ethernet frames can only be broadcasted to one VLAN by means of bridge forwarding, and broadcasting to multiple VLANs by means of bridge forwarding is not supported." *Id.* at 2:13-16. As such, broadcasting to multiple VLANs using bridge forwarding was not supported. Thus, prior to the inventions of the '709 Patent, there existed a need for a more thorough and efficient method of bridge forwarding between multiple VLANs.

47. The inventions of the '709 Patent provide technical solutions to the problems in the prior art described above. The '709 Patent seeks to address these and other problems in the prior art by providing a non-conventional, novel solution that allows the extension of bridge forwarding to provide cross-VLAN bridge forwarding of frames. The '709 Patent explains that "the cross-VLAN bridge forwarding of frames is realized by establishing the relationship between the {Port, VLAN} and the VSI and implementing bridge forwarding of frames among different {Port, VLAN}s, and the multiple-to-one relationship between multiple VLANs with one VSI." *Id.* at 3:23-32.

48. The inventions of the '709 Patent provide technical solutions to the problems in the prior art described above. The '709 Patent describes, for example, "a bridge forwarding method and a bridge forwarding apparatus to realize cross-VLAN bridge forwarding of frames." *Id.* at 2:20-22. The '709 Patent next describes supporting the multiple-to-one relationship between multiple VLANs with one VSI. The '709 Patent then describes source port filtering to prevent forwarding loops. The '709 Patent also discloses that "bridge forwarding among multi-layer VLAN IDs is supported by the present invention," which is not present in the prior art. *Id.* at 3:36-38.

49. The inventions of the '709 Patent improve computer and network equipment functionality by improving and solving problems in a computer or networked device's capability of performing bridge forwarding between multiple VLANs with better efficiency. The inventions of the '709 Patent provide a computer-based solution to a computer-specific problem. The inventions of the '709 Patent are improvements over the prior art and other techniques for bridge forwarding, and the '709 Patent enables a combination of features not present in the prior art and other techniques.

50. For example, the inventions of the '709 Patent provide for improved computer and network operation by enabling bridge forwarding to more efficiently use resources and prevent forwarding loops. The specification discloses that "during the process of frame forwarding, whether the input/output port is the same as the input/output VLAN ID is determined, so source port filtering can be implemented effectively to prevent forwarding loops." *Id.* at 3:33-36.

51. As another example, the inventions of the '709 Patent provide for improved computer and network operation by providing enhanced methods for bridge forwarding that include cross-VLAN bridge forwarding of frames. *E.g.*, *id.* at Abstract.

52. The claims of the '709 Patent contain an inventive concept to improve the functioning of computers and other networked devices. Claims 1, 4, 7, 16-18, 21, and 23 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the '709 Patent application was filed. These ordered combinations are set forth in claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent. The ordered combinations of elements in claim 1, 4, 7, 16-18, 21, and 23 were not well understood, routine or conventional at the time the '709 Patent application was filed. The ordered combinations of the

inventions of claims 1, 4, 7, 16-18, 21, and 23 are practical, particular, non-conventional and non-generic techniques of bridge forwarding.

53. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Cisco routers supporting Ethernet Flow Point functionality, including but not limited to the Cisco ASR900 series, ASR920 series, ASR1000 series, ASR9000 series, Catalyst 6500 series, ISR 4000 series, and CSR 1000v series routers ("Cisco EFP Products").

54. Cisco EFP Products are operable to forward frames between multiple VLANs. *See, e.g.*, https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-3/lxvpn/configuration/guide/b-l2vpn-cg53xasr9k.pdf; https://www.verizon.com/about/news/vzw/2010/01/pr2010-01-07a.

55. Cisco EFP Products are operable to receive, via an input port, a frame associated with a first virtual local area network (VLAN). For example, the Cisco ASR9000 series router is configured to support Ethernet Flow Point. *See, e.g.*, https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-3/lxvpn/configuration/guide/b-l2vpn-cg53xasr9k.pdf at 11 ("An Ethernet Flow Point (EFP) is a Layer 2 logical subinterface used to classify traffic under a physical or a bundle interface"). "You can bridge or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs." *Id.* The Cisco ASR9000 series router can be configured to

define data-forwarding behavior. *Id.* at 15 ("The EFP can be used to designate the frames belonging to a particular Ethernet flow forwarded in the data path").

56. Cisco EFP Products are operable to obtain an input VLAN identifier (ID) representing the first VLAN and a destination media access control (MAC) address of the received frame. For example, the configuration guide discloses:

> An EFP can be regarded as an instantiation of a particular service. An EFP is defined by a set of filters. These filters are applied to all the ingress traffic to classify the frames that belong to a particular EFP. An EFP *filter* is a set of entries, where each entry looks similar to the start of a packet (ignoring source/destination MAC address). Each entry usually contains 0, 1 or 2 VLAN tags. A packet that starts with the same tags as an entry in the filter is said to match the filter; if the start of the packet does not correspond to any entry in the filter then the packet does not match the filter.

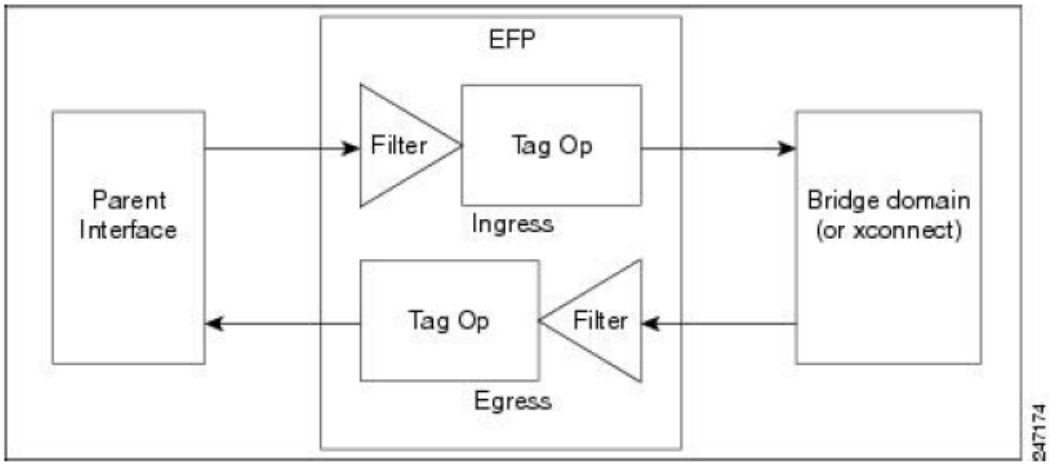
Id. at 11.

57. As a further example, "[t]he EFP identifies frames belonging to a particular flow on a given port, independent of their Ethernet encapsulation. . . . The frames can be matched to an EFP using: VLAN tag or tags." *Id.* at 13. The configuration guide further discloses several forwarding cases, including: "L2 Switched Service (Bridging)—The EFP is mapped to a bridge domain, where frames are switched based on their destination MAC address." *Id.* at 15-16.

58. Cisco EFP Products are operable to determine a Virtual Switching Instance (VSI) corresponding to the combination of the input port and the input VLAN ID. For example, "[a]n Ethernet Flow Point (EFP) is a Layer 2 logical subinterface used to classify traffic under a physical or a bundle interface. A physical interface can be a Gigabit Ethernet 0/0/0/1 or a 10 Gigabit Ethernet 0/0/0/0 interface and has ports on the line card. A bundle interface is a virtual interface, created by grouping physical interfaces together." *Id.* at 11. The configuration guide discloses that "[a]n EFP subinterface is configured to specify which traffic on ingress is vectored to that EFP. This is done by specifying a VLAN, range of VLANs, or QinQ tagging to match

against on ingress. All traffic on ingress is compared to each EFP's matching criterion, and processed by that EFP if a match occurs." *Id*. at 12. Figure 3 depicts the EFP model:

Figure 3: EFP Model



59. The configuration guide further discloses that "[d]ata frames are switched within a bridge domain based on the destination MAC address" and that "[i]ncoming frames are mapped to a bridge domain, based on either the ingress port or a combination of both an ingress port and a MAC header field." *Id*. at 186.

60. Cisco EFP Products are operable to obtain an output port and an output VLAN ID, wherein the output VLAN ID represents a second VLAN and wherein the output port and the output VLAN ID relate to the destination MAC address and the VSI. For example, the Cisco ASR9000 series routers allows operators to "perform a variety of operations on the traffic flows when a router is configured with EFPs on various interfaces. Also, you can bridge or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs. This traffic is a mixture of VLAN IDs, single or double (QinQ) encapsulation, and ethertypes." *Id*. at 11. For example, "EFP supports [] L2 header encapsulation modifications on both ingress and egress." *Id.* at 15. As a further example, the configuration guide discloses several

forwarding cases, including "L2 Switched Service (Bridging)—The EFP is mapped to a bridge domain, where frames are switched based on their destination MAC address." *Id.* at 15-16.

61. Cisco EFP Products are operable to communicate the received frame and the output VLAN ID to the obtained output port, wherein the output VLAN ID is different from the input VLAN ID. For example, the Cisco ASR9000 series router allows operators to perform numerous L2 header encapsulation modifications on both ingress and egress, which include:

> • Push 1 or 2 VLAN tags
> • Pop 1 or 2 VLAN tags
> . . .
> • Rewrite 1 or 2 VLAN tags:
> . . .
> • The VLAN ID. 0 can be specified for an outer VLAN tag to generate a priority-tagged frame.

Id. at 15.

62. Cisco EFP Products are operable to add the output VLAN ID to the received frame or to substitute the output VLAN ID for the input VLAN ID contained by the frame. For example, the Cisco ASR9000 series router allows operators to perform numerous L2 header encapsulation modifications on both ingress and egress, which include:

> • Rewrite 1 or 2 VLAN tags:
> • Rewrite outer tag
> • Rewrite outer 2 tags
> • Rewrite outer tag and push an additional tag
> • Remove outer tag and rewrite inner tag
> . . .
> • The VLAN ID. 0 can be specified for an outer VLAN tag to generate a priority-tagged frame.

Id. at 15.

63. Cisco EFP Products abandon the received frame prior to communicating, if it is determined that the output port is the same as the input port and the output VLAN ID is the same as the input VLAN ID. For example, the configuration guide discloses: "Data frames are

switched within a bridge domain based on the destination MAC address. Multicast, broadcast, and unknown destination unicast frames are flooded within the bridge domain. In addition, the source MAC address learning is performed on all incoming frames on a bridge domain. A learned address is aged out. Incoming frames are mapped to a bridge domain, based on either the ingress port or a combination of both an ingress port and a MAC header field. By default, split horizon is enabled for pseudowires under the same VFI." *Id.* at 186.

64. The first VLAN in Cisco EFP Products includes one or more VLANs on a same network port, or one or more VLANs on different ports of a same network, or one or more VLANs on different ports of more than one network. For example, the configuration guide discloses: "An EFP subinterface is configured to specify which traffic on ingress is vectored to that EFP. This is done by specifying a VLAN, range of VLANs, or QinQ tagging to match against on ingress." *Id.* at 12.

65. Cisco EFP Products have an input port configured to receive a frame from at least two virtual local area networks (VLAN). For example, the configuration guide discloses: "An EFP subinterface is configured to specify which traffic on ingress is vectored to that EFP. This is done by specifying a VLAN, range of VLANs, or QinQ tagging to match against on ingress." *Id.* at 12.

66. Cisco EFP Products have a forwarding unit that executes in a storing module storing a plurality of relationships between combinations of the input port and input VLAN identifier and Virtual Switching Instances (VSI); and storing MAC address forwarding tables corresponding to the VSI, wherein at least one combination of input port and input VLAN ID corresponds to one VSI. For example, the Cisco ASR9000 series routers allows operators to "perform a variety of operations on the traffic flows when a router is configured with EFPs on

various interfaces. Also, you can bridge or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs. This traffic is a mixture of VLAN IDs, single or double (QinQ) encapsulation, and ethertypes." *Id.* at 11. For example, "EFP supports [] L2 header encapsulation modifications on both ingress and egress." *Id.* at 15. As a further example, the configuration guide discloses several forwarding cases, including "L2 Switched Service (Bridging)—The EFP is mapped to a bridge domain, where frames are switched based on their destination MAC address." *Id.* at 15-16.

67. The forwarding unit in Cisco EFP Products executes in an input analyzing module obtaining the input VLAN ID and the destination MAC address of the received frame and outputting the input VLAN ID and the destination MAC address. For example, the configuration guide discloses:

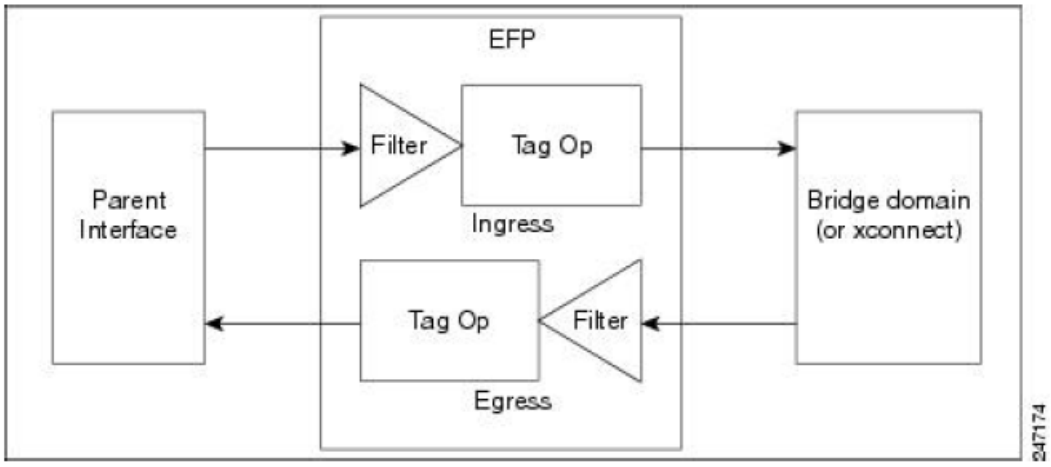
> An EFP can be regarded as an instantiation of a particular service. An EFP is defined by a set of filters. These filters are applied to all the ingress traffic to classify the frames that belong to a particular EFP. An EFP *filter* is a set of entries, where each entry looks similar to the start of a packet (ignoring source/destination MAC address). Each entry usually contains 0, 1 or 2 VLAN tags. A packet that starts with the same tags as an entry in the filter is said to match the filter; if the start of the packet does not correspond to any entry in the filter then the packet does not match the filter.

Id. at 11.

68. The forwarding unit in Cisco EFP Products executes in a first forwarding module determining the VSI corresponding to the combination of the input port and the input VLAN ID according to the relationship between the combination of the input port and the input VLAN ID and the VSI, and obtaining an output port and an output VLAN ID by searching the MAC address forwarding table corresponding to the VSI. For example, "[a]n Ethernet Flow Point (EFP) is a Layer 2 logical subinterface used to classify traffic under a physical or a bundle interface. A physical interface can be a Gigabit Ethernet 0/0/0/1 or a 10 Gigabit Ethernet 0/0/0/0

interface and has ports on the line card. A bundle interface is a virtual interface, created by grouping physical interfaces together." *Id*. at 11. The configuration guide discloses that "[a]n EFP subinterface is configured to specify which traffic on ingress is vectored to that EFP. This is done by specifying a VLAN, range of VLANs, or QinQ tagging to match against on ingress. All traffic on ingress is compared to each EFP's matching criterion, and processed by that EFP if a match occurs." *Id*. at 12. Figure 3 depicts the EFP model:

Figure 3: EFP Model



69. The configuration guide further discloses that "[d]ata frames are switched within a bridge domain based on the destination MAC address" and that "[i]ncoming frames are mapped to a bridge domain, based on either the ingress port or a combination of both an ingress port and a MAC header field." *Id*. at 186.

70. The configuration guide further discloses that operators can "perform a variety of operations on the traffic flows when a router is configured with EFPs on various interfaces. Also, you can bridge or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs. This traffic is a mixture of VLAN IDs, single or double (QinQ) encapsulation, and ethertypes." *Id*. at 11. For example, "EFP supports [] L2 header encapsulation modifications on both ingress and egress." *Id.* at 15. As a further example, the

configuration guide discloses several forwarding cases, including "L2 Switched Service (Bridging)—The EFP is mapped to a bridge domain, where frames are switched based on their destination MAC address." *Id.* at 15-16.

71. The forwarding unit in Cisco EFP Products executes in a second forwarding module forwarding the frame according to the output port and the output VLAN ID obtained by the first forwarding module. For example, the Cisco ASR9000 series router allows operators to perform numerous L2 header encapsulation modifications on both ingress and egress, which include:

> • Push 1 or 2 VLAN tags
> • Pop 1 or 2 VLAN tags
> . . .
> • Rewrite 1 or 2 VLAN tags:
> . . .
> • The VLAN ID. 0 can be specified for an outer VLAN tag to generate a priority-tagged frame.

Id. at 15.

72. Cisco EFP Products have an output port configured to communicate the received frame to more than one VLAN according to the output VLAN ID. For example, the configuration guide discloses that operators can "perform a variety of operations on the traffic flows when a router is configured with EFPs on various interfaces. Also, you can bridge or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs. This traffic is a mixture of VLAN IDs, single or double (QinQ) encapsulation, and ethertypes." *Id.* at 11.

73. The first forwarding module in Cisco EFP Products are further configured to instruct the second forwarding module to forward the frame after adding the output VLAN ID in the frame or substituting the output VLAN ID for the input VLAN ID in the frame. For

example, the Cisco ASR9000 series router allows operators to perform numerous L2 header encapsulation modifications on both ingress and egress, which include:

> • Rewrite 1 or 2 VLAN tags:
> • Rewrite outer tag
> • Rewrite outer 2 tags
> • Rewrite outer tag and push an additional tag
> • Remove outer tag and rewrite inner tag
> . . .
> • The VLAN ID. 0 can be specified for an outer VLAN tag to generate a priority-tagged frame.

Id. at 15.

74. The second forwarding module in Cisco EFP Products are further configured to detect, before forwarding the received frame to the output port, whether the output port and the output VLAN ID are the same as the input port and the input VLAN ID respectively; and abandoning the frame in which the output port and the output VLAN ID are the same as the input port and the input VLAN ID respectively. For example, the configuration guide discloses: "Data frames are switched within a bridge domain based on the destination MAC address. Multicast, broadcast, and unknown destination unicast frames are flooded within the bridge domain. In addition, the source MAC address learning is performed on all incoming frames on a bridge domain. A learned address is aged out. Incoming frames are mapped to a bridge domain, based on either the ingress port or a combination of both an ingress port and a MAC header field. By default, split horizon is enabled for pseudowires under the same VFI." *Id.* at 186.

75. The input VLAN ID in Cisco EFP Products comprises an input inner-layer VLAN ID and an input outer-layer VLAN ID; and the output VLAN ID in Cisco EFP Products comprises an output inner-layer VLAN ID and an output outer-layer VLAN ID. For example, the Cisco ASR9000 series routers allows operators to "perform a variety of operations on the traffic flows when a router is configured with EFPs on various interfaces. Also, you can bridge

or tunnel the traffic by many ways from one or more of the router's ingress EFPs to one or more egress EFPs. This traffic is a mixture of VLAN IDs, single or double (QinQ) encapsulation, and ethertypes." *Id*. at 11. For example, the Cisco ASR9000 series router allows operators to perform numerous L2 header encapsulation modifications on both ingress and egress, which include:

> • Rewrite 1 or 2 VLAN tags:
> • Rewrite outer tag
> • Rewrite outer 2 tags
> • Rewrite outer tag and push an additional tag
> • Remove outer tag and rewrite inner tag
> . . .
> • The VLAN ID. 0 can be specified for an outer VLAN tag to generate a priority-tagged frame.

Id. at 15.

76. As such, on information and belief, Verizon has directly infringed at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by (i) leasing, and/or using the Cisco EFP Products; (ii) making, offering for sale, and/or selling its services; and (iii) making, using, and/or importing into the United States the Cisco EFP Products, to infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent in violation of 35 U.S.C. § 271(a).). *See, e.g.*, https://www22.verizon.com/wholesale/access/order/guide/detail/Ethernet-Virtual-Circuit-Order-Guide.html.

77. On information and belief, Verizon has infringed at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by inducing others, including customers and network users that use the Cisco EFP Products and entities that install the Cisco EFP Products, to infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent in violation of 35 U.S.C. § 271(b).

78. On information and belief, Verizon takes active steps to induce infringement of at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by others, including its customers, and

Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent.

79. On information and belief, Verizon contributes to the infringement of at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by others, including its customers, network users, and contractors. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the use and/or importation of Cisco EFP Products. Such Cisco EFP Products are especially made or adapted for use to infringe at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent and are at least a material part of those claims, for example, as described above with respect to claim 1. The Cisco EFP Products, including the functionality contributing to infringement of the '709 Patent, are not suitable for substantial noninfringing use.

80. By way of at least Huawei's notice to Verizon in February 2019 and on March 29, 2019 (as well as this Complaint), Verizon knows of the '709 Patent and performs acts that it knows, or should know, induce, and/or contribute to the direct infringement of at least claims 1, 4, 7, 16-18, 21, and 23 of the '709 Patent by third parties.

81. Verizon undertook and continues its infringing actions despite an objectively high likelihood that such activities infringed the '709 Patent, is presumed valid. For example, Verizon has been aware of an objectively high likelihood that its actions constituted, and continue to constitute, infringement of the '709 Patent and that the '709 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the '709 Patent, nor could it reasonably subjectively believe that the '709 Patent is invalid. Despite that knowledge, subjective belief, and the objectively high

likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the '709 Patent.

82. Huawei has been irreparably harmed by Verizon's infringement of the '709 Patent and will continue to be harmed unless and until Verizon's infringement is enjoined by this Court.

83. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the '709 Patent pursuant to 35 U.S.C. § 271.

COUNT II: INFRINGEMENT OF PATENT NO. 8,154,986

84. Huawei realleges and incorporates by reference Paragraphs 1-83 above, as if fully set forth herein.

85. The U.S. Patent Office duly and properly issued the '986 Patent, entitled "Method for Fast Converging End-To-End Services and Provider Edge Equipment Thereof," on April 10, 2012. Huawei Technologies is the assignee of all right, title, and interest in and to the '986 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the '986 Patent is valid and enforceable. A true and correct copy of the '986 Patent is attached hereto as Exhibit B.

86. The '986 Patent provides novel and useful techniques and equipment for fast converging of a network after a node failure, so as to increase convergence speed as well as improve the service's reliability, overcoming the problems of the prior art and thereby improving the functioning of computer and network equipment. *See* the '986 Patent at Abstract.

87. The '986 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problem of "service convergence time" that is slower than requirements. *Id.* at 2:44-46. The background section of the '986 Patent provides Fig. 1 to describe a prior art convergence technique.

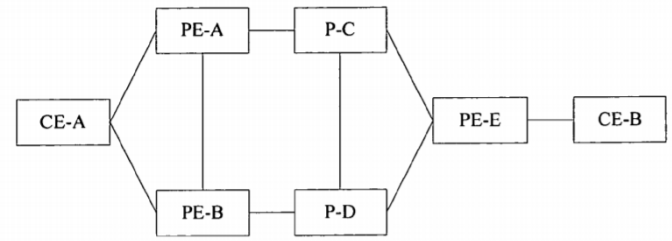


Figure 1 (Prior art)

88. With reference to Fig. 1, the '986 Patent explains that in the prior art, "the PE-E can detect the malfunction of the PE-A only through information, such as a Border Gateway Protocol (BGP) neighbor breaks down or an outer layer LSP tunnel is unavailable, etc., and the PE-E re-selects the VPN V4 route advertised by the PE-B." *Id.* at 2:22-26. "Before the PE-E fills the corresponding forwarding item with the route advertised by the PE-B, the terminal node of the outer layer LSP tunnel directed by the forwarding item of the forwarding engine of the PE-E is the PE-A all the time, and the PE-A has failed to function, therefore during the period from the malfunction appearing in the PE-A to the PE-E filling in the forwarding item with the route advertised by the PE-B, the CE-B is unable to access the CE-A, and the end-to-end service is interrupted." *Id.* at 2:31-39.

89. The '986 Patent further explains that in the prior art, when "the terminal node PE-A fails to function, the time for recovering the normal service transmission mainly depends on the service convergence time which is closely related to the number of the MPLS VPN inner routes and the number of hops of a bearer network." *Id.* at 2:40-44. The '986 Patent also explains that in the prior art, typically "the service convergence is about 5 s, which is far from the requirement that the end-to-end service convergence time should be less than 1 s, moreover, the end-to-end service convergence time will increase significantly with the increase in the number of MPLS VPN private network routes." *Id.* at 2:44-49.

90. The inventions of the '986 Patent provide technical solutions to the problems in the prior art described above. The '986 Patent describes, for example, "setting routing information and tunnel state information for each of at least two tunnels, by a double-ascription Provider Edge (PE) of a remote Customer Edge (CE) in the double-ascription PE itself which is connected with a nearby CE, before the nearby CE visits the remote CE, wherein, the double-ascription PE connected with the nearby CE serves as an initial node of each of the at least two tunnels, and at least two other PEs connected with the remote CE serve as terminal nodes of the at least two tunnels, respectively, and wherein the routing information and the tunnel state information of the at least two tunnels are stored in one route forwarding table in an IP network." *Id.* at 7:24-36. The '986 Patent further describes, for example, "detecting, by the double-ascription PE of the remote CE, tunnel states to obtain state information of the at least two tunnels." *Id.* at 7:37-39. The '986 Patent further describes, for example, "selecting, by the double-ascription PE of the remote CE, one or more available tunnels according to the state of each tunnel from the at least two tunnels." *Id.* at 7:40-42. The '986 Patent further describes, for example, "forwarding, by the double-ascription PE of the remote CE, service according to the routing information of the available tunnels selected." *Id.* at 7:43-45.

91. The inventions of the '986 Patent improve computer and network functionality by improving and solving problems in a computer or network device's capability to quickly converge the network after a node failure. The inventions of the '986 Patent provide a computer-based solution to a computer-specific problem. The inventions of the '986 Patent are improvements over the prior art and other techniques for convergence, and the '986 Patent enables a combination of features not present in the prior art and other techniques.

92. For example, the inventions of the '986 Patent provide for a "technical scheme that, by setting routing information for multiple tunnels, which are mutual backup tunnels or load sharing tunnels, in a double-ascription PE of a remote CE, and by detecting state information of the tunnels, it is possible for the double-ascription PE of the remote CE to forward the service directly according to the state information of the backup tunnel when the tunnel is unavailable, such as when a terminal node of the tunnel functions abnormally, thereby avoiding the procedure of re-selecting the optimal route." *Id.* at 3:24-33. "In addition, the end-to-end malfunction detection time can be less than 500 ms, even reaching 50 ms, by detecting an unavailable state of the tunnel using techniques such as BFD, tunnel fast convergence, etc." *Id.* at 3:33-36. The inventions of the '986 Patent further provide that, for example, "[t]he end-to-end malfunction detection time is independent of the private network route numbers that the MPLS VPN network bears." *Id.* at 3:37-39. The '986 Patent further discloses "it is possible to quickly and conveniently obtain the routing information of the mutual backup tunnels or the mutual load sharing tunnels by setting routing information." *Id*. at 3:39-42. "Therefore, the technical solution of the present invention can improve the service's reliability by increasing the end-to-end service convergence speed." *Id.* at 3:42-45.

93. The claims of the '986 Patent contain an inventive concept to improve the functioning of computers and other networked devices. Claims 1-6, 8, and 17 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the '986 Patent application was filed. These ordered combinations are set forth in claims 1-6, 8, and 17 of the '986 Patent. The ordered combinations of elements in claim 1-6, 8, and 17 were not well understood, routine or conventional at the time the '986 Patent application was filed. The ordered combinations of the inventions of claims 1-6,

8, and 17 are practical, particular, non-conventional, and non-generic solutions for fast converging an end-to-end service.

94. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1-6, 8, and 17 of the '986 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the '986 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Verizon's communications and/or content delivery networks, and associated network infrastructure that incorporate, for example, Cisco routers and switches (collectively, the "Cisco Convergence Products") including the ASR 9000 series, ASR 900 series, ASR 920 series, ASR 1000 series, ISR 4000 series, NCS 4200 series, Nexus 7000 products, and/or Juniper routers and switches (collectively, the "Juniper Convergence Products") including the Juniper MX Series and T series routers. *See, e.g.*, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=4860261 ("The Verizon Wireless network incorporates leading Cisco technologies, including the Cisco CRS-1 Carrier Routing System, the industry's only carrier routing system offering continuous system operation, service flexibility, and system longevity. Verizon Wireless is also deploying the new Cisco ASR 9000 Series Routers and Cisco ASR 1000 Series Routers to expand both capacity and capabilities of backhaul for its 3G/4G Mobile Internet services"); https://www.cisco.com/c/m/en_us/network-intelligence/service-provider/digital-transformation/verizon-tdm-to-ip-network-modernization.html ("Verizon selected Cisco's NCS 4200 system as one of its CEM packet switches. The packet network is Verizon's MPLS core."); https://investor.juniper.net/investor-relations/press-releases/press-release-details/2018/Juniper-Networks-Unveils-5G--and-IoT-Ready-Routing-Platform-to-

Unlock-Service-Creation-Opportunities/default.aspx (discussing Verizon's long-time use of Juniper Convergence Products); https://www.verizon.com/about/work/jobs/4126701-core-network-engineer (job posting requesting candidates with experience with Cisco Convergence Products and Juniper Convergence Products); https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/4441-docs-service-providers/2895/1/brkspg-2402.pdf at 9, 17 (discussing Verizon's use of Cisco Convergence Products).

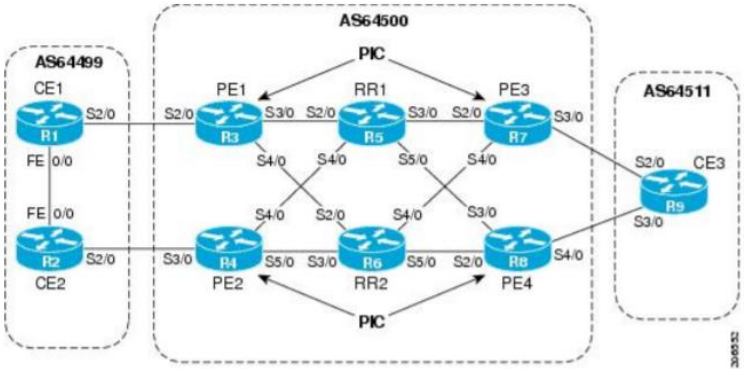
95. The Cisco Convergence Products are operable for fast converging an end-to-end service. *See, e.g.*, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-pic-edge-for-ip-and-mpls-vpn.pdf at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature improves BGP convergence after a network failure. This convergence is applicable to both core and edge failures and can be used in both IP and MPLS networks. The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover.").

96. With respect to at least claims 1-6 and 8, the Cisco Convergence Products are operable to set routing information and tunnel state information for each of at least two tunnels, by a double-ascription Provider Edge (PE) of a remote Customer Edge (CE) in the double-ascription PE itself which is connected with a nearby CE, before the nearby CE visits the remote CE, wherein, the double-ascription PE connected with the nearby CE serves as an initial node of each of the at least two tunnels, and at least two other PEs connected with the remote CE serve as terminal nodes of the at least two tunnels, respectively, and wherein the routing information and

the tunnel state information of the at least two tunnels are stored in one route forwarding table in an IP network. *See, e.g.*, *id.* at 4 ("BGP Fast Reroute (FRR) provides a best path and a backup or alternate path in BGP, RIB, and Cisco Express Forwarding. BGP FRR provides a fast reroute mechanism into the RIB and Cisco Express Forwarding (CEF) on the backup BGP next hop to reach a destination when the current best path is not available. BGP FRR precomputes a second best path in BGP and gives it to the RIB and Cisco Express Forwarding as a backup or alternate path, and CEF programs it into line cards. The BGP PIC feature provides the ability for CEF to quickly switch the traffic to the other egress ports if the current next hop or the link to this next hop goes down."); *id.* at 9:

The figure below shows a network that uses the BGP PIC feature on all the PE devices in an MPLS network.

Figure 4: Enabling BGP PIC on all PEs devices in the MPLS Network



The network includes the following components:

- eBGP sessions exist between the PE and CE devices.
- The PE devices are VPNv4 iBGP peers with reflect routers in the MPLS network.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through device CE3.
- CE3 is dual-homed with PE3 and PE4.
- PE1 has two paths to reach CE3 from the reflect routers:
  - PE3 is the primary path with the next hop as a PE3 address.
  - PE4 is the backup/alternate path with the next hop as a PE4 address.

97. The Cisco Convergence Products are operable to detect by the double-ascription PE of the remote CE, tunnel states to obtain state information of the at least two tunnels. *See*,

e.g., *id.* at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover."); *id.* at 2 ("An additional path for failover allows faster restoration of connectivity if a primary path is invalid or withdrawn."); *id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures."); *id.* at 4 ("If a PE node or link fails, then the failure is detected through IGP convergence.").

98. The Cisco Convergence Products are operable to select, by the double-ascription PE of the remote CE, one or more available tunnels according to the state of each tunnel from the at least two tunnels. *See, e.g.*, *id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures."); *id.* at 9 ("Thus, with BGP PIC enabled on PE3, Cisco Express Forwarding detects the node failure on PE3 and points the forwarding object to the backup/alternate node PE4.").

99. The Cisco Convergence Products are operable to forward, by the double-ascription PE of the remote CE, service according to the routing information of the available tunnels selected. *See, e.g.*, *id.* at 4 ("Therefore, BGP FRR sets up the best path and backup/alternate path. The BGP PIC feature provides the ability for Cisco Express Forwarding to quickly switch the traffic to the other egress ports if the current next hop or the link to this next hop goes down."); *id.* at 9 ("Thus, with BGP PIC enabled on PE3, Cisco Express Forwarding

detects the node failure on PE3 and points the forwarding object to the backup/alternate node PE4.").

100. With respect to at least claim 2, the Cisco Convergence Products are operable to perform the method of claim 1 wherein each of the tunnels comprises an inner layer tunnel and an outer layer tunnel; the inner layer tunnel is a Virtual Private Network (VPN) tunnel, and the outer layer tunnel is a Label Switching Path (LSP) tunnel or a Genetic Routing Encapsulation (GRE) tunnel or an Internet Protocol Security (IPSec) tunnel. *See, e.g., id.* at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover").

101. With respect to claim 3, the Cisco Convergence Products are operable to perform the method of claim 2 wherein, the step of the setting routing information of at least two tunnels by a double-ascription PE of a remote CE comprises the double-ascription PE of the remote CE setting optimal routing information and suboptimal routing information of the tunnels in the route forwarding table according to pre-configured matching strategies. *See, e.g., id.* at 16.

102. With respect to claim 4, the Cisco Convergence Products are operable to perform the method of claim 3 wherein, the procedure of setting a suboptimal routing information in the route forwarding table is setting the suboptimal routing information in the forwarding item of the optimal routing information in the route forwarding table. *See, e.g., id.* at 16.

103. With respect to claim 5, the Cisco Convergence Products are operable to perform the method of claim 2 wherein, the step of detecting tunnel states to obtain the state information of the at least two tunnels comprises when a control layer of the double-ascription PE of the

remote CE determines that some changes take place in the state of the outer layer tunnel of one of the at least two tunnels according to Bidirectional Forwarding Detection (BFD) or tunnel fast convergence techniques, advertising the available/unavailable state information of the tunnel to the forwarding engine. *See, e.g.*, *id.* at 5 ("A failure in the iBGP (remote) peer is detected by IGP; it may take a few seconds to detect the failure. Convergence can occur in subseconds or seconds, depending on whether PIC is enabled on the line cards."); *id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures.").

104. With respect to claim 6, the Cisco Convergence Products are operable to perform the method of claim 5 wherein there is a tunnel state field in the forwarding table of the forwarding engine and the step of advertising the available/unavailable state information of the outer layer tunnel of one of the at least two tunnels to the forwarding engine comprises the double-ascription PE of the remote CE advertising the available/unavailable state information of the outer layer tunnel of one of the at least two tunnels to the route forwarding table of the forwarding engine, and updating the content of state field of the corresponding item. *See, e.g.*, *id.* at 16; *id.* at 4.

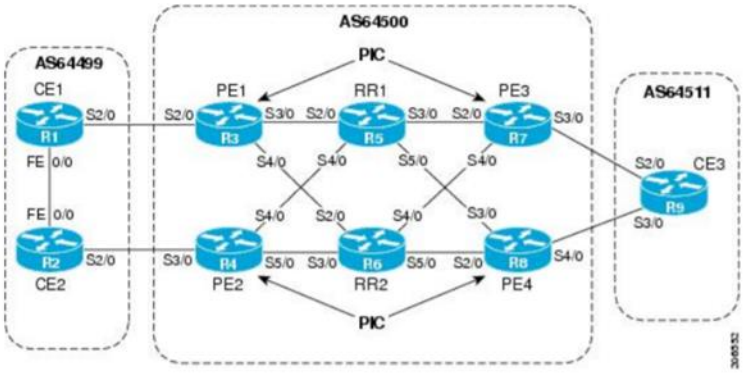
105. With respect to claim 8, the Cisco Convergence Products are operable to perform the method of claim 6 further comprising before forwarding the service to the remote CE through the backup tunnel, obtaining the state information of the backup tunnel and confirming that the state information of the backup tunnel is available. *See, e.g.*, *id.* at 16.

106. With respect to claim 17, the Cisco Convergence Products comprise a Provider Edge (PE) equipment. *See, e.g.*, https://www.cisco.com/c/en/us/td/docs/ios-

xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-pic-edge-for-ip-and-mpls-vpn.pdf at 9:

The figure below shows a network that uses the BGP PIC feature on all the PE devices in an MPLS network.

Figure 4: Enabling BGP PIC on all PEs devices in the MPLS Network



107. The Cisco Convergence Products comprise a storage module. *See, e.g., id.* at 3 ("With BGP PIC, Cisco Express Forwarding stores an alternate path per prefix.").

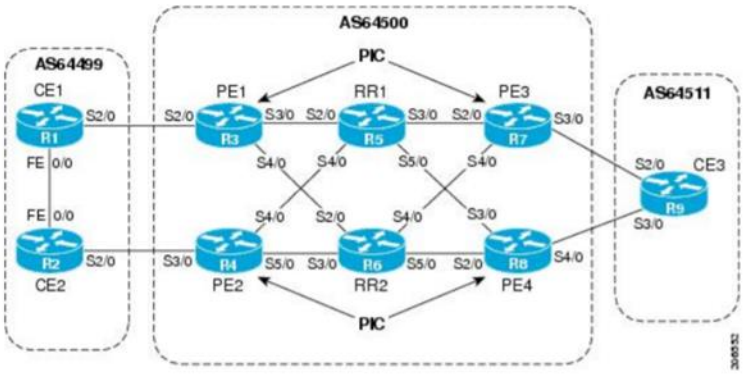
108. The Cisco Convergence Products comprise a tunnel state detecting module. *See, e.g., id.* at 3 ("Cisco Express Forwarding also listens to BFD events to rapidly detect local failures.").

109. The Cisco Convergence Products comprise a forwarding module. *See, e.g., id.* at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover.").

110. In the Cisco Convergence Products, the PE is a double-ascription PE of a remote Customer Edge (CE) and is connected with a nearby CE. *See, e.g., id.* at 9:

The figure below shows a network that uses the BGP PIC feature on all the PE devices in an MPLS network.

Figure 4: Enabling BGP PIC on all PEs devices in the MPLS Network



The network includes the following components:

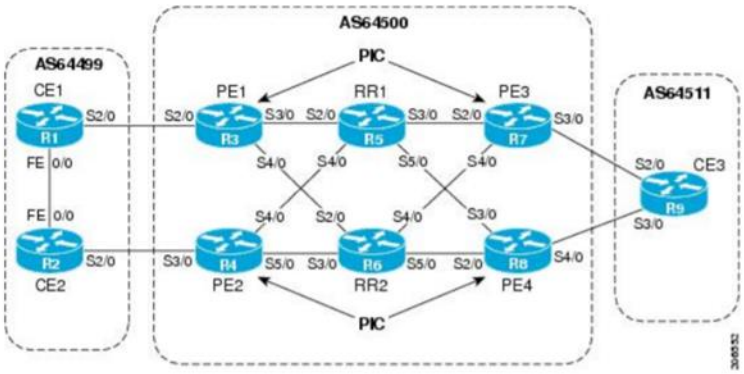
- eBGP sessions exist between the PE and CE devices.
- The PE devices are VPNv4 iBGP peers with reflect routers in the MPLS network.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through device CE3.
- CE3 is dual-homed with PE3 and PE4.
- PE1 has two paths to reach CE3 from the reflect routers:
  - PE3 is the primary path with the next hop as a PE3 address.
  - PE4 is the backup/alternate path with the next hop as a PE4 address.

111. In the Cisco Convergence Products, the storage module is configured to store routing information and tunnel state information for each of at least two tunnels, before the nearby CE visits the remote CE. *See, e.g., id.* at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover."); *id.* at 2 ("An additional path for failover allows faster restoration of connectivity if a primary path is invalid or withdrawn."); *id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures."); *id.* at 4 ("If a PE node or link fails, then the failure is detected through IGP convergence.").

112. In the Cisco Convergence Products, the double-ascription PE connected with the nearby CE serves as an initial node of each of the at least two tunnel, and at least two other PEs connected with the remote CE serve as terminal nodes of the at least two tunnels, respectively. *See, e.g., id.* at 9:

The figure below shows a network that uses the BGP PIC feature on all the PE devices in an MPLS network.

Figure 4: Enabling BGP PIC on all PEs devices in the MPLS Network



The network includes the following components:

- eBGP sessions exist between the PE and CE devices.
- The PE devices are VPNv4 iBGP peers with reflect routers in the MPLS network.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through device CE3.
- CE3 is dual-homed with PE3 and PE4.
- PE1 has two paths to reach CE3 from the reflect routers:
  - PE3 is the primary path with the next hop as a PE3 address.
  - PE4 is the backup/alternate path with the next hop as a PE4 address.

113. In the Cisco Convergence Products, the routing information and tunnel state information for each of the at least two tunnels are stored in one route forwarding table in an IP network. *See, e.g., id.* at 4 ("BGP Fast Reroute (FRR) provides a best path and a backup or alternate path in BGP, RIB, and Cisco Express Forwarding. BGP FRR provides a fast reroute mechanism into the RIB and Cisco Express Forwarding (CEF) on the backup BGP next hop to reach a destination when the current best path is not available. BGP FRR precomputes a second best path in BGP and gives it to the RIB and Cisco Express Forwarding as a backup or alternate

path, and CEF programs it into line cards. The BGP PIC feature provides the ability for CEF to quickly switch the traffic to the other egress ports if the current next hop or the link to this next hop goes down.").

114. In the Cisco Convergence Products, the tunnel state detecting module is configured to detect tunnel states of the at least two tunnels and update the tunnel state information stored in the storing module when the tunnel state is changed. *See, e.g., id.* at 1 ("The BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB), and Cisco Express Forwarding so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover."); *id.* at 2 ("An additional path for failover allows faster restoration of connectivity if a primary path is invalid or withdrawn."); *id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures."); *id.* at 4 ("If a PE node or link fails, then the failure is detected through IGP convergence.").

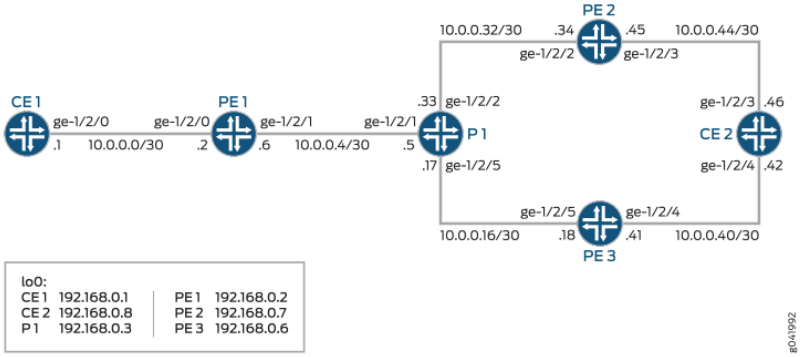
115. In the Cisco Convergence Products, the forwarding module is configured to select one or more available tunnels according to the state of each tunnel from the at least two tunnels stored in the storing module and forward service according to the routing information of the available tunnels selected. *See, e.g., id.* at 3 ("When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures."); *id.* at 9 ("Thus, with BGP PIC enabled on PE3, Cisco Express Forwarding detects the node failure on PE3 and points the forwarding object to the backup/alternate node PE4.").

116. The Juniper Convergence Products are operable for fast converging an end-to-end service. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE router. This already installed path is used until global convergence through the IGP is resolved. Using the alternative VPN route for forwarding until global convergence is complete reduces traffic loss.").

117. With respect to at least claims 1-6 and 8, the Juniper Convergence Products are operable to set routing information and tunnel state information for each of at least two tunnels, by a double-ascription Provider Edge (PE) of a remote Customer Edge (CE) in the double-ascription PE itself which is connected with a nearby CE, before the nearby CE visits the remote CE, wherein, the double-ascription PE connected with the nearby CE serves as an initial node of each of the at least two tunnels, and at least two other PEs connected with the remote CE serve as terminal nodes of the at least two tunnels, respectively, and wherein the routing information and the tunnel state information of the at least two tunnels are stored in one route forwarding table in an IP network. *See, e.g.*, *id.*; *id.* at 930-931 ("This example shows two customer edge (CE) routers, Device CE1 and Device CE2. Devices PE1, PE2, and PE3 are PE routers. Device P1 is a provider core router. Only Device PE1 has BGP PIC edge configured. The example uses the P1-PE2 link (P-PE) link to simulate the loss of a section of the network. For testing, the address 172.16.1.5/24 is added as a loopback interface address on Device CE2. The address is announced to Device PE2 and Device PE3 and is relayed by way of internal BGP (IBGP) IBGP to Device

PE1. On Device PE1, there are two paths to the 172.16.1.5/24 network. These are the primary and a backup path."); *id.* at 931:

Figure 76: BGP PIC Edge Scenario



See also id. at 940:

From Device PE1, run the **show route extensive table customer1.inet.0 172.16.1.0/24** command.

```
user@PE1> show route extensive table customer1.inet.0 172.16.1.0/24

customer1.inet.0: 7 destinations, 12 routes (7 active, 0 holddown, 0 hidden)
172.16.1.0/24 (3 entries, 2 announced)
        State: <CalcForwarding>
TSI:
KRT in-kernel 172.16.1.0/24 -> {indirect(262146), indirect(262142)}
Page 0 idx 0, (group ebgp type External) Type 1 val 0x950a62c (adv_entry)
   Advertised metrics:
     Nexthop: Self
     AS path: [100] 102 I
     Communities: target:100:1
Path 172.16.1.0 from 192.168.0.6 Vector len 4.  Val: 0
        @BGP    Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9514a74
                Next-hop reference count: 7
                Source: 192.168.0.6
                Next hop type: Router, Next hop index: 990
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299824, Push 299856(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299824: None; Label 299856: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.6
                Label operation: Push 299824
                Label TTL action: prop-ttl
                Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006
                State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.6+45824
                Announcement bits (1): 1-BGP_RT_Background
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299824
                Localpref: 100
                Router ID: 192.168.0.6
```

See also id. at 941:

```
        BGP     Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9515570
                Next-hop reference count: 7
                Source: 192.168.0.7
                Next hop type: Router, Next hop index: 933
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299856, Push 299872(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299856: None; Label 299872: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.7
                Label operation: Push 299856
                Label TTL action: prop-ttl
                Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005
                State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>
                Inactive reason: Not Best in its group - Router ID
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.7+10985
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299856
                Localpref: 100
```

See also id. at 942-943:

```
        #Multipath Preference: 255
                  Next hop type: Indirect
                  Address: 0x9578010
                  Next-hop reference count: 4
                  Next hop type: Router, Next hop index: 990
                  Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                  Label operation: Push 299824, Push 299856(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299824: None; Label 299856: None;
                  Session Id: 0x280002
                  Next hop type: Router, Next hop index: 933
                  Next hop: 10.0.0.5 via ge-1/2/1.0
                  Label operation: Push 299856, Push 299872(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299856: None; Label 299872: None;
                  Session Id: 0x280002
                  Protocol next hop: 192.168.0.6
                  Label operation: Push 299824
                  Label TTL action: prop-ttl
                  Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006 Weight
0x1
                  Protocol next hop: 192.168.0.7
                  Label operation: Push 299856
                  Label TTL action: prop-ttl
                  Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005 Weight
```

```
0x4000
                State: <ForwardingOnly Int Ext>
                Inactive reason: Forwarding use only
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: 102 I
                Communities: target:100:1
```

See also https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.pdf at 696-697:

From Device PE0, run the **show route forwarding-table destination 192.168.1.5 extensive** command.

`user@PE0>` **show route forwarding-table destination 192.168.1.5 extensive**

```
  Routing table: default.inet [Index 0]
Internet:

Destination:  192.168.1.5/24
  Route type: user
  Route reference: 0                    Route interface-index: 0
  Multicast RPF nh index: 0
  Flags: sent to PFE
  Next-hop type: unilist                Index: 1048576  Reference: 7401
  Next-hop type: indirect               Index: 1048574  Reference: 2
                         Weight: 0x1
  Nexthop: 10.0.0.6
  Next-hop type: unicast                Index: 623      Reference: 8
```

```
  Next-hop interface: ge-0/0/0.0  Weight: 0x1
  Next-hop type: indirect               Index: 1048575  Reference: 2
                         Weight: 0x4000
  Nexthop: 10.0.0.2
  Next-hop type: unicast                Index: 624      Reference: 8
  Next-hop interface: ge-0/0/1.0  Weight: 0x4000
```

Meaning

Junos OS uses the next hops and the **weight** values to select a backup path when a link failure occurs. The next-hop weight has one of the following values:

- 0x1 indicates the primary path with active next hops.
- 0x4000 indicates the backup path with passive next hops.

118. The Juniper Convergence Products are operable to detect by the double-ascription PE of the remote CE, tunnel states to obtain state information of the at least two tunnels. *See, e.g.*, *id.* at 673 ("When reachability to an egress router in a network fails, the IGP detects this outage, and the link state propagates this information throughout the network and advertises the

BGP next hop for that prefix as unreachable."); *id.* ("On a BGP PIC enabled router, Junos OS installs the backup path for the indirect next hop on the Routine Engine and also provides this route to the Packet Forwarding Engine and IGP. When an IGP loses reachability to a prefix with one or more routes, it signals to the Routing Engine with a single message prior to updating the routing tables. The Routing Engine signals to the Packet Forwarding Engine that an indirect next hop has failed, and traffic must be rerouted using the backup path. Routing to the impacted destination prefix continues using the backup path even before BGP starts recalculating the new next hops for the BGP prefixes. The router uses this backup path to reduce traffic loss until the global convergence through the BGP is resolved.").

119. The Juniper Convergence Products are operable to select, by the double-ascription PE of the remote CE, one or more available tunnels according to the state of each tunnel from the at least two tunnels. *See, e.g.*, *id.* at 673 ("However, with the BGP PIC feature enabled, even before BGP recalculates the best path for those affected prefixes, the Routing Engine signals the data plane to switch to the standby next best path. Hence traffic loss is minimum. The new routes are calculated even while the traffic is being forwarded, and these new routes are pushed down to the data plane. Therefore, the number of BGP prefixes affected does not impact the time taken from the time traffic outage occurs to the point of time at which BGP signals the loss of reachability."); *id.* at 696:

Meaning

Junos OS uses the next hops and the **weight** values to select a backup path when a link failure occurs. The next-hop weight has one of the following values:

- 0x1 indicates the primary path with active next hops.
- 0x4000 indicates the backup path with passive next hops.

120. The Juniper Convergence Products are operable to forward, by the double-ascription PE of the remote CE, service according to the routing information of the available tunnels selected. *See, e.g.*, *id.* at 673 ("However, with the BGP PIC feature enabled, even before

BGP recalculates the best path for those affected prefixes, the Routing Engine signals the data plane to switch to the standby next best path. Hence traffic loss is minimum. The new routes are calculated even while the traffic is being forwarded, and these new routes are pushed down to the data plane. Therefore, the number of BGP prefixes affected does not impact the time taken from the time traffic outage occurs to the point of time at which BGP signals the loss of reachability.").

121. With respect to at least claim 2, the Juniper Convergence Products are operable to perform the method of claim 1 wherein each of the tunnels comprises an inner layer tunnel and an outer layer tunnel; the inner layer tunnel is a Virtual Private Network (VPN) tunnel, and the outer layer tunnel is a Label Switching Path (LSP) tunnel or a Genetic Routing Encapsulation (GRE) tunnel or an Internet Protocol Security (IPSec) tunnel. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 940:

From Device PE1, run the **show route extensive table customer1.inet.0 172.16.1.0/24** command.

```
user@PE1> show route extensive table customer1.inet.0 172.16.1.0/24

customer1.inet.0: 7 destinations, 12 routes (7 active, 0 holddown, 0 hidden)
172.16.1.0/24 (3 entries, 2 announced)
        State: <CalcForwarding>
TSI:
KRT in-kernel 172.16.1.0/24 -> {indirect(262146), indirect(262142)}
Page 0 idx 0, (group ebgp type External) Type 1 val 0x950a62c (adv_entry)
   Advertised metrics:
     Nexthop: Self
     AS path: [100] 102 I
     Communities: target:100:1
Path 172.16.1.0 from 192.168.0.6 Vector len 4.  Val: 0
        eBGP    Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9514a74
                Next-hop reference count: 7
                Source: 192.168.0.6
                Next hop type: Router, Next hop index: 990
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299824, Push 299856(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299824: None; Label 299856: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.6
                Label operation: Push 299824
                Label TTL action: prop-ttl
                Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006
                State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.6+45824
                Announcement bits (1): 1-BGP_RT_Background
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299824
                Localpref: 100
                Router ID: 192.168.0.6
```

See also id. at 941:

```
        BGP     Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9515570
                Next-hop reference count: 7
                Source: 192.168.0.7
                Next hop type: Router, Next hop index: 933
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299856, Push 299872(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299856: None; Label 299872: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.7
                Label operation: Push 299856
                Label TTL action: prop-ttl
                Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005
                State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>
                Inactive reason: Not Best in its group - Router ID
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.7+10985
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299856
                Localpref: 100
```

id. at 942-943:

```
        #Multipath Preference: 255
                  Next hop type: Indirect
                  Address: 0x9578010
                  Next-hop reference count: 4
                  Next hop type: Router, Next hop index: 990
                  Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                  Label operation: Push 299824, Push 299856(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299824: None; Label 299856: None;
                  Session Id: 0x280002
                  Next hop type: Router, Next hop index: 933
                  Next hop: 10.0.0.5 via ge-1/2/1.0
                  Label operation: Push 299856, Push 299872(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299856: None; Label 299872: None;
                  Session Id: 0x280002
                  Protocol next hop: 192.168.0.6
                  Label operation: Push 299824
                  Label TTL action: prop-ttl
                  Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006 Weight
0x1
                  Protocol next hop: 192.168.0.7
                  Label operation: Push 299856
                  Label TTL action: prop-ttl
                  Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005 Weight
```

122. With respect to claim 3, the Juniper Convergence Products are operable to perform the method of claim 2 wherein, the step of the setting routing information of at least two tunnels by a double-ascription PE of a remote CE comprises the double-ascription PE of the remote CE setting optimal routing information and suboptimal routing information of the tunnels in the route forwarding table according to pre-configured matching strategies. *See, e.g.*, *id.* at 940:

From Device PE1, run the **show route extensive table customer1.inet.0 172.16.1.0/24** command.

```
user@PE1> show route extensive table customer1.inet.0 172.16.1.0/24

customer1.inet.0: 7 destinations, 12 routes (7 active, 0 holddown, 0 hidden)
172.16.1.0/24 (3 entries, 2 announced)
        State: <CalcForwarding>
TSI:
KRT in-kernel 172.16.1.0/24 -> {indirect(262146), indirect(262142)}
Page 0 idx 0, (group ebgp type External) Type 1 val 0x950a62c (adv_entry)
   Advertised metrics:
     Nexthop: Self
     AS path: [100] 102 I
     Communities: target:100:1
Path 172.16.1.0 from 192.168.0.6 Vector len 4.  Val: 0
        eBGP    Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9514a74
                Next-hop reference count: 7
                Source: 192.168.0.6
                Next hop type: Router, Next hop index: 990
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299824, Push 299856(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299824: None; Label 299856: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.6
                Label operation: Push 299824
                Label TTL action: prop-ttl
                Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006
                State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.6+45824
                Announcement bits (1): 1-BGP_RT_Background
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299824
                Localpref: 100
                Router ID: 192.168.0.6
```

See also id. at 941:

```
        BGP     Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9515570
                Next-hop reference count: 7
                Source: 192.168.0.7
                Next hop type: Router, Next hop index: 933
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299856, Push 299872(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299856: None; Label 299872: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.7
                Label operation: Push 299856
                Label TTL action: prop-ttl
                Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005
                State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>
                Inactive reason: Not Best in its group - Router ID
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.7+10985
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299856
                Localpref: 100
```

id. at 942-943:

```
        #Multipath Preference: 255
                  Next hop type: Indirect
                  Address: 0x9578010
                  Next-hop reference count: 4
                  Next hop type: Router, Next hop index: 990
                  Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                  Label operation: Push 299824, Push 299856(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299824: None; Label 299856: None;
                  Session Id: 0x280002
                  Next hop type: Router, Next hop index: 933
                  Next hop: 10.0.0.5 via ge-1/2/1.0
                  Label operation: Push 299856, Push 299872(top)
                  Label TTL action: prop-ttl, prop-ttl(top)
                  Load balance label: Label 299856: None; Label 299872: None;
                  Session Id: 0x280002
                  Protocol next hop: 192.168.0.6
                  Label operation: Push 299824
                  Label TTL action: prop-ttl
                  Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006 Weight
0x1
                  Protocol next hop: 192.168.0.7
                  Label operation: Push 299856
                  Label TTL action: prop-ttl
                  Load balance label: Label 299856: None;
                Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005 Weight
```

123. With respect to claim 4, the Juniper Convergence Products are operable to perform the method of claim 3 wherein, the procedure of setting a suboptimal routing information in the route forwarding table is setting the suboptimal routing information in the forwarding item of the optimal routing information in the route forwarding table. *See, e.g.*, *id.* at 927.

124. With respect to claim 5, the Juniper Convergence Products are operable to perform the method of claim 2 wherein, the step of detecting tunnel states to obtain the state information of the at least two tunnels comprises when a control layer of the double-ascription PE of the remote CE determines that some changes take place in the state of the outer layer tunnel of one of the at least two tunnels according to Bidirectional Forwarding Detection (BFD) or tunnel fast convergence techniques, advertising the available/unavailable state information of the tunnel to the forwarding engine. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.pdf at 673 ("When an IGP loses reachability to a prefix with one or more routes, it signals to the Routing Engine with a single message prior to updating the routing tables. The Routing Engine signals to the Packet Forwarding Engine that an indirect next hop has failed, and traffic must be rerouted using the backup path").

125. With respect to claim 6, the Juniper Convergence Products are operable to perform the method of claim 5 wherein there is a tunnel state field in the forwarding table of the forwarding engine and the step of advertising the available/unavailable state information of the outer layer tunnel of one of the at least two tunnels to the forwarding engine comprises the double-ascription PE of the remote CE advertising the available/unavailable state information of the outer layer tunnel of one of the at least two tunnels to the route forwarding table of the forwarding engine, and updating the content of state field of the corresponding item. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE route.").

126. With respect to claim 8, the Juniper Convergence Products are operable to perform the method of claim 6 further comprising before forwarding the service to the remote CE through the backup tunnel, obtaining the state information of the backup tunnel and confirming that the state information of the backup tunnel is available. *See, e.g.*, *id.* at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE route.").

127. With respect to claim 17, the Juniper Convergence Products comprise a Provider Edge (PE) equipment. *See, e.g.*, *id.* at 930. ("This example shows two customer edge (CE) routers, Device CE1 and Device CE2. Devices PE1, PE2, and PE3 are PE routers. Device P1 is a provider core router. Only Device PE1 has BGP PIC edge configured.").

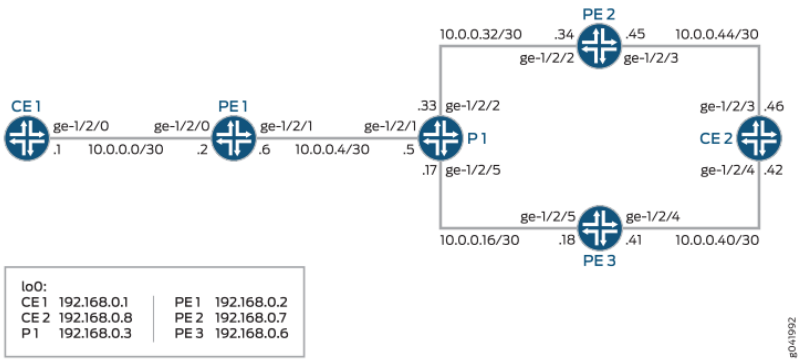
128. The Juniper Convergence Products comprise a storage module. *See, e.g.*, *id.* at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE router. This already installed path is used until global convergence through the IGP is resolved. Using the alternative VPN route for forwarding until global convergence is complete reduces traffic loss.").

129. The Juniper Convergence Products comprise a tunnel state detecting module. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.pdf at 673 ("When reachability to an egress router in a network fails, the IGP detects this outage, and the link state propagates this information throughout the network and advertises the BGP next hop for that prefix as unreachable.").

130. The Juniper Convergence Products comprise a forwarding module. *See, e.g.*, *id.* at 673 ("On a BGP PIC enabled router, Junos OS installs the backup path for the indirect next hop on the Routine Engine and also provides this route to the Packet Forwarding Engine and IGP. When an IGP loses reachability to a prefix with one or more routes, it signals to the Routing Engine with a single message prior to updating the routing tables. The Routing Engine signals to the Packet Forwarding Engine that an indirect next hop has failed, and traffic must be rerouted using the backup path. Routing to the impacted destination prefix continues using the backup path even before BGP starts recalculating the new next hops for the BGP prefixes. The router uses this backup path to reduce traffic loss until the global convergence through the BGP is resolved.").

131. In the Juniper Convergence Products, the PE is a double-ascription PE of a remote Customer Edge (CE) and is connected with a nearby CE. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE router. This already installed path is used until global convergence through the IGP is resolved. Using the alternative VPN route for forwarding until global convergence is complete reduces traffic loss."); *id.* at 930-931 ("This example shows two customer edge (CE) routers, Device CE1 and Device CE2. Devices PE1, PE2, and PE3 are PE routers. Device P1 is a provider core router. Only Device PE1 has BGP PIC edge configured. The example uses the P1-PE2 link (P-PE) link to simulate the loss of a section of the network. For testing, the address 172.16.1.5/24 is added as a loopback interface address on Device CE2. The address is announced to Device PE2 and Device PE3 and is relayed by way of internal BGP (IBGP) IBGP to Device PE1. On Device PE1, there are two paths to the 172.16.1.5/24 network. These are the primary and a backup path."); *id.* at 931:

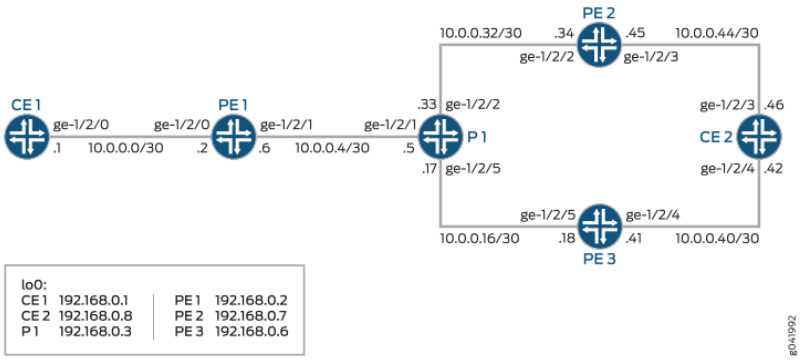
Figure 76: BGP PIC Edge Scenario



132. In the Juniper convergence products, the storage module is configured to store routing information and tunnel state information for each of at least two tunnels, before the nearby CE visits the remote CE. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE router. This already installed path is used until global convergence through the IGP is resolved. Using the alternative VPN route for forwarding until global convergence is complete reduces traffic loss.").

133. In the Juniper Convergence Products, the double-ascription PE connected with the nearby CE serves as an initial node of each of the at least two tunnel, and at least two other PEs connected with the remote CE serve as terminal nodes of the at least two tunnels, respectively. *See, e.g.*, *id.* at 930-931 ("This example shows two customer edge (CE) routers, Device CE1 and Device CE2. Devices PE1, PE2, and PE3 are PE routers. Device P1 is a provider core router. Only Device PE1 has BGP PIC edge configured. The example uses the P1-PE2 link (P-PE) link to simulate the loss of a section of the network. For testing, the address 172.16.1.5/24 is added as a loopback interface address on Device CE2. The address is announced to Device PE2 and Device PE3 and is relayed by way of internal BGP (IBGP) IBGP to Device PE1. On Device PE1, there are two paths to the 172.16.1.5/24 network. These are the primary and a backup path."); *id.* at 931:

Figure 76: BGP PIC Edge Scenario



134. In the Juniper Convergence Products, the routing information and tunnel state information for each of the at least two tunnels are stored in one route forwarding table in an IP network. *See, e.g.*, https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-layer-3.pdf at 927 ("BGP Prefix-Independent Convergence (PIC) Edge allows you to install a Layer 3 VPN route in the forwarding table as an alternate path, enabling fast failover when a PE router fails or you lose connectivity to a PE router. This already installed path is used until global convergence through the IGP is resolved. Using the alternative VPN route for forwarding until global convergence is complete reduces traffic loss."); *id.* at 940:

From Device PE1, run the **show route extensive table customer1.inet.0 172.16.1.0/24** command.

```
user@PE1> show route extensive table customer1.inet.0 172.16.1.0/24
```

```
customer1.inet.0: 7 destinations, 12 routes (7 active, 0 holddown, 0 hidden)
172.16.1.0/24 (3 entries, 2 announced)
        State: <CalcForwarding>
TSI:
KRT in-kernel 172.16.1.0/24 -> {indirect(262146), indirect(262142)}
Page 0 idx 0, (group ebgp type External) Type 1 val 0x950a62c (adv_entry)
   Advertised metrics:
     Nexthop: Self
     AS path: [100] 102 I
     Communities: target:100:1
Path 172.16.1.0 from 192.168.0.6 Vector len 4.  Val: 0
        @BGP    Preference: 170/-101
                Route Distinguisher: 100:1
                Next hop type: Indirect
                Address: 0x9514a74
                Next-hop reference count: 7
                Source: 192.168.0.6
                Next hop type: Router, Next hop index: 990
                Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                Label operation: Push 299824, Push 299856(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Load balance label: Label 299824: None; Label 299856: None;
                Session Id: 0x280002
                Protocol next hop: 192.168.0.6
                Label operation: Push 299824
                Label TTL action: prop-ttl
                Load balance label: Label 299824: None;
                Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006
                State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
                Local AS:   100 Peer AS:   100
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: BGP_100.192.168.0.6+45824
                Announcement bits (1): 1-BGP_RT_Background
                AS path: 102 I
                Communities: target:100:1
                Import Accepted
                VPN Label: 299824
                Localpref: 100
                Router ID: 192.168.0.6
```

See also id. at 941:

```
        BGP    Preference: 170/-101
               Route Distinguisher: 100:1
               Next hop type: Indirect
               Address: 0x9515570
               Next-hop reference count: 7
               Source: 192.168.0.7
               Next hop type: Router, Next hop index: 933
               Next hop: 10.0.0.5 via ge-1/2/1.0, selected
               Label operation: Push 299856, Push 299872(top)
               Label TTL action: prop-ttl, prop-ttl(top)
               Load balance label: Label 299856: None; Label 299872: None;
               Session Id: 0x280002
               Protocol next hop: 192.168.0.7
               Label operation: Push 299856
               Label TTL action: prop-ttl
               Load balance label: Label 299856: None;
               Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005
               State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>
               Inactive reason: Not Best in its group - Router ID
               Local AS:   100 Peer AS:   100
               Age: 1:38:13    Metric2: 1
               Validation State: unverified
               Task: BGP_100.192.168.0.7+10985
               AS path: 102 I
               Communities: target:100:1
               Import Accepted
               VPN Label: 299856
               Localpref: 100
```

See also id. at 942-943:

```
        #Multipath Preference: 255
                   Next hop type: Indirect
                   Address: 0x9578010
                   Next-hop reference count: 4
                   Next hop type: Router, Next hop index: 990
                   Next hop: 10.0.0.5 via ge-1/2/1.0, selected
                   Label operation: Push 299824, Push 299856(top)
                   Label TTL action: prop-ttl, prop-ttl(top)
                   Load balance label: Label 299824: None; Label 299856: None;
                   Session Id: 0x280002
                   Next hop type: Router, Next hop index: 933
                   Next hop: 10.0.0.5 via ge-1/2/1.0
                   Label operation: Push 299856, Push 299872(top)
                   Label TTL action: prop-ttl, prop-ttl(top)
                   Load balance label: Label 299856: None; Label 299872: None;
                   Session Id: 0x280002
                   Protocol next hop: 192.168.0.6
                   Label operation: Push 299824
                   Label TTL action: prop-ttl
                   Load balance label: Label 299824: None;
                  Indirect next hop: 0x96bc104 262146 INH Session ID: 0x280006 Weight
0x1
                   Protocol next hop: 192.168.0.7
                   Label operation: Push 299856
                   Label TTL action: prop-ttl
                   Load balance label: Label 299856: None;
                  Indirect next hop: 0x96bc000 262142 INH Session ID: 0x280005 Weight
```

```
0x4000
                State: <ForwardingOnly Int Ext>
                Inactive reason: Forwarding use only
                Age: 1:38:13    Metric2: 1
                Validation State: unverified
                Task: RT
                Announcement bits (1): 0-KRT
                AS path: 102 I
                Communities: target:100:1
```

See also https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.pdf at 696-697:

From Device PE0, run the **show route forwarding-table destination 192.168.1.5 extensive** command.

`user@PE0>` **show route forwarding-table destination 192.168.1.5 extensive**

```
  Routing table: default.inet [Index 0]
Internet:

Destination:  192.168.1.5/24
  Route type: user
  Route reference: 0                    Route interface-index: 0
  Multicast RPF nh index: 0
  Flags: sent to PFE
  Next-hop type: unilist                Index: 1048576  Reference: 7401
  Next-hop type: indirect               Index: 1048574  Reference: 2
                          Weight: 0x1
  Nexthop: 10.0.0.6
  Next-hop type: unicast                Index: 623      Reference: 8
```

```
  Next-hop interface: ge-0/0/0.0  Weight: 0x1
  Next-hop type: indirect               Index: 1048575  Reference: 2
                          Weight: 0x4000
  Nexthop: 10.0.0.2
  Next-hop type: unicast                Index: 624      Reference: 8
  Next-hop interface: ge-0/0/1.0  Weight: 0x4000
```

Meaning

Junos OS uses the next hops and the **weight** values to select a backup path when a link failure occurs. The next-hop weight has one of the following values:

- 0x1 indicates the primary path with active next hops.
- 0x4000 indicates the backup path with passive next hops.

135. In the Juniper Convergence Products, the tunnel state detecting module is configured to detect tunnel states of the at least two tunnels and update the tunnel state information stored in the storing module when the tunnel state is changed. *See, e.g.*,

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/config-guide-routing-bgp.pdf at 673 ("When reachability to an egress router in a network fails, the IGP detects this outage, and the link state propagates this information throughout the network and advertises the BGP next hop for that prefix as unreachable"; *id.* ("On a BGP PIC enabled router, Junos OS installs the backup path for the indirect next hop on the Routine Engine and also provides this route to the Packet Forwarding Engine and IGP. When an IGP loses reachability to a prefix with one or more routes, it signals to the Routing Engine with a single message prior to updating the routing tables. The Routing Engine signals to the Packet Forwarding Engine that an indirect next hop has failed, and traffic must be rerouted using the backup path. Routing to the impacted destination prefix continues using the backup path even before BGP starts recalculating the new next hops for the BGP prefixes. The router uses this backup path to reduce traffic loss until the global convergence through the BGP is resolved.").

136. In the Juniper Convergence Products, the forwarding module is configured to select one or more available tunnels according to the state of each tunnel from the at least two tunnels stored in the storing module and forward service according to the routing information of the available tunnels selected. *See, e.g.*, *id.* at 673 ("However, with the BGP PIC feature enabled, even before BGP recalculates the best path for those affected prefixes, the Routing Engine signals the data plane to switch to the standby next best path. Hence traffic loss is minimum. The new routes are calculated even while the traffic is being forwarded, and these new routes are pushed down to the data plane. Therefore, the number of BGP prefixes affected does not impact the time taken from the time traffic outage occurs to the point of time at which BGP signals the loss of reachability."); *id.* at 696:

Meaning

Junos OS uses the next hops and the **weight** values to select a backup path when a link failure occurs. The next-hop weight has one of the following values:

- 0x1 indicates the primary path with active next hops.
- 0x4000 indicates the backup path with passive next hops.

137. As such, on information and belief, Verizon has directly infringed at least claims 1-6, 8, and 17 of the '986 Patent by at least, for example, (i) using the Cisco Convergence Products and Juniper Convergence Products within its network for fast convergence in a manner that infringes at least claims 1-6, 8, and 17 of the '986 Patent; (ii) making networks and systems that incorporate Cisco Convergence Products and Juniper Convergence Products in a manner that infringes at least claims 1-6, 8, and 17 of the '986 Patent and by using such components in its communications and/or content delivery networks; and (iii) selling and offering for sale network services that use the Cisco Convergence Products and Juniper Convergence Products in a manner that infringes at least claims 1-6, 8, and 17 of the '986 Patent.

138. On information and belief, Verizon has infringed at least claims 1-6, 8, and 17 of the '986 Patent by inducing others, including customers and network users that use the Cisco Convergence Products and the Juniper Convergence Products and entities that install the Cisco Convergence Products and the Juniper Convergence Products, to infringe at least claims 1-6, 8, and 17 of the '986 Patent in violation of 35 U.S.C. § 271(b).

139. On information and belief, Verizon takes active steps to induce infringement of at least claims 1-6, 8, and 17 of the '986 Patent by others, including its customers, and Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others.

140. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1-6, 8, and 17 of the '986 Patent.

141. On information and belief, Verizon contributes to the infringement of at least claims 1-6, 8, and 17 of the ’986 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or importation by Verizon of the Cisco Convergence Products and the Juniper Convergence Products. Such Cisco Convergence Products and Juniper Convergence Products are especially made for or adapted for use to infringe at least claims 1-6, 8, and 17 of the ’986 Patent and are at least a material part of those claims, for example, as described above. The Cisco Convergence Products and the Juniper Convergence Products, including the functionality contributing to infringement of the ’986 Patent, are not suitable for substantial noninfringing use.

142. By way of at least Huawei’s notice to Verizon in February 2019 and on March 29, 2019 (as well as this Complaint), Verizon knows of the ’986 Patent and performs acts that it knows, or should know, induce and/or contribute to the direct infringement of at least claims 1-6, 8, and 17 of the ’986 Patent by third parties.

143. Verizon undertook and continues its infringing actions despite an objectively high likelihood that such activities infringed the ’986 Patent, which is presumed valid. For example, Verizon has been aware of an objectively high likelihood that its actions constituted, and continue to constitute, infringement of the ’986 Patent and that the ’986 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the ’986 Patent, nor could it reasonably subjectively believe that the ’986 Patent is invalid. Despite that knowledge, subjective belief, and the objectively high likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the ’986 Patent.

144. Huawei has been irreparably harmed by Verizon's infringement of the '986 Patent and will continue to be harmed unless and until Verizon's infringement is enjoined by this Court.

145. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the '986 Patent pursuant to 35 U.S.C. § 271.

COUNT III: INFRINGEMENT OF PATENT NO. 10,027,693

146. Huawei realleges and incorporates by reference Paragraphs 1-145 above, as if fully set forth herein.

147. The U.S. Patent Office duly and properly issued the '693 Patent, entitled "Method, Device and System for Alerting against Unknown Malicious Codes within a Network Environment," on July 17, 2018. Huawei Digital is the assignee of all right, title, and interest in and to the '693 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the '693 Patent is valid and enforceable. A true and correct copy of the '693 Patent is attached hereto as Exhibit C.

148. The '693 Patent provides novel, useful and more effective and efficient techniques for protecting users from malicious downloads. When hackers discover new security vulnerabilities, they quickly develop malicious code to exploit the vulnerabilities and typically deploy that code over the Internet. *See* the '693 Patent at 1:27-32. The longer it takes to identify the malicious code and release a patch, the more damage can result. *See id.* at 1:32-41.

149. Prior to the inventions of the '693 Patent, network gateway devices such as those operated by Internet Service Providers ("ISPs") were unable to report suspicious code downloaded by users. *Id.* at 1:42-43. And antivirus software may not be installed and/or properly maintained on end user terminals, making both the terminals and the surrounding network more vulnerable to the propagation of malicious code. *Id.* at 1:51-54.

150. The ’693 Patent provide technical solutions to the problems in the prior art described above. The ’693 Patent discloses, for example, a technique whereby the network device records the source path of a file requested by a terminal for download. *See, e.g.*, *id.* at 3:26-31. The network device judges, based on the request for the file or the data stream carrying the file whether it is some form of executable file. *See, e.g.*, *id.* at 3:32-34. If the file requested for download is an executable file, the network device sends a first alert including the source path to a monitoring device. *See, e.g.*, *id.* at 3:35-37.

151. The monitoring device downloads the executable file from the provided source path and either compares the characteristics of it to other known malicious code or runs the executable in a sandbox to determine the likelihood of the executable file being malicious. *See, e.g.*, *id.* at 5:24-61. The maliciousness of the file is determined. *See, e.g.*, *id.* at 5:41-43, 5:59-61. The monitoring device sends a second alert to the network device that “includes maliciousness of the suspicious code, or includes both the maliciousness of the suspicious code and the Botnet topology information.” *See, e.g.*, *id.* at 6:8-11. From the information in the second alert, the network device can intercept the suspicious code. *See, e.g.*, *id.* at 6:15-17. The second alarm information may also contain information regarding the topology of a Botnet, and the network device may use this topology information to intercept packets transmitted in the Botnet. *See, e.g.*, *id.* at 6:18-22.

152. The inventions of the ’693 Patent improve network functionality by improving and solving problems in a networked device’s capability of preventing the download and spread of malicious code more thoroughly and with better efficiency. The inventions of the ’693 Patent provide a computer-based solution to a computer-specific problem. The inventions of the ’693 Patent are improvements over the prior art and other techniques for preventing malware attacks,

and the ’693 Patent enables a combination of features not present in the prior art and other techniques.

153. For example, the inventions of the ’693 Patent provide for improved network security by preventing malware attacks independently from and transparently to the user terminal requesting the malware.

154. By way of further example, the inventions of the ’693 Patent provide for improved computer and network operation by more thoroughly preventing malware attacks through an architecture where network entities send queries about suspicious downloads to a monitoring service that is able to aggregate knowledge of malicious code from various network devices.

155. As such, the ’693 inventions thereby prevent malware attacks more thoroughly and with better efficiency, which represents a concrete improvement over prior art techniques.

156. The claims of the ’693 Patent contain an inventive concept to improve the functioning of computers and other networked devices. Claims 1, 3, 5, and 8 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the ’693 Patent application was filed. These ordered combinations are set forth in claims 1, 3, 5, and 8 of the ’693 Patent. The ordered combinations of elements in claim 1, 3, 5, and 8 were not well understood, routine or conventional at the time the ’693 Patent application was filed. The ordered combinations of the inventions of claims 1, 3, 5, and 8 are practical, particular, non-conventional, and non-generic techniques of protecting a client computer from malware transmitted over a network such as the Internet.

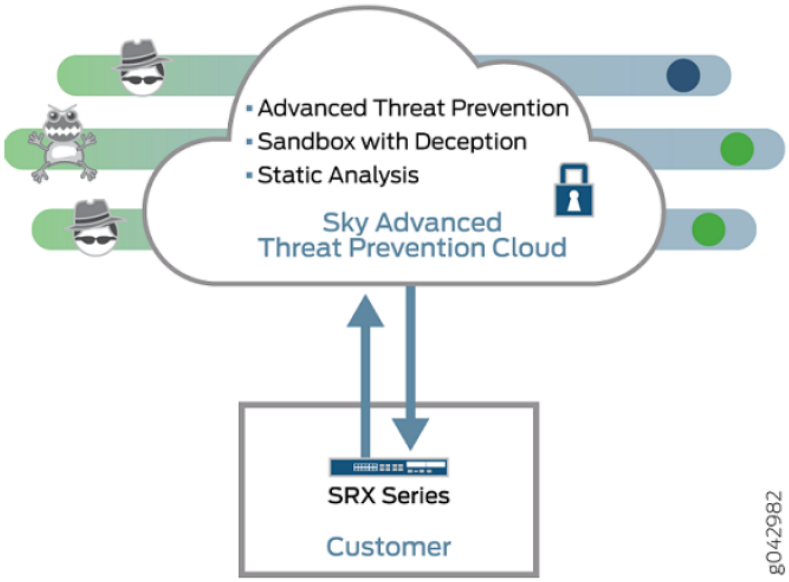
157. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1, 3, 5, and 8 of the ’693 Patent

by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the '693 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Juniper SRX Series and/or virtualized SRX ("vSRX") Services Gateways supporting Juniper Sky Advanced Threat Protection ("Juniper ATP Client Products") and the Juniper Sky Advanced Threat Protection Appliance and/or Cloud service ("Juniper ATP Server Products") (collectively, "Juniper ATP Products").

158. Juniper ATP Client Products are network devices that alert against unknown malicious codes. *See, e.g.*, https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/pathway-pages/sky-atp-admin-guide.pdf at 3-4:

About Juniper Sky Advanced Threat Prevention

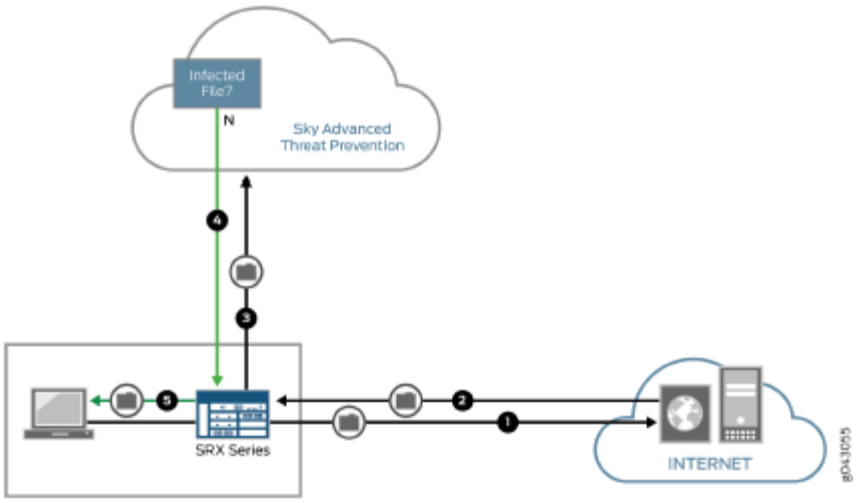
Juniper Sky™ Advanced Threat Prevention (Juniper Sky ATP) is a security framework that protects all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system. See Figure 1 on page 4.



Juniper Sky ATP protects your network by performing the following tasks:

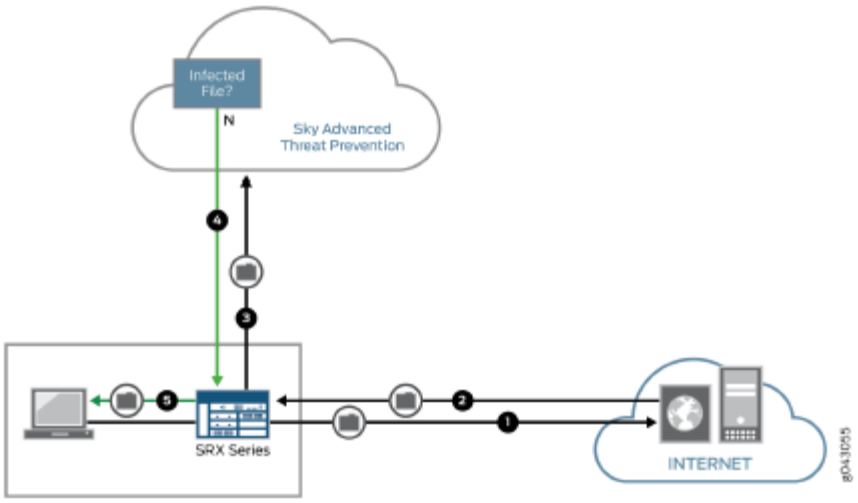
- The SRX Series device extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.
- The SRX Series device blocks known malicious file downloads and outbound C&C traffic.

159. Juniper ATP Client Products receive a request sent by a terminal for obtaining a file from a network entity and a data stream carrying the file. *See, e.g., id.* at 8:



Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.

160. Juniper ATP Client Products record a source path carried in the request, wherein the network entity provides the file on the source path. *See, e.g., id.* at 8, 157-158, 181:



Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.

HTTP File Download Overview

Access this page from the Monitor menu.

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures or URLs. From the main page, click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.

URL	The URL from which the file originated. NOTE: Enter text in the space at the top of the column to filter the data.

Juniper Sky Advanced Threat Prevention Policy Overview

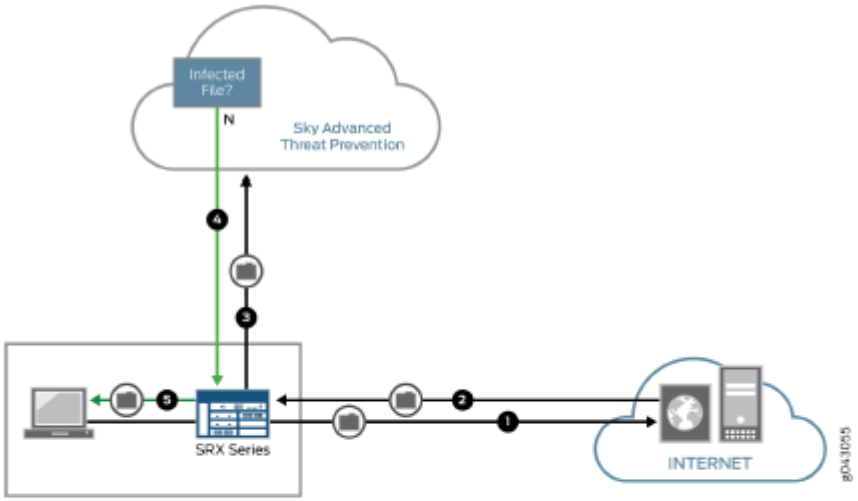
The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

161. Juniper ATP Client Products judge whether the file is an executable file according to at least one of: the request and the data stream carrying the file. *See, e.g.*, *id.* at 7-8, 95:

How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see "How is Malware Analyzed and Detected?" on page 10.



Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.

Benefits of File Inspection Profiles

- Allows you to create file categories to send to the cloud for scanning rather than having to list every single type of file you want scanned.
- Allows you to configure multiple scanning categories based on file type, adding and removing file types when necessary, increasing or decreasing granularity.

Table 20: File Category Contents

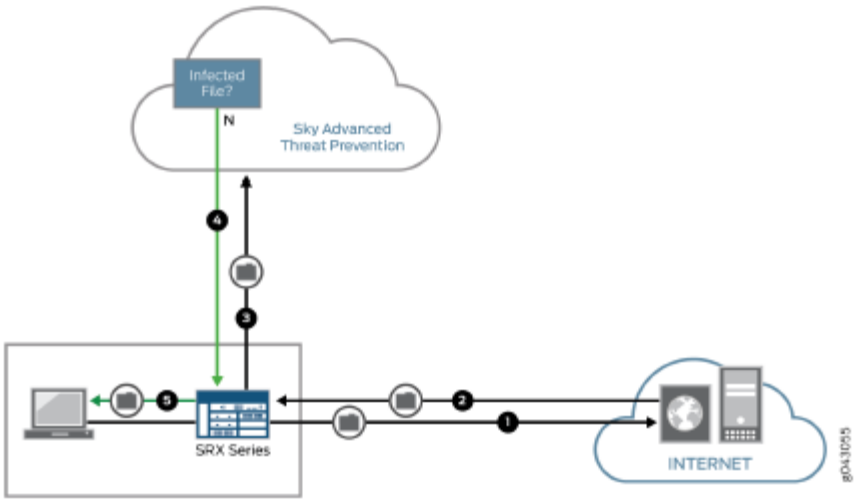
Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
ELF	Executable and Linkable Format (ELF) is a standard file format for executable files, object code, and libraries.

162. When the Juniper ATP Client Products judge the file is an executable file, the Juniper ATP Client Products send first alert information that carries the source path to a monitoring device. *See, e.g., id.* at 7-8, 181:

How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see "How is Malware Analyzed and Detected?" on page 10.



Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.

Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

163. Juniper ATP Client Products receive second alarm information sent by the monitoring device after further detecting the file downloaded according to the source path by the monitoring device. *See, e.g.*, *id.* at 7, 181:

How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see "How is Malware Analyzed and Detected?" on page 10.

Juniper Sky Advanced Threat Prevention Policy Overview

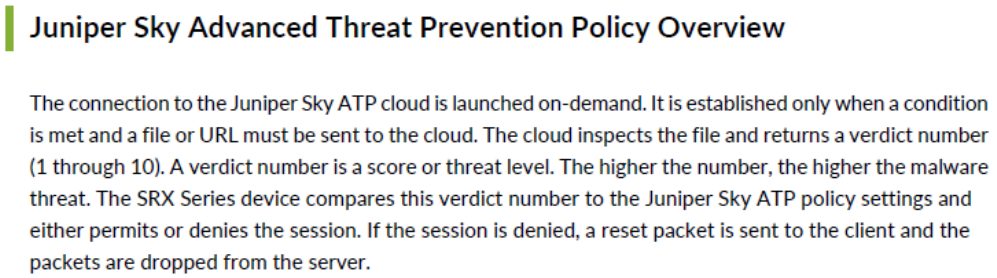
The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

164. Juniper ATP Client Products intercept the executable file according to one of the maliciousness of the executable file; or the executable file and packets transmitted in a Botnet according to the second alarm information comprising the maliciousness of the executable file and Botnet topology information. *See, e.g.*, *id.* at 7, 181:

How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see "How is Malware Analyzed and Detected?" on page 10.



Juniper Sky Advanced Threat Prevention Policy Overview

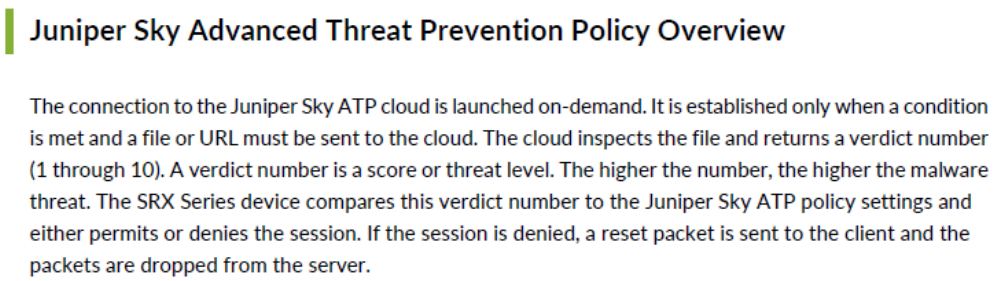
The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

165. With respect to claim 3, Juniper ATP Client Products comprise computing hardware and a non-transitory computer-readable storage medium including computer-executable instructions executed by the computing hardware to perform the operations recited in paragraphs 158 through 164 above.

166. With respect to claim 5, Juniper ATP Products are a system comprising a network device (e.g., a Juniper ATP Client Product) and a monitoring device (e.g., a Juniper ATP Server Product).

167. Juniper ATP Client Products comprise a first computing hardware and a first non-transitory computer-readable storage medium including a first set of computer-executable instructions executed by the first computing hardware to perform, on the network device, the operations recited in paragraphs 158 through 164 above.

168. Juniper ATP Server Products receive the first alert information from the network device. *See, e.g.*, *id.* at 181:



Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

169. Juniper ATP Server Products download an executable file according to the source path. *See, e.g., id.* at 181, 158:

Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Table 35: HTTP Scanning Data Fields *(continued)*

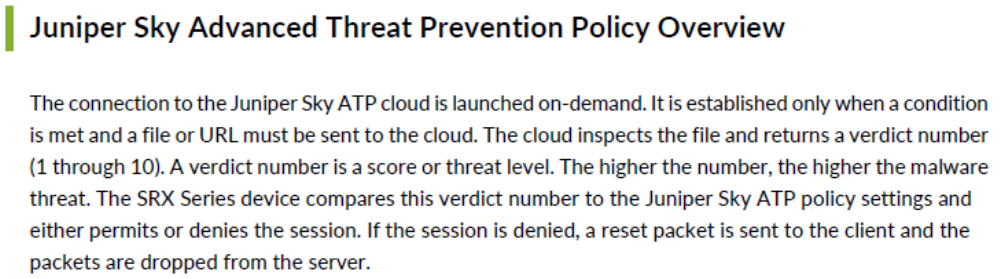
Field	Definition
Threat Level	The threat score. **NOTE:** Click the three vertical dots at the top of the column to filter the information on the page by threat level.
Filename	The name of the file, including the extension. **NOTE:** Enter text in the space at the top of the column to filter the data.
Last Submitted	The time and date of the most recent scan of this file.
URL	The URL from which the file originated.

170. Juniper ATP Server Products detect the executable file to confirm maliciousness of the executable file. *See, e.g., id.* at 181:

Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

171. Juniper ATP Server Products send the second alarm information to the network device, wherein the second alarm information comprises one of: maliciousness of the executable file, and both the maliciousness of the executable file and Botnet topology information. *See, e.g., id.* at 181:



Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

172. Juniper ATP Server Products comprise a second computing hardware and a second non-transitory computer-readable storage medium including a second set of computer-executable instructions executed by the second computing hardware to perform the operations recited in paragraphs 168 through 171 above.

173. With respect to claim 8, Juniper ATP Client Products comprise a non-transitory computer readable medium storing instructions for execution by a processor, the instructions causing the processor to be configured to provide the operations recited in paragraphs 158 through 164 above.

174. As such, on information and belief, Verizon has directly infringed at least claims 1, 3, 5, and 8 of the '693 Patent by at least, for example, making, using, selling, and offering for sale Juniper ATP Products. For example, "Verizon Wireless has selected Juniper Networks' SRX Series Services Gateway to provide added network protection for mobile data users." https://www.convergedigest.com/2010/02/verizon-wireless-selects-juniper-srx.html. On information and belief, Verizon uses multiple Juniper ATP Client Products in its network that are used with the Juniper ATP Server Products:

Managed Devices. Applicable MRCs and NRCs in the Contract are based on management type and size of Managed Device, as listed below. Device models not identified here are "nonstandard CPE." Verizon may impose different terms for Managed WAN that it provides for nonstandard CPE, or decline to provide Managed WAN for nonstandard CPE in whole or in part, at its sole discretion. Customer acknowledges that certain device models may support Router Management and not SD WAN Management, or vice versa.

4.1 **Extra Small:**

- CISCO ROUTERS: 8XX Series;
- JUNIPER ROUTERS: SRX 1XX
- ADTRAN NETVANTA ROUTER: Special 3201 Model
- DIGI ROUTERS: WR-44
- CradlePoint: MBR1xxx, IBR6xx
- Viptela: vEdge 1xx

4.2 **Small:**

- CISCO ROUTERS: Series 1XXX, 2XXX, and 43xx Series;
- ADTRAN NETVANTA ROUTERS: Series 1XXX, 2XXX, and 3XXX;
- ADTRAN TOTAL ACCESS ("TA") ROUTERS: Series 9xx;
- JUNIPER ROUTERS: J23XX and J43XX; SRX 2xx and 3xx Series; NFXxxx
- NORTEL ROUTERS Series 1XXX
- Viptela: vEdge 1xxx

4.3 **Medium:**

- CISCO ROUTERS: Series 3XXX and 44XX;
- ADTRAN NETVANTA ROUTERS: Series 4XXX and 5XXX;
- JUNIPER ROUTERS: J63XX; SRX 6xx Series
- NORTEL ROUTERS Series 3XXX
- Viptela: vEdge 2xxx

https://enterprise.verizon.com/service_guide/reg/cp_mwan_plus_managed_wan_service_2016JUL15_mk.htm.

Juniper Sky ATP Component Support Table

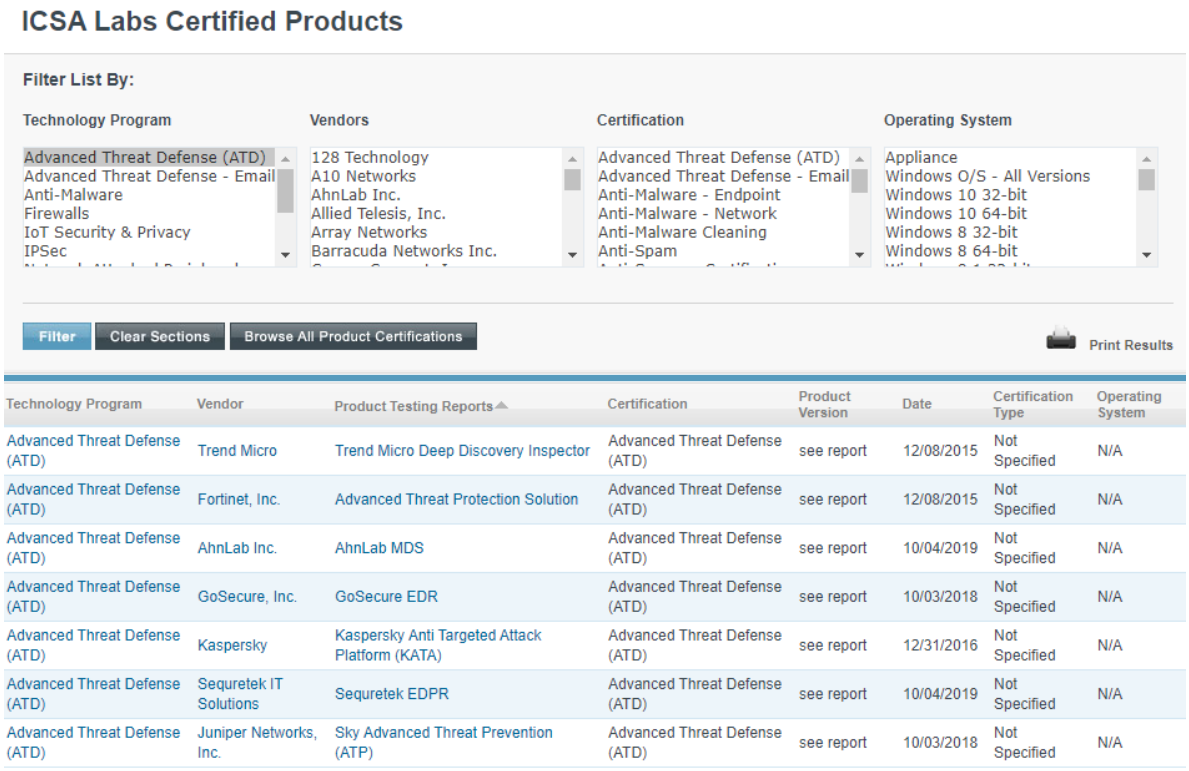
The following product versions have been tested and are supported with Juniper Sky ATP.

Platform	Hardware Requirements	Software Versions
vSRX Series		Junos 15.1X49-D60 and above
SRX Series	SRX320, SRX300	Junos 18.3R1 and above
SRX Series	SRX4100, SRX4200, SRX4600	Junos 15.1X49-D65 and above for SRX4100 and SRX4200 Junos 17.4R1-S1 and above for SRX4600
SRX Series	SRX340, SRX345, SRX550m	Junos 15.1X49-D60 and above
SRX Series	SRX5800, SRX5600, SRX5400	Junos 15.1X49-D50 and above
SRX Series	SRX1500	Junos 15.1X49-D33 and above

https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-supported-platforms-guide.pdf. As another example, on information and belief, Verizon uses the Juniper ATP Server Products:

> Following ICSA Labs' recently completed Q2 2019 advanced threat defense (ATD) and ATD-email test cycle, security solutions from 5 security vendors - Fortinet, GoSecure - Powered by CounterTack, Juniper, Kaspersky and Trend Micro - were able to detect most new and little known malicious threats while having minimal false positives.

https://www.icsalabs.com/news-article/five-security-solutions-maintain-icsa-labs-advanced-threat-defense-atd-certification-af. The Juniper ATP Server Products are used for free by supported Juniper ATP Client Products. https://www.juniper.net/documentation/en_US/release-independent/licensing/topics/topic-map/advanced-threat-prevention-licensing.html#id-licenses-for-juniper-sky-advanced-threat-prevention-atp ("The free model solution is available on all supported SRX Series devices (see the Supported Platforms Guide) and for customers that have a valid support contract, but only scans executable file types (see Juniper Sky Advanced Threat Prevention Profile Overview). Based on this result, the SRX Series device can allow the traffic or perform inline blocking.").



ICSA Labs Certified Products

Filter List By:

Technology Program	Vendors	Certification	Operating System
Advanced Threat Defense (ATD)	128 Technology	Advanced Threat Defense (ATD)	Appliance
Advanced Threat Defense - Email	A10 Networks	Advanced Threat Defense - Email	Windows O/S - All Versions
Anti-Malware	AhnLab Inc.	Anti-Malware - Endpoint	Windows 10 32-bit
Firewalls	Allied Telesis, Inc.	Anti-Malware - Network	Windows 10 64-bit
IoT Security & Privacy	Array Networks	Anti-Malware Cleaning	Windows 8 32-bit
IPSec	Barracuda Networks Inc.	Anti-Spam	Windows 8 64-bit

Filter | Clear Sections | Browse All Product Certifications | Print Results

Technology Program	Vendor	Product Testing Reports	Certification	Product Version	Date	Certification Type	Operating System
Advanced Threat Defense (ATD)	Trend Micro	Trend Micro Deep Discovery Inspector	Advanced Threat Defense (ATD)	see report	12/08/2015	Not Specified	N/A
Advanced Threat Defense (ATD)	Fortinet, Inc.	Advanced Threat Protection Solution	Advanced Threat Defense (ATD)	see report	12/08/2015	Not Specified	N/A
Advanced Threat Defense (ATD)	AhnLab Inc.	AhnLab MDS	Advanced Threat Defense (ATD)	see report	10/04/2019	Not Specified	N/A
Advanced Threat Defense (ATD)	GoSecure, Inc.	GoSecure EDR	Advanced Threat Defense (ATD)	see report	10/03/2018	Not Specified	N/A
Advanced Threat Defense (ATD)	Kaspersky	Kaspersky Anti Targeted Attack Platform (KATA)	Advanced Threat Defense (ATD)	see report	12/31/2016	Not Specified	N/A
Advanced Threat Defense (ATD)	Sequretek IT Solutions	Sequretek EDPR	Advanced Threat Defense (ATD)	see report	10/04/2019	Not Specified	N/A
Advanced Threat Defense (ATD)	Juniper Networks, Inc.	Sky Advanced Threat Prevention (ATP)	Advanced Threat Defense (ATD)	see report	10/03/2018	Not Specified	N/A

https://www.icsalabs.com/products?tid%5b%5d=5352.

https://www.juniper.net/assets/uk/en/local/pdf/infographics/3050066-en.pdf. ICSA Labs is a division of Verizon. *See, e.g.*, https://www.icsalabs.com/about-icsa-labs.

175. On information and belief, Verizon has infringed at least claims 1, 3, 5, and 8 of the '693 Patent by inducing others to infringe at least claims 1, 3, 5, and 8 of the '693 Patent in violation of 35 U.S.C. § 271(b).

176. On information and belief, Verizon takes active steps to induce infringement of at least claims 1, 3, 5, and 8 of the '693 Patent by others, including its customers, and Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. Such active steps include, but are not limited to, encouraging, advertising (including by internet websites, television, store displays, print advertisements, *etc.*), promoting, and instructing others to use network services that utilize Juniper ATP Products. *See supra*, paragraph 174; *see also* https://digiworld.news/news/36143/verizon-cloud-marketplace-simplifies-cloud-purchasing-experience ("Verizon Enterprise Solutions is simplifying the cloud-purchasing experience for its clients, with the launch of Verizon Cloud Marketplace, a key

foundational component of the company's robust ecosystem of enterprise-class technologies. . . . A virtualized version of the award-winning Juniper Networks SRX Series Services Gateway, Firefly Perimeter can be easily deployed and managed centrally or individually as a full-featured virtual firewall for each department, application or tenant."); https://investor.juniper.net/investor-relations/press-releases/press-release-details/2016/Juniper-Networks-Joins-Verizons-Tech-Partner-Ecosystem-for-Virtual-Network-Services/default.aspx ("Verizon business customers can elect to use Juniper Networks vSRX, one of the industry's most efficient and powerful virtual firewalls, as a VNF through Verizon's Virtual Network Services to protect data assets and remove network threats. As one of the industry's fastest virtual security and routing platforms available, Juniper Networks vSRX delivers core firewall, networking, advanced security and automated lifecycle management for cloud environments."); https://www.channelfutures.com/cloud-2/verizon-launches-cloud-marketplace ("Verizon Enterprise Solutions has announced the launch of Verizon Cloud Marketplace, the company's online storefront for cloud-based services. As of the launch, the Cloud Marketplace features pre-built cloud services from several partner companies, including AppDynamics, Hitachi Data Systems, Juniper Networks (JNPR), pfSense and Tervela."); https://www.cloudcomputing-news.net/news/2014/nov/19/verizon-announces-its-cloud-marketplace-open-business/ ("Verizon Enterprise Solutions has announced the official launch of its Verizon Cloud Marketplace, a store for software certified to operate in the Verizon cloud. The communications provider has been aggressive in its cloud push in recent months, and is opening up this one-stop shop with a variety of partners, including AppDynamics, Hitachi and Juniper Networks.").

177. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1, 3, 5, and 8 of the '693 Patent, including for example, by prompting them to use network services that utilize Juniper ATP Products.

178. On information and belief, Verizon contributes to the infringement of at least claims 1, 3, 5, and 8 of the '693 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or importation by Verizon of network services that utilize Juniper ATP Products. Such Juniper ATP Products are especially made for or adapted for use to infringe at least claims 1, 3, 5, and 8 of the '693 Patent and are at least a material part of those claims, for example, as described above with respect to claim 1. The Juniper ATP Products, including the functionality contributing to infringement of the '693 Patent, are not suitable for substantial noninfringing use.

179. By way of at least Huawei's notice to Verizon in February 2019 and on March 29, 2019 (as well as this Complaint), Verizon knows of the '693 Patent and performs acts that it knows, or should know, induce and/or contribute to the direct infringement of at least claims 1, 3, 5, and 8 of the '693 Patent by third parties.

180. Verizon undertook and continues its infringing actions despite an objectively high likelihood that such activities infringed the '693 Patent, which is presumed valid. For example, Verizon has been aware of an objectively high likelihood that its actions constituted, and continue to constitute, infringement of the '693 Patent and that the '693 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the '693 Patent, nor could it reasonably subjectively believe that the '693 Patent is invalid. Despite that knowledge, subjective belief, and the objectively high

likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the '693 Patent.

181. Huawei has been irreparably harmed by Verizon's infringement of the '693 Patent and will continue to be harmed unless and until Verizon's infringement is enjoined by this Court.

182. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the '693 Patent pursuant to 35 U.S.C. § 271.

COUNT IV: INFRINGEMENT OF PATENT NO. 7,609,288

183. Huawei realleges and incorporates by reference Paragraphs 1-182 above, as if fully set forth herein.

184. The U.S. Patent Office duly and properly issued the '288 Patent, entitled "Method and apparatus of transferring the desktop of PC to video communication terminal," on October 27, 2009. Huawei Technologies is the assignee of all right, title, and interest in and to the '288 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the '288 Patent is valid and enforceable. A true and correct copy of the '288 Patent is attached hereto as Exhibit D.

185. The '288 Patent provides novel, useful and more effective and efficient techniques for transferring desktop information of a PC to a video communication terminal (e.g., a local video communication terminal and a remote video communication terminal) that overcome the problems of the prior art and thereby improve the functioning of computer and network equipment. *See, e.g.*, '288 Patent at Abstract.

186. The '288 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problem of transferring desktop information of a PC to a video communication terminal. '288 Patent at 1:16-19. With the rising demand for reliable video communications and videoconferencing,

conference participants frequently need to transfer desktop information to a location with high quality and efficient network utilization. *Id.* at 1:24-29. Previous attempts to solve this problem had various disadvantages. *Id.* at 1:44-46.

187. Before the invention of the ’288 Patent, one solution involved projecting desktop information of a PC with a projector, capturing the projected image with the video camera of a local videoconference terminal, and transferring the desktop information to a remote video communication terminal after processing. *Id.* at 1:30-36. The ’288 Patent recognized that, in order to maintain higher clarity, this solution required the captured image to be smaller. *Id.* at 1:46-49.

188. Another solution from before the invention of the ’288 Patent involved transforming the desktop information to a standard PAL/NTSC (Phase Alternating Line/National Television System Committee) format signal with a VGA (Video Graphic Array) converter, inputting the PAL/NTSC format signal to the local videoconference terminal as one of the video source signals, and transferring the desktop information to a remote video communication terminal after processing. *Id.* at 1:36-43. The ’288 Patent recognized that there is a loss in the VGA converter during the conversion of the digital signal to an analog signal, so the clarity of the images decreases greatly. *Id.* at 1:49-56. Thus, prior to the inventions of the ’288 Patent, there existed a need for a higher quality and more efficient method for transferring desktop information of a PC to a video communication terminal.

189. The inventions of the ’288 Patent provide technical solutions to the problems in the prior art described above. The ’288 Patent describes, for example, capturing desktop information of the PC after receiving a triggering command, and converting a PC format of the desktop information into a format of a local video communication terminal. *Id.* at 2:1-4. The

converted desktop format is encoded in a mode ensured by the local video communication terminal and sent to the local video communication terminal. *Id.* at 2:5-8. The local video communication terminal receives the coded bit stream and transfers the coded bit stream to a remote video communication terminal through a transmission channel after processing. *Id.* at 2:9-12.

190. The inventions of the ’288 Patent improve computer and network equipment functionality by improving and solving problems in a computer or networked device’s capability of transferring desktop information of a PC to a video communication terminal with higher quality and better efficiency. The inventions of the ’288 Patent provide a computer-based solution to a computer-specific problem. The inventions of the ’288 Patent are improvements over the prior art and other techniques for transferring desktop information of a PC to a video communication terminal, and the ’288 Patent enables a combination of features not present in the prior art and other techniques.

191. For example, the inventions of the ’288 Patent provide for improved computer and network operation by transferring desktop information of a PC directly in a digital coded bit stream mode without converting the digital signal to analog signal. This provides the additional advantage of avoiding the losses associated with a VGA converter and improving the clarity at the video communication terminal.

192. As another example, the inventions of the ’288 Patent provide for improved computer and network operation by allowing the desktop information to be pre-processed before transmission. This allows for a reduction in the amount of bandwidth required. This also allows for the displayed content to include text files, films, or anything else that can be displayed on a PC screen.

193. As another example, the inventions of the ’288 Patent provide for improved computer and network operation by allowing moving images and the desktop information to be transmitted simultaneously or alternatively. *See, e.g.*, ’288 Patent at 2:47-48.

194. The claims of the ’288 Patent contain an inventive concept to improve the functioning of computers and other networked devices. Claims 1, 2, 5, 7, 9, 10, 12, and 14 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the ’288 Patent application was filed. These ordered combinations are set forth in claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent. The ordered combinations of elements in claim 1, 2, 5, 7, 9, 10, 12, and 14 were not well understood, routine or conventional at the time the ’288 Patent application was filed. The ordered combinations of the inventions of claims 1, 2, 5, 7, 9, 10, 12, and 14 are practical, particular, non-conventional and non-generic techniques of transferring desktop information of a PC to a remote video communication terminal.

195. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the ’288 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Cisco Webex from Verizon, and/or Cisco room video endpoints such as the Cisco MX, SX, and IX series, and Cisco Spark Room Series, and/or the components thereof, which allow for transferring desktop information of a PC to a remote video communication terminal. In addition, users of Cisco Webex from Verizon infringe at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent by, for example, using the capabilities of

Cisco Webex from Verizon to transfer desktop information of a PC to a video communication terminal.

196. Cisco Webex from Verizon transfers desktop information of a PC to a video communication terminal. For example, Cisco Webex from Verizon transfers desktop information of a PC to either a local or remote participant. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html ("Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.").

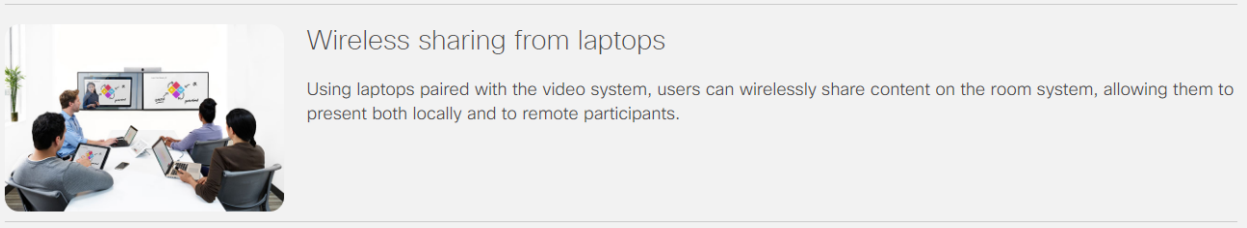
197. Cisco Webex from Verizon captures desktop information of the PC after receiving a triggering command. For example, Cisco Webex from Verizon captures desktop information at certain intervals, resulting in "snapshots" of desktop information. *See, e.g.*, https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

198. Cisco Webex from Verizon converts a PC format of the desktop information into a format of a local video communication terminal. For example, Cisco Webex from Verizon converts a PC format of the desktop information into a format of a local Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

199. Cisco Webex from Verizon encodes the converted desktop format in a mode ensured by the local video communication terminal. For example, Cisco Webex from Verizon encodes the converted desktop information into a mode ensured by the local Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

200. Cisco Webex from Verizon sends the coded bit stream to the local video communication terminal. For example, Cisco Webex from Verizon sends the coded bit stream to the local Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

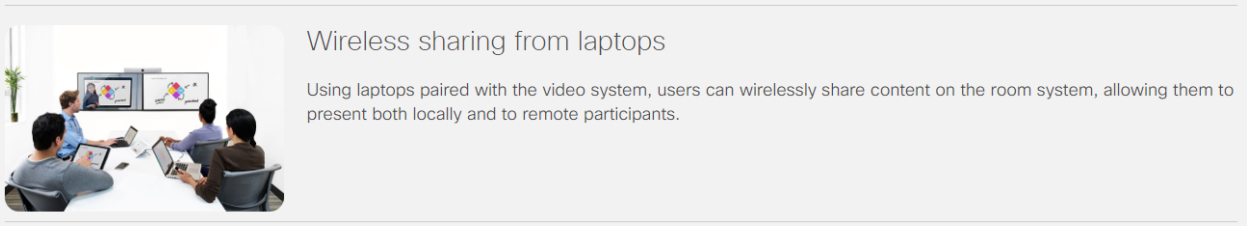
Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

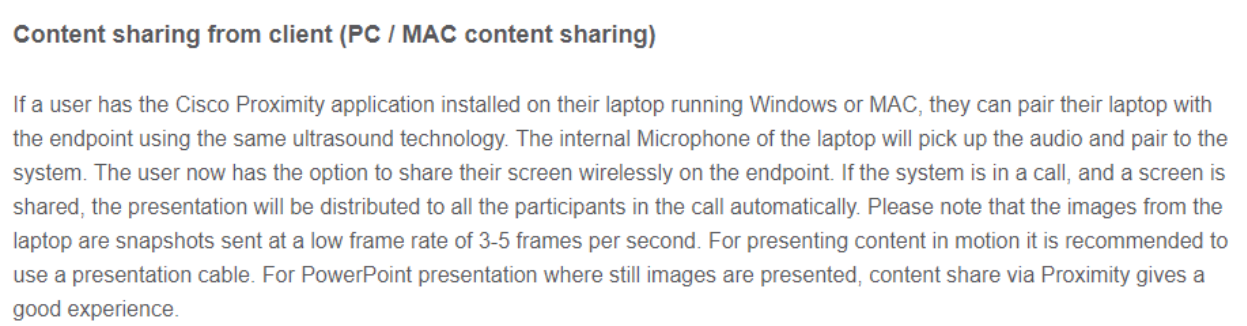
https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

201. Cisco Webex from Verizon receives the coded bit stream by the local video communication terminal. For example, the local Cisco room video endpoint receives the coded bit stream. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



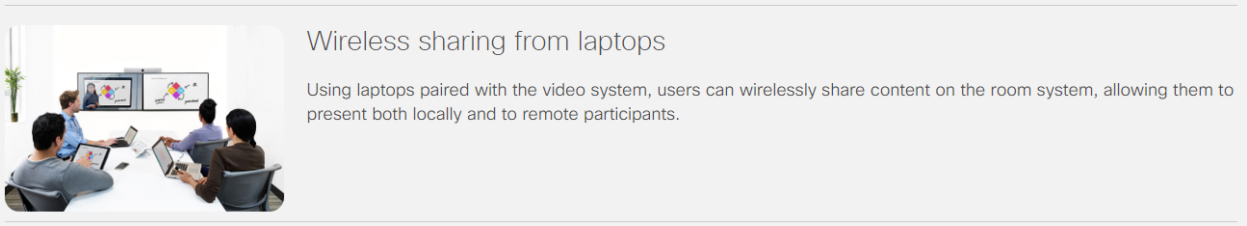
Id.

Id.



https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

202. Cisco Webex from Verizon transfers the coded bit stream to a remote video communication terminal through transmission channel after processing. For example, Cisco Webex from Verizon transfers the coded bit stream to any remote participants in the call after processing. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

203. With respect to claim 2, Cisco Webex from Verizon pre-processes the captured desktop information. *See, e.g.*, https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

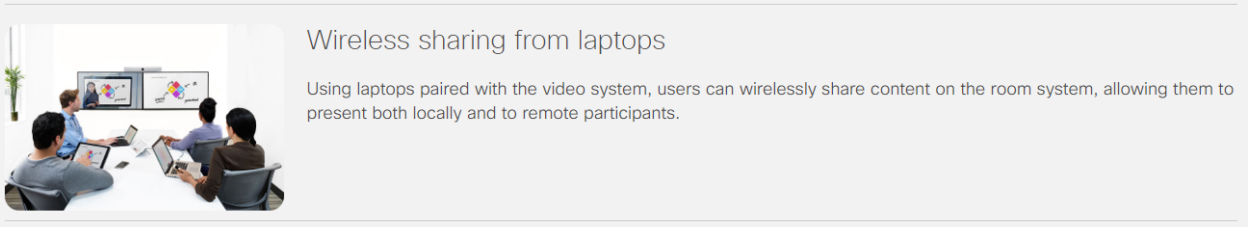
Id.

204. With respect to claim 5, Cisco Webex from Verizon captures desktop information of the PC from a video memory of the PC.

205. With respect to claim 7, Cisco Webex from Verizon simultaneously transfers the coded bit stream of the desktop information and that of a local image in a multiplex encoding mode.

206. With respect to claim 9, Verizon uses an apparatus for transferring desktop information of a PC to a video communication terminal. For example, a PC with Cisco Webex from Verizon transfers desktop information of a PC to either a local or remote participant. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html ("Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.").

207. Further with respect to claim 9, Verizon uses an apparatus comprising a background processing-device, capturing desktop information of the PC, converting the captured desktop information from a PC format to a format of a local video communication terminal. For example, a PC with Cisco Webex from Verizon captures desktop information of the PC and converts a PC format of the desktop information into a format of a local Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

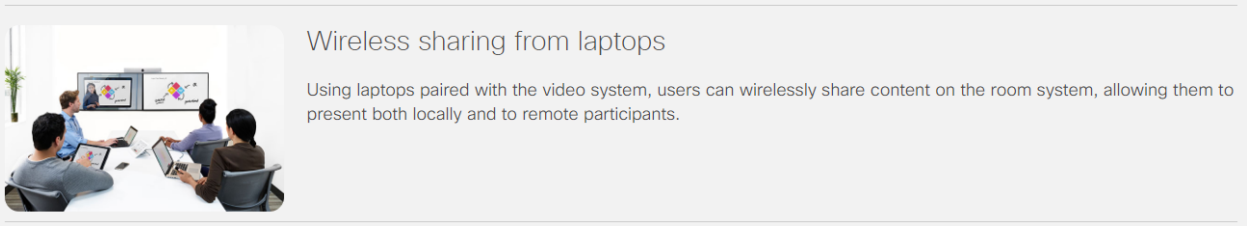
Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

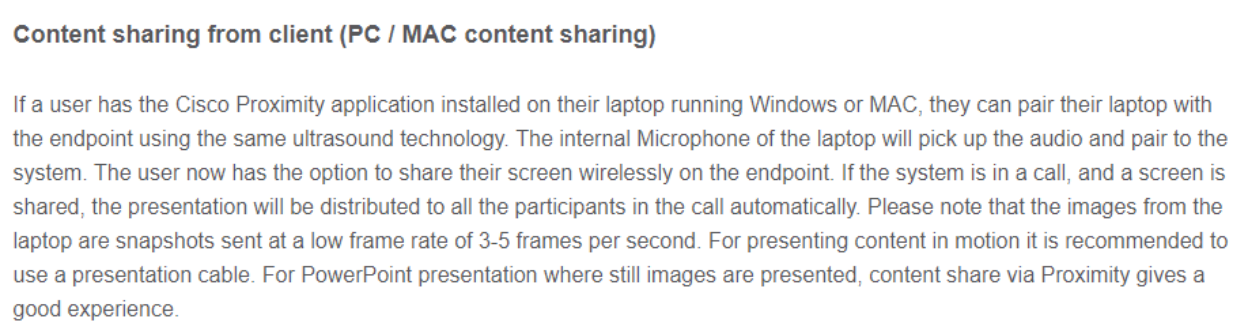
https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

208. Further with respect to claim 9, Verizon uses an apparatus comprising a background processing-device, encoding the converted format to a coded bit stream and outputting. For example, a PC with Cisco Webex from Verizon encodes the converted desktop information into a coded bit stream and outputs to the local Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



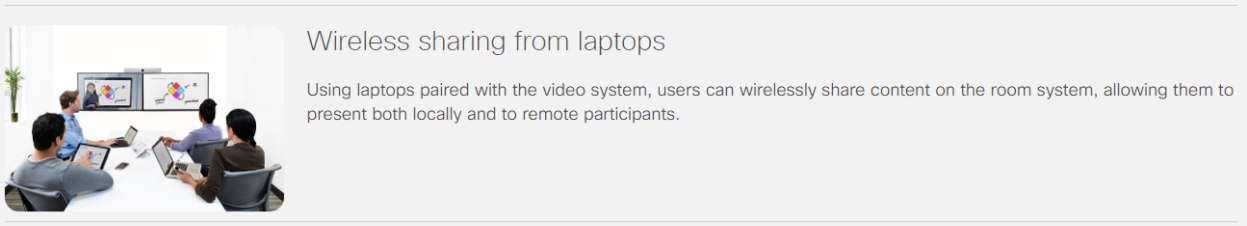
Id.

Id.



https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

209. Further with respect to claim 9, Verizon uses an apparatus further comprising a terminal processing-device, transferring the coded bit stream from the background processing-device to a remote video communication terminal. For example, a local Cisco room video endpoint transfers the coded bit stream to any remote participants in the call. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

210. With respect to claim 10, Verizon uses an apparatus wherein the background processing-device comprises: a capture driver, sending out a triggering command; a capturing device, receiving the triggering command from the capture driver and capturing the desktop information, then outputting; an image converter, receiving the captured desktop information from the capturing device and converting into the format of the local video communication terminal, then outputting; a background encoder, encoding output signal from said image converter into the coded bit stream; and a background bit stream sender, sending the coded bit stream to the terminal processing-device. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

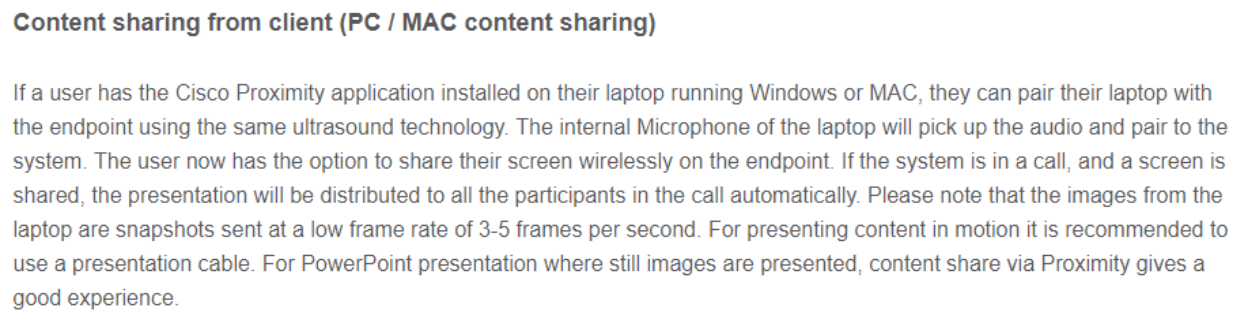
211. With respect to claim 12, Verizon uses an apparatus wherein the terminal processing-device comprises a terminal bit stream transmitter that transfers the coded bit stream to the remote video communication terminal. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

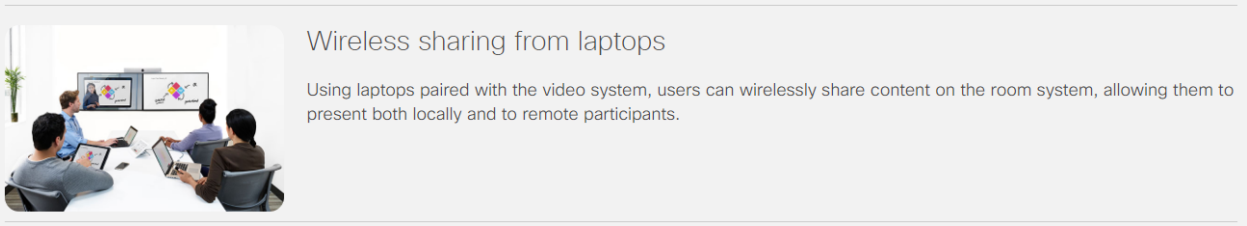
Id.

Id.



https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

212. With respect to claim 14, Verizon uses an apparatus wherein the terminal processing-device further comprises a terminal encoder that encodes a local image and then outputs to the terminal bit stream transmitter. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

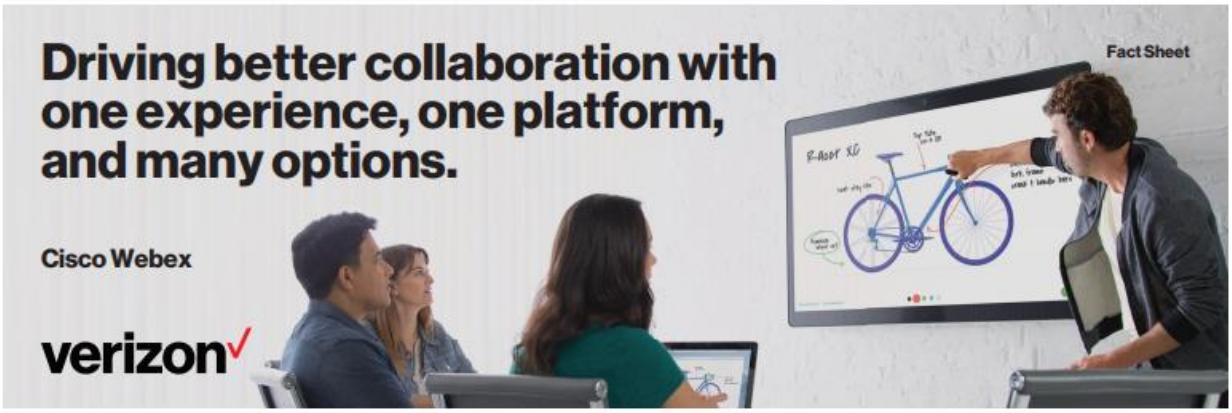
https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

213. As such, on information and belief, Verizon has directly infringed at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent by at least, for example, performing testing of Cisco Webex from Verizon.

214. On information and belief, Verizon has infringed at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent by inducing others, including users of Cisco Webex from Verizon that it sells and/or offers, to infringe at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent in violation of 35 U.S.C. § 271(b).

215. On information and belief, Verizon takes active steps to induce infringement of at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the ’288 Patent by others, including its customers, and Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. Such active steps include, but are not limited to, encouraging, advertising (including by internet websites, television, store displays, print advertisements, *etc.*),

promoting, and instructing others to use and/or how to transfer desktop information of a PC to a video communication terminal. Such video communication terminals include those made, sold, offered for sale, and/or imported by Verizon, such as the various Cisco room video endpoints. For example, Verizon induces users of Cisco Webex by Verizon to use one or more claimed inventions of the '288 Patent by instructing users how to transfer desktop information of a PC to a video communication terminal, such as a Cisco room video endpoint. *See, e.g.*, https://enterprise.verizon.com/products/business-communications/unified-communications-and-collaboration/cisco-webex/.



https://enterprise.verizon.com/resources/factsheets/2018/cisco-webex.pdf. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the '288 Patent.

216. On information and belief, Verizon contributes to the infringement of at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the '288 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or importation by Verizon of Cisco Webex by Verizon and/or Cisco room video endpoints. Such Cisco Webex by Verizon and/or Cisco room video endpoints are especially made for or adapted for use to infringe claims 1, 2, 5, 7, 9, 10, 12, and 14 of the '288

Patent and are at least a material part of those claims, for example, as described above with respect to claim 1. Cisco Webex by Verizon and/or Cisco room video endpoints, including the functionality contributing to infringement of the '288 Patent, are not suitable for substantial noninfringing use.

217. By way of at least Huawei's notice to Verizon on March 29, 2019 (as well as this Complaint), Verizon knows of the '288 Patent and performs acts that it knows, or should know, induce and/or contribute to the direct infringement of at least claims 1, 2, 5, 7, 9, 10, 12, and 14 of the '288 Patent by third parties.

218. Verizon undertook and continues its infringing actions despite a high likelihood that such activities infringed the '288 Patent, which is presumed valid. For example, Verizon has been aware of a high likelihood that its actions constituted, and continue to constitute, infringement of the '288 Patent and that the '288 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the '288 Patent, nor could it reasonably subjectively believe that the patent is invalid. Despite that knowledge, subjective belief, and the objectively high likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the '288 Patent.

219. Huawei has been irreparably harmed by Verizon's infringement of the '288 Patent and will continue to be harmed unless and until Verizon's infringement is enjoined by this Court.

220. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the '288 Patent pursuant to 35 U.S.C. § 271.

COUNT V: INFRINGEMENT OF PATENT NO. 9,521,366

221. Huawei realleges and incorporates by reference Paragraphs 1-220 above, as if fully set forth herein.

222. The U.S. Patent Office duly and properly issued the '366 Patent, entitled "Method and apparatus for playing conference signal, video conference terminal, and mobile device" on December 13, 2016. Huawei Technologies is the assignee of all right, title, and interest in and to the '366 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the '366 Patent is valid and enforceable. A true and correct copy of the '366 Patent is attached hereto as Exhibit E.

223. The '366 Patent provides novel, useful and more effective and efficient techniques for playing a conference signal that overcome the problems of the prior art and thereby improve the functioning of computer and network equipment. *See, e.g.*, '366 Patent at Abstract.

224. The '366 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problem of playing a conference signal. '366 Patent at 1:17-20. With the rising demand for reliable video communications and videoconferencing, conference participants frequently need to display a main stream signal and a presentation stream signal at the same time. *Id.* at 1:24-62. Previous attempts to solve this problem included various disadvantages. *Id.* at 2:12-17.

225. Before the invention of the '366 Patent, one solution required the presentation stream signal to be displayed on a display device of the site in a picture in picture (PIP) manner, that is, to display the main stream signal in full screen, and display the presentation stream signal in an inset window, or display the presentation stream signal in full screen, and display the main stream signal in an inset window. *Id.* at 1:67-2:11. The '366 Patent recognized that a size of a signal displayed in an inset window is relatively small, and a signal that is displayed in an inset window blocks a part of a signal that is displayed in full screen, which leads to relatively

undesirable effects of displaying the main stream signal and the presentation stream signal. *Id.* at 2:12-17. Thus, prior to the inventions of the '366 Patent, there existed a need for a higher quality and more efficient method for displaying a main stream signal and a presentation stream signal at the same time.

226. The inventions of the '366 Patent provide technical solutions to the problems in the prior art described above. The '366 Patent describes, for example, establishing a connection channel between a mobile device held by a conference participant located at a site and a video conference terminal located at the site. *Id.* at 2:32-36. A first type of signal is sent through the connection channel to the mobile device for play. *Id.* at 2:36-40. A second type of signal is sent to a primary playing device of the site for play. *Id.* at 2:40-42. When the first type signal is a presentation stream signal, the second type signal is a main stream signal, and when the first type signal is the main stream signal, the second type signal is the presentation stream signal. *Id.* at 2:42-46.

227. The inventions of the '366 Patent improve computer and network equipment functionality by improving and solving problems in a computer or networked device's capability of playing a conference signal with higher quality and better efficiency. The inventions of the '366 Patent provide a computer-based solution to a computer-specific problem. The inventions of the '366 Patent are improvements over the prior art and other techniques for playing a conference signal, and the '366 Patent enables a combination of features not present in the prior art and other techniques.

228. For example, the inventions of the '366 Patent provide for improved computer and network operation by displaying a main stream signal and a presentation stream signal without requiring one signal to be displayed in an inset window. This provides the additional

advantage of improving the display's quality and avoiding an inset window blocking a part of a signal that is displayed in full screen.

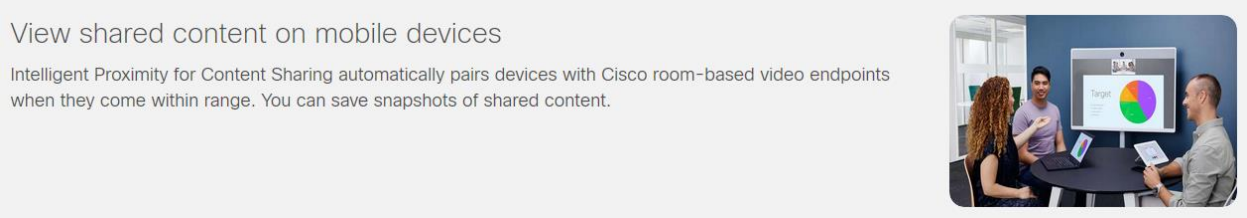
229. As another example, the inventions of the '366 Patent provide for improved computer and network operation by establishing a connection channel between a plurality of mobile devices held by a plurality of conference participants located at a site and a video conference terminal located at the site. As such, the '366 inventions thereby allow users to play a conference signal, for example, with higher quality and more efficiency, which represents a concrete improvement over prior art techniques.

230. The claims of the '366 Patent contain an inventive concept to improve the functioning of computers and other networked devices. Claims 1, 5, 8, 12, 15-17, 19, and 20 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the '366 Patent application was filed. These ordered combinations are set forth in claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent. The ordered combinations of elements in claim 1, 5, 8, 12, 15-17, 19, and 20 were not well understood, routine or conventional at the time the '366 Patent application was filed. The ordered combinations of the inventions of claims 1, 5, 8, 12, 15-17, 19, and 20 are practical, particular, non-conventional and non-generic techniques of playing a conference signal.

231. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the '366 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Cisco Webex from Verizon, mobile devices, Cisco room video

endpoints such as the Cisco MX, SX, IX series and Cisco Spark Room series, and/or the components thereof which allow for playing a conference signal. In addition, users of Cisco Webex from Verizon infringe at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent by, for example, using the capabilities of Cisco Webex from Verizon to play a conference signal.

232. Cisco Webex from Verizon plays a conference signal. For example, Cisco Webex from Verizon plays a conference signal locally and to remote participants. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html ("Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.").



Id.

233. Cisco Webex from Verizon establishes a connection channel between a plurality of mobile devices held by a plurality of conference participants located at a site and a video conference terminal located at the site, wherein the video conference terminal comprises a primary playing device. For example, Cisco Webex from Verizon establishes a connection channel between a plurality of mobile devices held by conference participants and a Cisco room video endpoint, which includes a device with picture, sound, and video playing capabilities. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Maximum simultaneous connections

The solution is using the web server part of the endpoint, this limits the maximum number of simultaneous connections and the number depends on the capabilities of the codec. The following is the maximum number of allowed clients. Exceeding this will display a notification in the application.

Video System model	Maximum simultaneous connections
Cisco TelePresence SX10 and SX10N Quick Set	7
Cisco TelePresence SX20 Quick Set	7
Cisco TelePresence SX80, MX700, MX800 and MX800D	10
Cisco TelePresence MX200 G2 and MX300 G2	7
Cisco DX70 and Cisco DX80	3
Cisco Webex Room Series	7 30*
Cisco Webex Board	7

** From CE9.4.0 if the Proximity service "ContentShare ToClients" is disabled.*

Id.

How Cisco Proximity Works

When the Intelligent Proximity services are enabled on a video endpoint, an inaudible ultrasonic sound token will be played through the video system loudspeakers. The Cisco Proximity client application running on the mobile device will record this token through its integrated microphone. The token contains information on how to connect to the video system over the network.

The mobile device will decode the token and try to establish a secure connection to the video system. To establish the connection, the mobile device needs to be able to reach the IPv4 address of the video system in the room on port 443 (HTTPS).

https://www.cisco.com/c/dam/m/zh_cn/projectworkplace/assets/pdf/proximity-networking.pdf.

234. Cisco Webex from Verizon sends, through the established connection channel, a first type signal in to-be-played signals to each of the mobile devices for play, wherein the to-be-played signals are signals that are received by the video conference terminal and are to be played. For example, Cisco Webex from Verizon sends, through the established connection channel, a slideshow signal in to-be-played signal to a plurality of conference participants' mobile devices for play, and the to-be-played signals are signals that are received by the Cisco room video endpoint and are to be played. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

View shared content on mobile devices

Intelligent Proximity for Content Sharing automatically pairs devices with Cisco room-based video endpoints when they come within range. You can save snapshots of shared content.

Id.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

235. Cisco Webex from Verizon sends a second type signal in the to-be-played signals to the primary playing device of the site for play. For example, Cisco Webex from Verizon sends a video signal in to-be-played signals to the Cisco room video endpoint's device with picture, sound, and video playing capabilities for play. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

View shared content on mobile devices

Intelligent Proximity for Content Sharing automatically pairs devices with Cisco room-based video endpoints when they come within range. You can save snapshots of shared content.

Id.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

236. Cisco Webex from Verizon sends a first type signal and second type signal, wherein the first type signal is a presentation stream signal when the second type signal is a main stream signal, or the first type signal is the main stream signal when the second type signal is the presentation stream signal. For example, Cisco Webex from Verizon sends a video signal to the primary playing device of the Cisco room video endpoint and a slideshow signal to each of the mobile devices. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

237. Cisco Webex from Verizon sends a presentation stream signal and main stream signal, wherein the presentation stream signal comprises at least one of a document and a demonstration slide to be displayed and the main stream signal comprises real-time content to be displayed. For example, Cisco Webex from Verizon sends a video signal that comprises real-time content to be displayed and a slideshow signal that comprises a demonstration slide to be displayed. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

238. With respect to claim 5, Cisco Webex from Verizon plays a conference signal implemented by a mobile device. For example, Cisco Webex from Verizon plays a conference signal implemented by a mobile device. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html ("Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.").

View shared content on mobile devices

Intelligent Proximity for Content Sharing automatically pairs devices with Cisco room-based video endpoints when they come within range. You can save snapshots of shared content.

Id.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation.

xConfiguration Proximity Services ContentShare ToClients: <Enabled/Disabled>

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

239. Further with respect to claim 5, Cisco Webex from Verizon establishes a connection channel between the mobile device held by a conference participant located at a site and a video conference terminal located at the site, wherein the video conference terminal comprises a primary playing device. For example, Cisco Webex from Verizon establishes a connection channel between the mobile devices held by conference participants and a Cisco room video endpoint, which includes a device with picture, sound, and video playing capabilities. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

Maximum simultaneous connections

The solution is using the web server part of the endpoint, this limits the maximum number of simultaneous connections and the number depends on the capabilities of the codec. The following is the maximum number of allowed clients. Exceeding this will display a notification in the application.

Video System model	Maximum simultaneous connections
Cisco TelePresence SX10 and SX10N Quick Set	7
Cisco TelePresence SX20 Quick Set	7
Cisco TelePresence SX80, MX700, MX800 and MX800D	10
Cisco TelePresence MX200 G2 and MX300 G2	7
Cisco DX70 and Cisco DX80	3
Cisco Webex Room Series	7 30*
Cisco Webex Board	7

** From CE9.4.0 if the Proximity service "ContentShare ToClients" is disabled.*

Id.

How Cisco Proximity Works

When the Intelligent Proximity services are enabled on a video endpoint, an inaudible ultrasonic sound token will be played through the video system loudspeakers. The Cisco Proximity client application running on the mobile device will record this token through its integrated microphone. The token contains information on how to connect to the video system over the network.

The mobile device will decode the token and try to establish a secure connection to the video system. To establish the connection, the mobile device needs to be able to reach the IPv4 address of the video system in the room on port 443 (HTTPS).

https://www.cisco.com/c/dam/m/zh_cn/projectworkplace/assets/pdf/proximity-networking.pdf.

240. Further with respect to claim 5, Cisco Webex from Verizon receives, through the established connection channel, a type of signal that is sent by the video conference terminal, wherein the type of signal is selected from to-be-played signals comprising at least two different types of signals. For example, Cisco Webex from Verizon receives, through the established connection channel, a slideshow signal sent by the video conference terminal, wherein the slideshow signal is selected from to-be-played signals comprising at least slideshow signal and a video signal. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

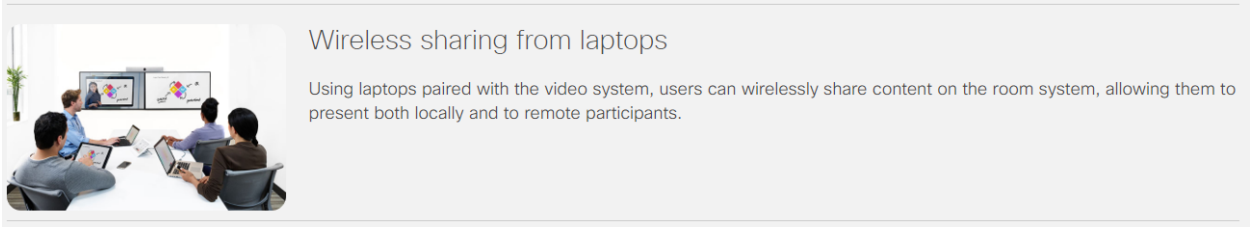
Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

241. Further with respect to claim 5, Cisco Webex from Verizon plays the type of signal selected from the to-be-played signals comprising the at least two different types of signals, wherein another type of signal selected from the to-be-played signals comprising the at least two different types of signals is played at the primary playing device. For example, Cisco Webex from Verizon plays the slideshow signal selected from the to-be-played signals wherein the video signal is played at the primary playing device. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.



Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

242. Further with respect to claim 5, Cisco Webex from Verizon plays the type of signal selected wherein the type of signal is a presentation stream signal or a main stream signal, wherein the presentation stream signal comprises at least one of a document and a demonstration slide to be displayed and the main stream signal comprises real-time content to be displayed. For example, Cisco Webex from Verizon plays a video signal on the primary playing device of the Cisco room video endpoint and a slideshow signal on each of the mobile devices. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

243. With respect to claim 8, Cisco room video endpoints are a video conference terminal. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

244. Further with respect to claim 8, Cisco room video endpoints have a processor configured to establish a connection channel between a plurality of mobile devices held by a plurality of conference participants located at a site and the video conference terminal located at the site. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

Maximum simultaneous connections

The solution is using the web server part of the endpoint, this limits the maximum number of simultaneous connections and the number depends on the capabilities of the codec. The following is the maximum number of allowed clients. Exceeding this will display a notification in the application.

Video System model	Maximum simultaneous connections
Cisco TelePresence SX10 and SX10N Quick Set	7
Cisco TelePresence SX20 Quick Set	7
Cisco TelePresence SX80, MX700, MX800 and MX800D	10
Cisco TelePresence MX200 G2 and MX300 G2	7
Cisco DX70 and Cisco DX80	3
Cisco Webex Room Series	7 30*
Cisco Webex Board	7

** From CE9.4.0 if the Proximity service "ContentShare ToClients" is disabled.*

Id.

How Cisco Proximity Works

When the Intelligent Proximity services are enabled on a video endpoint, an inaudible ultrasonic sound token will be played through the video system loudspeakers. The Cisco Proximity client application running on the mobile device will record this token through its integrated microphone. The token contains information on how to connect to the video system over the network.

The mobile device will decode the token and try to establish a secure connection to the video system. To establish the connection, the mobile device needs to be able to reach the IPv4 address of the video system in the room on port 443 (HTTPS).

https://www.cisco.com/c/dam/m/zh_cn/projectworkplace/assets/pdf/proximity-networking.pdf.

245. Further with respect to claim 8, Cisco room video endpoints have a signal distributor configured to send, through the connection channel established by the processor, a first type signal in to-be-played signals to each of the mobile devices for play, wherein the to-be-played signals are signals that are received by the video conference terminal and are to be played. For example, Cisco room video endpoints have a signal distributor configured to send, through the connection channel established by the processor, a slideshow signal in to-be-played signals to a plurality of conference participants' mobile devices for play, and the to-be-played signals are signals that are received by the Cisco room video endpoint and are to be played. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

246. Further with respect to claim 8, Cisco room video endpoints have a signal distributor further configured to send a second type signal in the to-be-played signals to a primary playing device of the site for play. For example, Cisco room video endpoints have a signal distributor further configured to send a video signal in to-be-played signals to the Cisco room video endpoint's device with picture, sound, and video playing capabilities for play. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

247. Further with respect to claim 8, in the Cisco room video endpoints, the first type signal is a presentation stream signal when the second type signal is a main stream signal, or the first type signal is the main stream signal when the second type signal is the presentation stream signal. For example, the Cisco room video endpoints send a video signal to the primary playing device of the Cisco room video endpoint and a slideshow signal to each of the mobile devices.

See, e.g., https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

248. Further with respect to claim 8, in the Cisco room video endpoints, the presentation stream signal comprises at least one of a document and a demonstration slide to be displayed, and the main stream signal comprises real-time content to be displayed. For example, Cisco room video endpoints send a video signal that comprises real-time content to be displayed and a slideshow signal that comprises a demonstration slide to be displayed. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

249. With respect to claim 12, mobile devices with Cisco Webex from Verizon include a processor configured to establish a connection channel between the mobile device located at a site and a video conference terminal located at the site, wherein the video conference terminal comprises a primary playing device. For example, mobile devices with Cisco Webex from Verizon include a processor configured to establish a connection channel between the mobile devices held by conference participants and a Cisco room video endpoint, which includes a device with picture, sound, and video playing capabilities. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

Maximum simultaneous connections

The solution is using the web server part of the endpoint, this limits the maximum number of simultaneous connections and the number depends on the capabilities of the codec. The following is the maximum number of allowed clients. Exceeding this will display a notification in the application.

Video System model	Maximum simultaneous connections
Cisco TelePresence SX10 and SX10N Quick Set	7
Cisco TelePresence SX20 Quick Set	7
Cisco TelePresence SX80, MX700, MX800 and MX800D	10
Cisco TelePresence MX200 G2 and MX300 G2	7
Cisco DX70 and Cisco DX80	3
Cisco Webex Room Series	7 30*
Cisco Webex Board	7

** From CE9.4.0 if the Proximity service "ContentShare ToClients" is disabled.*

Id.

How Cisco Proximity Works

When the Intelligent Proximity services are enabled on a video endpoint, an inaudible ultrasonic sound token will be played through the video system loudspeakers. The Cisco Proximity client application running on the mobile device will record this token through its integrated microphone. The token contains information on how to connect to the video system over the network.

The mobile device will decode the token and try to establish a secure connection to the video system. To establish the connection, the mobile device needs to be able to reach the IPv4 address of the video system in the room on port 443 (HTTPS).

https://www.cisco.com/c/dam/m/zh_cn/projectworkplace/assets/pdf/proximity-networking.pdf.

250. Further with respect to claim 12, mobile devices with Cisco Webex from Verizon include a signal receiver configured to receive, through the connection channel established by the processor, a type of signal that is sent by the video conference terminal, wherein the type of signal is selected from to-be-played signals comprising at least two different types of signals. For example, mobile devices with Cisco Webex from Verizon include a signal receiver configured to receive, through the established connection channel, a slideshow signal sent by the video conference terminal, wherein the slideshow signal is selected from to-be-played signals comprising at least slideshow signal and a video signal. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

251. Further with respect to claim 12, mobile devices with Cisco Webex from Verizon include a player configured to play the type of signal selected from the to-be-played signals comprising the at least two different types of signals. For example, mobile devices with Cisco Webex from Verizon include a player configured to play the slideshow signal selected from the to-be-played signals comprising at least the slideshow signal and the video signal. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing towards client

This service will enable the content sharing from the endpoint to a mobile device. While the system is in a call and a participant is sharing a presentation, the mobile device that is paired to the system will receive snapshots of the on-going presentation for review. The user has the option to save the slides to their mobile device storage for later review as well. If arriving late to a meeting the codec will save the last 10 snapshots, which will be available for anyone who is pairing their mobile device late so they can look at the previous slides without interfering the on-going presentation. When this service is disabled, the Webex Room Series can pair up to 30 clients at the same time. If enabled the limit will be 7 (**from CE9.4.0**).

Id.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

252. Further with respect to claim 12, in mobile devices with Cisco Webex from Verizon, another type of signal selected from the to-be-played signals comprises the at least two different types of signals is played at the primary playing device. For example, in mobile devices with Cisco Webex from Verizon, another type of signal selected from the to-be-played signals is played at the Cisco room video endpoint's device with picture, sound, and video playing capabilities for play. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

Wireless sharing from laptops

Using laptops paired with the video system, users can wirelessly share content on the room system, allowing them to present both locally and to remote participants.

Id.

Cisco room video endpoints supported

Intelligent Proximity for Content Sharing is supported on Cisco MX, SX and IX Series, and Cisco Spark Room Series.

Id.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

253. Further with respect to claim 12, in mobile devices with Cisco Webex from Verizon, the type of signal is a presentation stream signal or a main stream signal, wherein the presentation stream signal comprises at least one of a document and a demonstration slide to be displayed, and the main stream signal comprises real-time content to be displayed. For example, in mobile devices with Cisco Webex from Verizon, a video signal plays on the primary playing device of the Cisco room video endpoint and a slideshow signal plays on each of the mobile devices. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

254. With respect to claim 15, Cisco Webex from Verizon sends a first type signal and second type signal, wherein the first type signal is the presentation stream signal and the second type signal is the main stream signal. For example, Cisco Webex from Verizon sends a video signal to the primary playing device of the Cisco room video endpoint and a slideshow signal to each of the mobile devices. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

255. With respect to claim 16, Cisco Webex from Verizon sends a presentation stream signal and main stream signal, wherein the presentation stream signal comprises a plurality of first subtype signals, wherein the first subtype signals comprise at least one of the document and the demonstration slide that is shared by another site, wherein the main stream signal comprises a plurality of second subtype signals, and wherein the second subtype signals comprise at least one of an image signal collected in real-time or a speech signal collected in real-time. For example, Cisco Webex from Verizon sends a video and speech signal collected in real-time to the primary playing device of the Cisco room video endpoint and a slideshow signal that is shared by another site to each of the mobile devices. *See, e.g.*,

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

256. With respect to claim 17, Cisco Webex from Verizon establishes a connection channel between the mobile device held by a conference participant located at a site and a video conference terminal located at the site, wherein the connection between the mobile device and

the video conference terminal is a direct connection. For example, Cisco Webex from Verizon establishes a direct connection between the mobile device and the Cisco room video endpoint, where no routing mobile device (or relay mobile device) exists between the mobile device and the Cisco room video endpoint. *See, e.g.*, https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html.

https://community.cisco.com/t5/mobile-applications-documents/troubleshooting-guide-cisco-proximity/ta-p/3148841.

Content sharing from client (PC / MAC content sharing)

If a user has the Cisco Proximity application installed on their laptop running Windows or MAC, they can pair their laptop with the endpoint using the same ultrasound technology. The internal Microphone of the laptop will pick up the audio and pair to the system. The user now has the option to share their screen wirelessly on the endpoint. If the system is in a call, and a screen is shared, the presentation will be distributed to all the participants in the call automatically. Please note that the images from the laptop are snapshots sent at a low frame rate of 3-5 frames per second. For presenting content in motion it is recommended to use a presentation cable. For PowerPoint presentation where still images are presented, content share via Proximity gives a good experience.

Id.

Maximum simultaneous connections

The solution is using the web server part of the endpoint, this limits the maximum number of simultaneous connections and the number depends on the capabilities of the codec. The following is the maximum number of allowed clients. Exceeding this will display a notification in the application.

Video System model	Maximum simultaneous connections
Cisco TelePresence SX10 and SX10N Quick Set	7
Cisco TelePresence SX20 Quick Set	7
Cisco TelePresence SX80, MX700, MX800 and MX800D	10
Cisco TelePresence MX200 G2 and MX300 G2	7
Cisco DX70 and Cisco DX80	3
Cisco Webex Room Series	7 30*
Cisco Webex Board	7

** From CE9.4.0 if the Proximity service "ContentShare ToClients" is disabled.*

Id.

How Cisco Proximity Works

When the Intelligent Proximity services are enabled on a video endpoint, an inaudible ultrasonic sound token will be played through the video system loudspeakers. The Cisco Proximity client application running on the mobile device will record this token through its integrated microphone. The token contains information on how to connect to the video system over the network.

The mobile device will decode the token and try to establish a secure connection to the video system. To establish the connection, the mobile device needs to be able to reach the IPv4 address of the video system in the room on port 443 (HTTPS).

https://www.cisco.com/c/dam/m/zh_cn/projectworkplace/assets/pdf/proximity-networking.pdf.

257. With respect to claim 19, Cisco room video endpoints have a processor further configured to determine a master mobile device according to capability information of a plurality of mobile devices held by a plurality of conference participants at the site and control a switching of signals played by the primary playing device and the mobile devices according to a selection received from the master mobile device. *See, e.g.*, https://help.webex.com/en-us/WBX86712/How-Do-I-Use-the-Anyone-Can-Share-Feature-in-Webex-Meetings.

Attendees

It is recommended that you ask permission from the host or current presenter before you share content. Sharing while another participant is presenting will cause their share in progress to end. Their shared screen, application, or presentation will be replaced by your shared content. Your shared material will be viewed by all participants.

Solution:

Any participant can share content in the meeting by simply selecting 'Share' on the Quick Start, Menu Bar and Floating Icon Tray. This feature makes it easier to change presenters in a meeting and improves the overall collaboration experience. If hosts want more control over sharing, they can disable this feature while the meeting is in progress. This option can also be disabled for the site in Cisco Webex Meetings Site Administration as it is enabled by default.

Id.

258. With respect to claim 20, mobile devices with Cisco Webex from Verizon include a processor further configured to send a switching play request message to switch a signal played by a primary playing device and the mobile device. *See*, *e.g.*, https://help.webex.com/en-us/WBX86712/How-Do-I-Use-the-Anyone-Can-Share-Feature-in-Webex-Meetings.

Attendees

It is recommended that you ask permission from the host or current presenter before you share content. Sharing while another participant is presenting will cause their share in progress to end. Their shared screen, application, or presentation will be replaced by your shared content. Your shared material will be viewed by all participants.

Solution:

Any participant can share content in the meeting by simply selecting 'Share' on the Quick Start, Menu Bar and Floating Icon Tray. This feature makes it easier to change presenters in a meeting and improves the overall collaboration experience. If hosts want more control over sharing, they can disable this feature while the meeting is in progress. This option can also be disabled for the site in Cisco Webex Meetings Site Administration as it is enabled by default.

Id.

259. As such, on information and belief, Verizon has directly infringed at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the ’366 Patent by at least, for example, (i) performing testing of Cisco Webex from Verizon; (ii) making, using, offering for sale, selling, and/or importing into the United States its mobile devices; and (iii) making, using, offering for sale, selling, and/or importing into the United States Cisco room video endpoints.

260. On information and belief, Verizon has infringed at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent by inducing others, including users of Cisco Webex from Verizon that it sells and/or offers, to infringe at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent in violation of 35 U.S.C. § 271(b).

261. On information and belief, Verizon takes active steps to induce infringement of at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent by others, including its customers, and Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. Such active steps include, but are not limited to, encouraging, advertising (including by internet websites, television, store displays, print advertisements, *etc.*), promoting, and instructing others to use and/or how to play a conference signal. Such conference signals are played on devices including those made, sold, offered for sale, and/or imported by Verizon, such as the various Cisco room video endpoints and various mobile devices. For example, Verizon induces users of Cisco Webex by Verizon to use one or more claimed inventions of the '366 Patent by instructing users how to play a conference signal on a video conference terminal, such as a Cisco room video endpoint, or on a mobile device. *See, e.g.*, https://enterprise.verizon.com/products/business-communications/unified-communications-and-collaboration/cisco-webex/.

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent, including for example, by prompting them to use Cisco Webex by Verizon to play a conference signal.

262. On information and belief, Verizon contributes to the infringement of at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or import by Verizon of Cisco Webex by Verizon, Cisco room video endpoints, and/or mobile devices. Such Cisco Webex by Verizon, Cisco room video endpoints, and/or mobile devices are especially adapted for use to infringe at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the '366 Patent and are at least a material part of those claims, for example, as described above with respect to claim 1. Cisco Webex by Verizon, Cisco room video endpoints, and/or mobile devices are not suitable for substantial noninfringing use.

263. By way of at least Huawei's notice to Verizon on March 29, 2019 (as well as this Complaint), Verizon knows of the '366 Patent and performs acts that it knows, or should know,

induce, and/or contribute to the direct infringement of at least claims 1, 5, 8, 12, 15-17, 19, and 20 of the ’366 Patent by third parties.

264. Verizon undertook and continues its infringing actions despite a high likelihood that such activities infringed the ’366 Patent, which is presumed valid. For example, Verizon has been aware of a high likelihood that its actions constituted, and continue to constitute, infringement of the ’366 Patent and that the ’366 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the ’366 Patent, nor could it reasonably subjectively believe that the patent is invalid. Despite that knowledge, subjective belief, and the objectively high likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the ’366 Patent.

265. Huawei has been irreparably harmed by Verizon’s infringement of the ’366 Patent and will continue to be harmed unless and until Verizon’s infringement is enjoined by this Court.

266. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the ’366 Patent pursuant to 35 U.S.C. § 271.

COUNT VI: INFRINGEMENT OF U.S. PATENT NO. 7,715,832

267. Huawei realleges and incorporates by reference paragraphs 1-266 above, as if fully set forth herein.

268. The U.S. Patent Office duly and properly issued the ’832 Patent, entitled “Mobile Terminal and a Method for Implementing the Guardianship Function,” on May 11, 2010. Huawei Technologies is the assignee of all right, title, and interest in and to the ’832 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the ’832 Patent is valid and enforceable. A true and correct copy of the ’832 Patent is attached hereto as Exhibit F.

269. The ’832 Patent provides novel, useful and more effective and efficient techniques for implementing a guardianship function at a mobile terminal that overcome the problems of the prior art and thereby improve the functioning of computer and network equipment.

270. The ’832 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problem of implementing a guardianship function at a mobile terminal. Here, guardians (such as parents) frequently equipped their wards (such as children) with a mobile terminal, such as a cell phone, but when the parent needed to determine the child’s status, the parent had no choice but to contact the child on the parent’s own initiative. *Id.* at 1:22-28. This made it difficult for the parent to monitor the child’s use of the mobile terminal. *Id.* at 1:28-30. Previous attempts to solve this problem included various disadvantages.

271. The inventions of the ’832 Patent provide technical solutions to the problems in the prior art described above. The ’832 Patent describes, for example, collecting data by the processing hardware related to use of the mobile terminal, analyzing the data by the processing hardware and determining the use of the mobile terminal according the analyzing, and sending a short message from the mobile terminal used for notifying the determined use of the mobile terminal. *See, e.g.*, the ’832 Patent at 9:62-11:58. The ’832 Patent further describes receiving at the mobile terminal a remote control message for indicating that a running of at least one program at the mobile terminal should be stopped, and stopping the running of the at least one program according to the remote control message. *See, e.g., id.* at 13:4-28.

272. The inventions of the ’832 Patent improve computer functionality by improving and solving problems in a computer’s capability of implementing a guardianship function at a

mobile terminal more thoroughly and with better efficiency. The inventions of the '832 Patent provide a computer-based solution to a computer-specific problem. The inventions of the '832 Patent are improvements over the prior art and other techniques for implementing a guardianship function at a mobile terminal, and the '832 Patent enables a combination of features not present in the prior art and other techniques.

273. For example, the inventions of the '832 Patent provide for improved computer operation by implementing a guardianship function at a mobile terminal, which allows the parent to monitor – and control – the child's phone use.

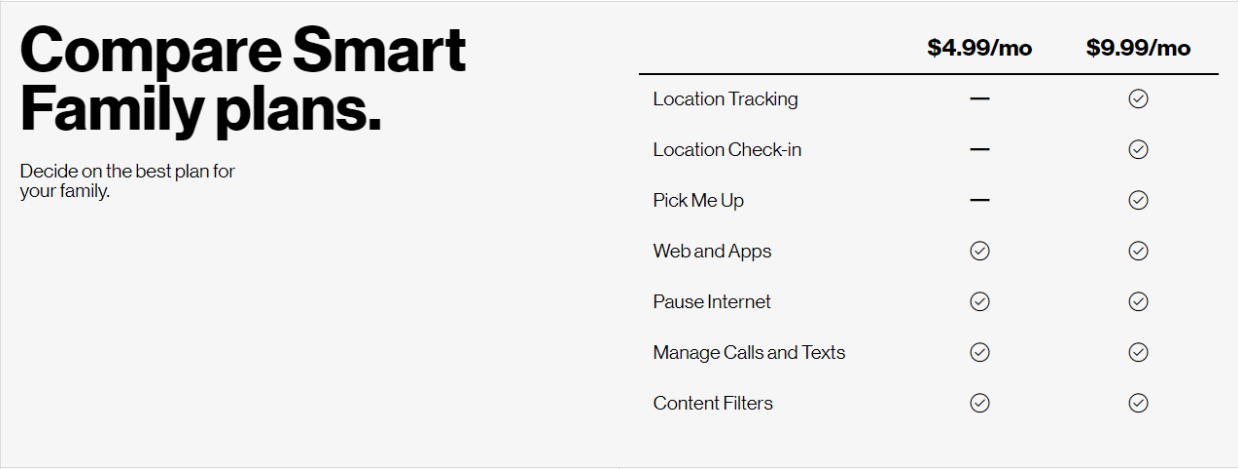
274. By way of further example, the inventions of the '832 Patent provide for improved computer operation by allowing configuration commands to be sent to the child's mobile terminal to establish parental control requirements, implementing a guardianship function at a mobile terminal that collects data from the child's mobile terminal, analyzes the data to determine the mobile terminal's use, and sends a short message to inform the guardian of the use, and implementing a remote control message for indicating that a running of at least one program at the mobile terminal should be stopped, and stopping the running of the at least one program according to the remote control message.

275. As such, the '832 inventions thereby allow users to implement a guardianship function at a mobile terminal more thoroughly and with better efficiency, which represents a concrete improvement over prior art techniques.

276. The claims of the '832 Patent contain an inventive concept improve the functioning of computers and other networked devices. Claims 7-9 claim ordered combinations of activities of a computer or networked device that were new, novel, innovative, and unconventional at the time the '832 Patent application was filed. These ordered combinations

are set forth in claims 7-9 of the '832 Patent. The ordered combinations of elements in claims 7-9 were not well understood, routine or conventional at the time the '832 Patent application was filed. The ordered combinations of the inventions of claims 7-9 are practical, particular, non-conventional, and non-generic techniques of implementing a guardianship function at a mobile terminal.

277. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe through Verizon's Smart Family Service (formerly known as FamilyBase):



https://www.verizonwireless.com/solutions-and-services/verizon-smart-family/. *See also* https://wbillpay.verizonwireless.com/vzw/nos/safeguards/safeguardLandingPage.action.

278. For example, Verizon infringes at least claims 7-9 of the '832 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the '832 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Verizon's Smart Family Service (formerly known as FamilyBase) and/or the components thereof, which allows for implementing a guardianship function at a mobile terminal. And users of the Verizon Smart Family Service directly infringe at least claims 7-9 of the '832 Patent by,

for example, using the capabilities of the Verizon Smart Family Service to implement a guardianship function at a mobile terminal. *See* https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("Verizon Smart Family is a service that offers location services and parental controls for all of your family members' phones.").

279. With respect to at least claims 7-9, the Verizon Smart Family Service is operable to implement a guardianship function at a mobile terminal having processing hardware and memory. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("Verizon Smart Family is a service that offers location services and parental controls for all of your family members' phones."); *id.* ("Make sure the Smart Family Companion app is downloaded on your child's phone.).

280. The Verizon Smart Family Service is operable to collect data by the processing hardware related to use of the mobile terminal. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("Tap Agree to provide parental consent for the Smart Family app to collect information from your child's phone in order to provide the Smart Family service to you and your family."); *id.* ("You'll be taken to the child's system settings. Follow the instructions to set up the child's VPN profile to collect web and app activity, enable content filters and enforce time restrictions.").

281. The Verizon Smart Family Service is operable to analyze the data by the processing hardware and determining the use of the mobile terminal according the analyzing. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("You'll see a list of contacts your child has been communicating with."); *id.* ("You'll see a detailed view of your child's call and text activity for that day."); *id.* ("You'll see a detailed view of the day's activities, including specific websites and apps visited in each category.").

282. The Verizon Smart Family Service is operable to send a short message from the mobile terminal used for notifying the determined use of the mobile terminal. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("You'll see a list of contacts your child has been communicating with."); *id.* ("You'll see a detailed view of your child's call and text activity for that day."); *id.* ("You'll see a detailed view of the day's activities, including specific websites and apps visited in each category.").

283. The Verizon Smart Family Service is operable to receive at the mobile terminal a remote control message for indicating that a running of at least one program at the mobile terminal should be stopped. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("Set up content filters: You must be paired with your child's Smart Family Companion app to use content filters."); *id.* ("View child's web and app activity: You must be paired with your child's Smart Family Companion app to use this feature.").

284. The Verizon Smart Family Service is operable to stop the running of the at least one program according to the remote control message. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("Set up content filters: You must be paired with your child's Smart Family Companion app to use content filters."); *id.* ("Tap the switch for each filter you want to turn on or off."); *id.* ("Follow the instructions to set up the child's VPN profile to collect web and app activity, enable content filters and enforce time restrictions."); *id.* ("Pause child's internet: You must be paired with your child's Smart Family Companion app to pause internet."); *id.* ("1. Select the child at the top of the screen. 2. Tap Pause internet. 3. Tap OK."); *id.* ("View child's web and app activity: You must be paired with your child's Smart Family Companion app to use this feature."). *See also* https://www.verizonwireless.com/support/verizon-smart-family-faqs/ ("How can I block a

website or app? … You can set up content filters to block all websites and apps in a variety of content categories.").

285. With respect to claim 8, the Verizon Smart Family Service is operable to identify whether the short message received contains a predefined password, and when the short message received contains a predefined password, determine the short message received is the remote control message.

286. With respect to claim 9, the Verizon Smart Family Service is operable to perform the method of claim 7, wherein, the use of the mobile terminal comprises any one or any combination of the followings: playing games, opening a data service application and making a call. *See, e.g.*, https://www.verizonwireless.com/support/how-to-use-verizon-smart-family/ ("You'll see a list of contacts your child has been communicating with."); *id.* ("You'll see a detailed view of your child's call and text activity for that day."); *id.* ("You'll see a detailed view of the day's activities, including specific websites and apps visited in each category."). *See also* https://www.verizonwireless.com/support/verizon-smart-family-faqs/ ("How can I block a website or app? … You can set up content filters to block all websites and apps in a variety of content categories.").

287. As such, on information and belief, Verizon has directly infringed at least claims 7-9 of the '832 Patent by at least, for example, performing testing of the Verizon Smart Family Service in the United States, in violation of 35 U.S.C. § 271(a).

288. On information and belief, Verizon has infringed at least claims 7-9 of the '832 Patent by inducing others, including users of the Verizon Smart Family Service that it sells and/or offers, to infringe at least claims 7-9 of the '832 Patent in violation of 35 U.S.C. § 271(b).

289. On information and belief, Verizon takes active steps to induce infringement of at least claims 7-9 of the ’832 Patent by others, including its customers, and Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. Such active steps include, but are not limited to, encouraging, advertising (including by internet websites, television, store displays, print advertisements, *etc.*), promoting, and instructing others to use and/or how to implement a guardianship function at a mobile terminal in the United States. For example, Verizon induces users of the Verizon Smart Family Service to use one or more claimed inventions of the ’832 Patent by instructing users how to implement a guardianship function at a mobile terminal, such as via the web pages above. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 7-9 of the ’832 Patent.

290. On information and belief, Verizon contributes to the infringement of at least claims 7-9 of the ’832 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or importation by Verizon of mobile terminals, such as cell phones and tablets, that operate Verizon Smart Family Services. Such mobile terminals are especially made for or adapted for use to infringe at least claims 7-9 of the ’832 Patent and are at least a material part of those claims, for example, as described above with respect to claim 7. The Verizon Smart Family Services, including the functionality contributing to infringement of the ’832 Patent, are not suitable for substantial noninfringing use.

291. By way of at least Huawei’s notice to Verizon on March 29, 2019 (and this Complaint), Verizon knows of the ’832 Patent and performs acts that it knows, or should know,

induce and/or contribute to the direct infringement of at least claims 7-9 of the ’832 Patent by third parties.

292. Verizon undertook and continues its infringing actions despite an objectively high likelihood that such activities infringed the ’832 Patent, which is presumed valid. For example, Verizon has been aware of an objectively high likelihood that its actions constituted, and continue to constitute, infringement of the ’832 Patent and that the ’832 Patent is valid since at least March 29, 2019. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the ’832 Patent, nor could it reasonably subjectively believe that the ’832 Patent is invalid. Despite that knowledge, subjective belief, and the objectively high likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the ’832 Patent.

293. Huawei has been irreparably harmed by Verizon’s infringement of the ’832 Patent and will continue to be harmed unless and until Verizon’s infringement is enjoined by this Court.

294. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the ’832 Patent pursuant to 35 U.S.C. § 271.

COUNT VII: INFRINGEMENT OF U.S. PATENT NO. 8,761,839

295. Huawei realleges and incorporates by reference paragraphs 1-294 above, as if fully set forth herein.

296. The U.S. Patent Office duly and properly issued the ’839 Patent, entitled “Method and Mobile Terminal for Processing Contacts,” on June 24, 2014. Huawei Device is the assignee of all right, title, and interest in and to the ’839 Patent and possesses the exclusive right of recovery for past, present, and future infringement. Each and every claim of the ’839 Patent is valid and enforceable. A true and correct copy of the ’839 Patent is attached hereto as Exhibit G.

297. The ’839 Patent provides novel, useful and more effective and efficient techniques for processing contacts in a mobile terminal, which enhance the capability of intelligent interaction between the mobile terminal and the user, overcoming the problems of the prior art and thereby improving the functioning of computer equipment. *See* the ’839 Patent at Abstract.

298. The ’839 Patent is generally directed to a novel and inventive technical solution to a problem relating to computer technology, and in particular to the problem of processing contacts of a mobile terminal. *See id.* at 1:23-34. “A contact application is a program storing specific contact information (such as names, portraits, or mobile phone numbers) of contacts according to a present format.” *Id*. at 1:29-32. “A contact application interface is an interface that is displayed on the touch screen of a mobile phone after the contact application receives a command entered by a user.” *Id*. at 1:32-35. At the time of the ’839 Patent, on prior art contact application interfaces, “contacts are displayed in name mode, and are arranged in rows simply according to the initial letters or the stroke numbers of names.” *Id*. at 1:37-40. Also, in the prior art, “contacts are displayed in portrait and name mode, and are arranged simply to form a 9-block vision, a 12-block vision, and so on.” *Id*. at 1:40-42. The ’839 Patent explains that “the modes for processing contacts by the mobile terminal in the prior art cannot reflect different contacts in an intuit manner, which reduces the capability of intelligent interaction between the mobile terminal and the user.” *Id*. at 1:42-46.

299. The inventions of the ’839 Patent provide technical solutions to the problems in the prior art described above. The ’839 Patent describes, for example, that in accordance with the techniques of the ’839 Patent, the “mobile terminal sets a mapping relationship between an attribute value of an attribute of a contact and a display effect of a contact bubble corresponding

to the contact." *See, e.g.*, the '839 Patent at 1:52-55. The '839 Patent further describes that the "mobile terminal obtains the attribute value locally or from a network device and determines the display effect of the contact bubble according to the mapping relationship and the distinctive attribute value. The mobile terminal then displays the contact bubble on a screen of the mobile terminal according to the attribute value of the contact." *Id.* at 1:55-60; *see also* Fig. 3. As the patent explains: "The mapping relationship between different values of distinctive attributes of contacts and display effects of contact icons is specifically a mapping relationship between contacts with distinctive attributes of different values and display effects of icons." *Id.* at 3:58-62. Thus, according to these and other solutions taught in the '839 Patent, "different contacts can be displayed intuitively in a mobile terminal, which enhances the capability of intelligent interaction between the mobile terminal and a user." *Id.* at 2:7-12. The result is a "distinctive display," with enhanced contact bubbles that is "different from the display mode (contact list) of contacts in the prior art" that "displays contacts more intuitively on the touch screen, to enhance the capability of a man-machine interaction of the mobile terminal having a touch screen, and also improves the user experience." *See id.* at 4:2-10.

300. As further described in the '839 Patent, for example, a "location of a contact bubble may also be indicated by values in the X and Y directions. First, the size of a contact bubble may be calculated through junction points between bubble edges and grids, and then the contact bubble is simulated into a square. The size of the contact bubble is also the size of the square. According to calculation of the square size, location information (X1, Y1) of the center point of the contact bubble is obtained, and the location information (X1, Y1) of the center point is used as the location information of the contact bubble, where X1 is the value of the center

point in the X direction, and Y1 is the value of the center point in the Y direction." *Id.* at 11:19-30.

301. The '839 Patent also teaches, for example, "matching" a touch point of a user to location information of a certain contact bubble: "Specifically, the matching method may be: calculating a distance between location information (X1, Y1) of a contact bubble and location information (X2, Y2) of a touch point. If the calculated result is smaller than a preset value, it is regarded that the matching succeeds, and a contact selection command is triggered. If the matching does not succeed, it is regarded that the touch point is an invalid touch point, and no operation command is triggered or a prompt command is triggered, where the prompt command is used to prompt the user that the touch point is an invalid touch point." *Id.* at 11:50-60.

302. The '839 Patent further teaches that "when a user uses a finger to touch a contact on a screen, a mobile terminal may obtain an operation command of the user through a touch screen." *Id.* at 11:64-67. The "operation track of a user" is obtained, and the selected contact bubble can be moved according to the operation track. *Id.* at 12:9-14.

303. Specific methods are taught by the '839 Patent to determine whether the "contact bubble has an overlapping area with a preset call area," which may result in calling the contact. *Id.* 12:14-13:10.

304. The inventions of the '839 Patent improve computer functionality by improving and solving problems in a mobile terminal's capability of intelligent interaction with a user, providing a "distinctive display" for a contact application interface. The inventions of the '839 Patent provide a computer-based solution to a computer-specific problem. The inventions of the '839 Patent are improvements over the prior art and other techniques for the processing and

display of contacts, and the '839 Patent enables a combination of features not present in the prior art and other techniques.

305. For example, the inventions of the '839 Patent provide for improved computer operation by providing a solution that "is different from the display mode (contact list) of contacts in the prior art, and displays the contacts more intuitively on the touch screen, to enhance the capability of man-machine interaction of the mobile terminal having a touch screen, and also improves the user experience," including a "distinctive display" in which "contacts with distractive attributes of different values are displayed according to the mapping relationship by using different display effects." '839 Patent at 4:2-10.

306. By way of further example, the inventions of the '839 Patent provide for improved computer operation by providing a solution in which "the call processing of a contact can be completed by only moving fingers simply, which saves the time for a user to perform call operations, greatly improves the capability of intelligent interaction of a mobile terminal, and improves the user experience of the user." '839 Patent at 13:66-14:4.

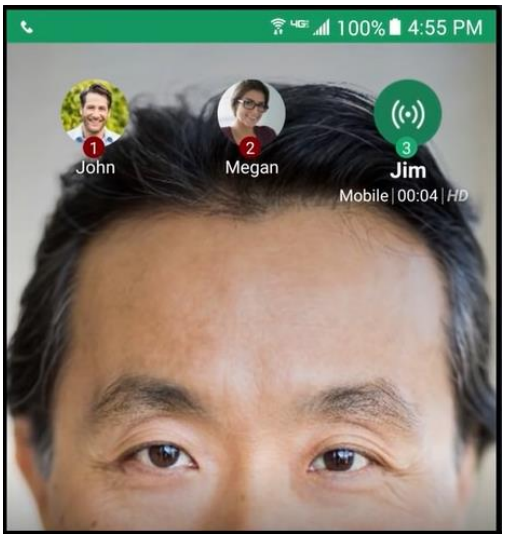
307. As such, the '839 inventions thereby provide a contact application interface with a distinctive display which allows the mobile terminal to intuitively interact with users, with an improved user experience, which represents a concrete improvement over prior art techniques.

308. The claims of the '839 Patent contain an inventive concept improve the functioning of computers devices. Claims 1, 3, 5, 10-11, and 15-17 claim ordered combinations of activities of a computer device that were new, novel, innovative, and unconventional at the time the '839 Patent application was filed. These ordered combinations are set forth in at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent. The ordered combinations of elements in claims 1, 3, 5, 10-11, and 15-17 were not well understood, routine or conventional at the time

the ’839 Patent application was filed. The ordered combinations of the inventions of claims 1, 3, 5, 10-11, and 15-17 are practical, particular, non-conventional, and non-generic techniques of processing contacts of a mobile terminal.

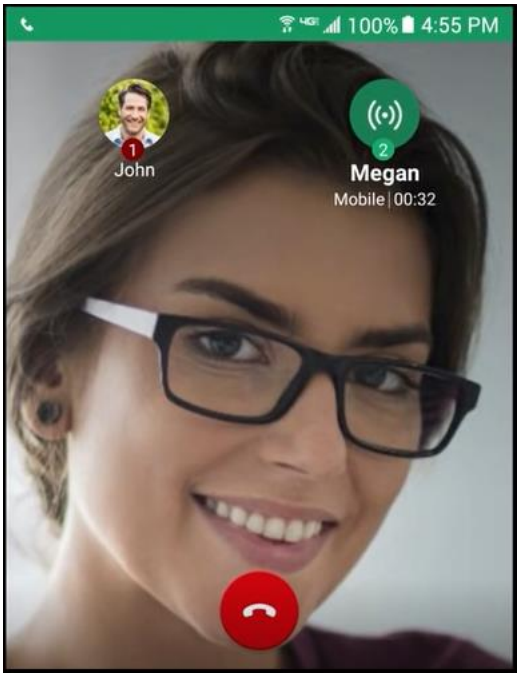
309. In violation of 35 U.S.C. § 271, Verizon has directly infringed, contributed to the infringement of, and/or induced others to infringe at least claims 1, 3, 5, 10-11, and 15-17 of the ’839 Patent by, among other things, making, using, offering for sale, selling, and/or importing into the United States unlicensed systems, products, and/or services that infringe such claims of the ’839 Patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, Verizon’s One Talk application, which allows for conference call management using enhanced contact bubbles. In addition, users of Verizon’s One Talk application infringe at least claims 1, 3, 5, 10-11, and 15-17 of the ’839 Patent by, for example, using the capabilities of Verizon’s One Talk application to provide for conference call management using enhanced contact bubbles on a mobile terminal. *See, e.g.*, “One Talk - Handling multiple mobile calls: Verizon Tutorial Video,” *available at* https://www.youtube.com/watch?v=pEoQm0blmCo (“Tutorial Video”).

310. With respect to at least claims 1, 3, 5, 10-11, and 15-17, Verizon’s One Talk application sets a mapping relationship between an attribute value of an attribute of a contact and a display effect of a contact bubble corresponding to the contact. *See, e.g.*, Tutorial Video at 0:29 (“All of your current calls are displayed as bubbles on the top of your screen”) (changing contact bubble for “Jim” to reflect currently active call):

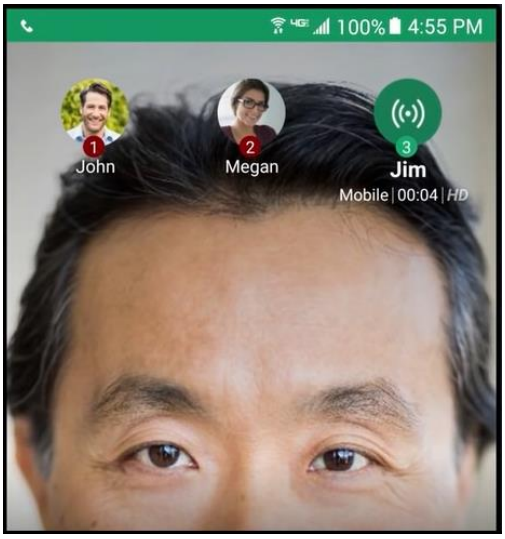


311. Verizon's One Talk application obtains the attribute value, e.g., a value indicating whether the call is active, locally or from a network device.

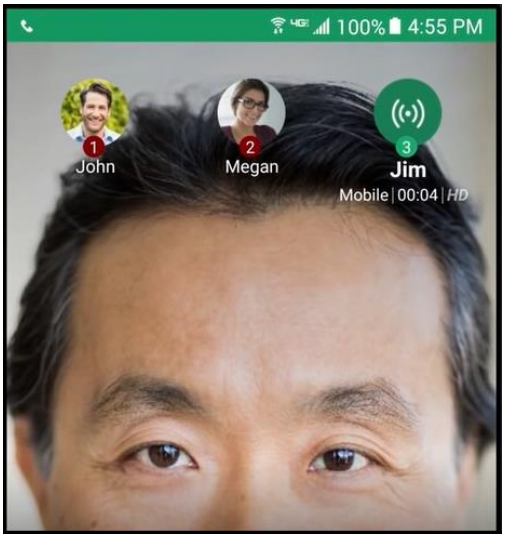
312. Verizon's One Talk application determines the display effect of the contact bubble according to the mapping relationship and the distinctive attribute value. *See, e.g.*, Tutorial Video (determining whether to display a contact's photo or a fixed icon according to whether that contact is currently active or on hold):



313. Verizon's One Talk application displays the contact bubble on a screen of the mobile terminal according to the attribute value of the contact. *See, e.g.*, Tutorial Video (displaying the contact bubbles according to their active or on-hold status):



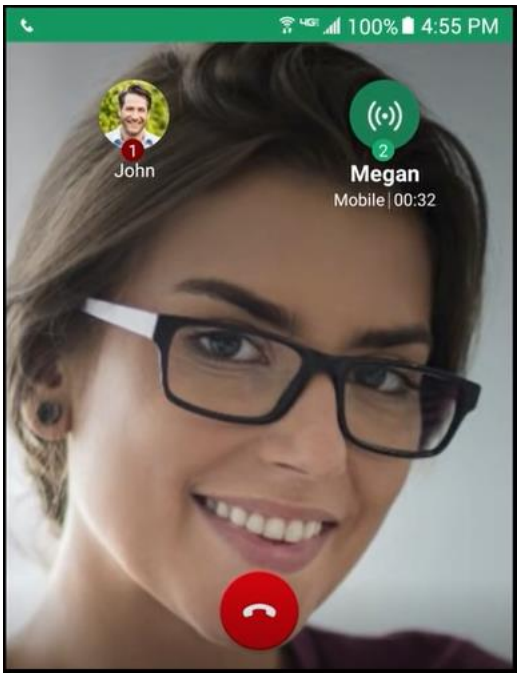
314. With respect to claim 3, the attribute in Verizon's One Talk application comprises a contact attribute that indicates time of communication between the mobile terminal and the contact within a preset time. *See, e.g.*, Tutorial Video at 0:29 (showing call time for "Jim"):

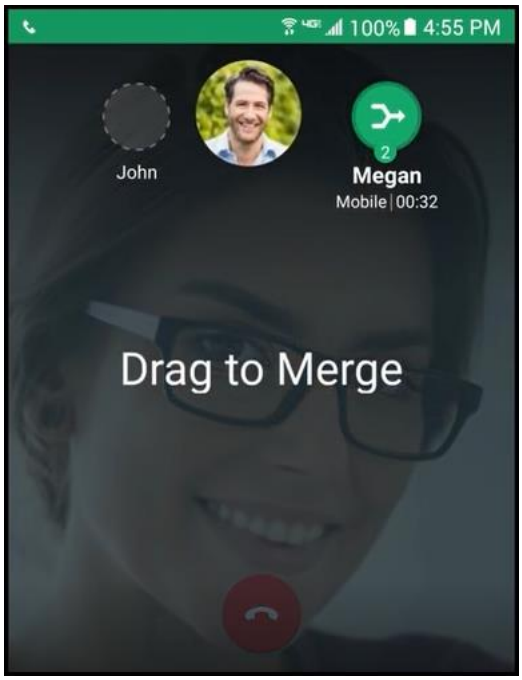


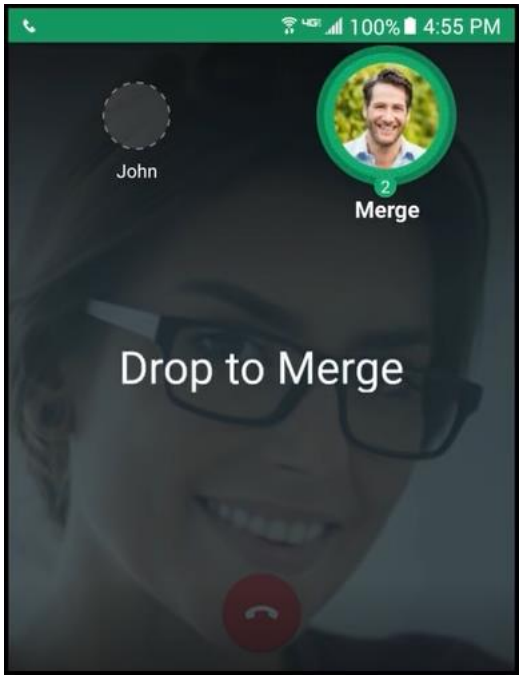
315. With respect to claim 5, the attribute in Verizon's One Talk application comprises a group attribute and a contact attribute, a value of the mapping relationship is a sum of values of

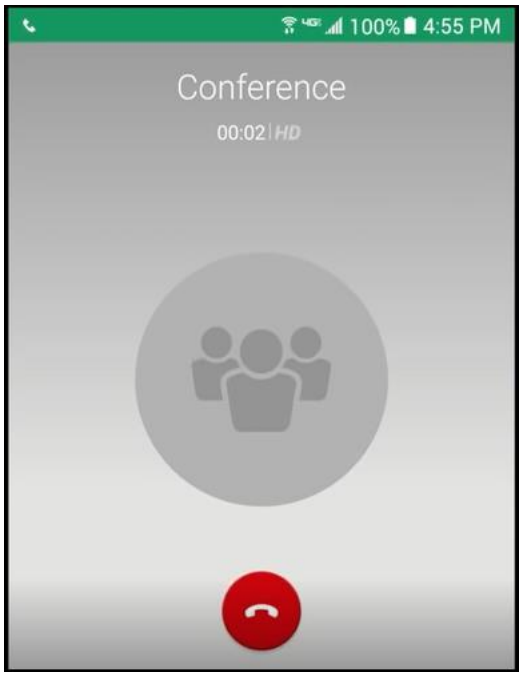
the group attribute and the contact attribute of the contact. See, e.g., "One Talk - Using 6-way Conference Calling: Verizon Tutorial Video," *available at* https://www.youtube.com/watch?v=KZsxX4lfD84 at 0:31: (displaying either a contact's photo or a fixed icon according to whether that contact is part of the "Conference" group and also reflecting whether the contact is currently active):

316. With respect to claim 10, Verizon's One Talk application obtains a contact selection command of a user of the mobile terminal, and determines at least one contact bubble; obtains an operation track of the user; moves the at least one contact bubble according to the operation track; determines that the at least one contact bubble overlaps a preset call area; and calls the contact represented by the at least one contact bubbles after the determination. *See, e.g.*, Tutorial Video at 0:39 ("To merge calls for a group conversation, just drag a call on hold over your currently active call"):


100% 4:55 PM
John
Megan
Mobile | 00:32

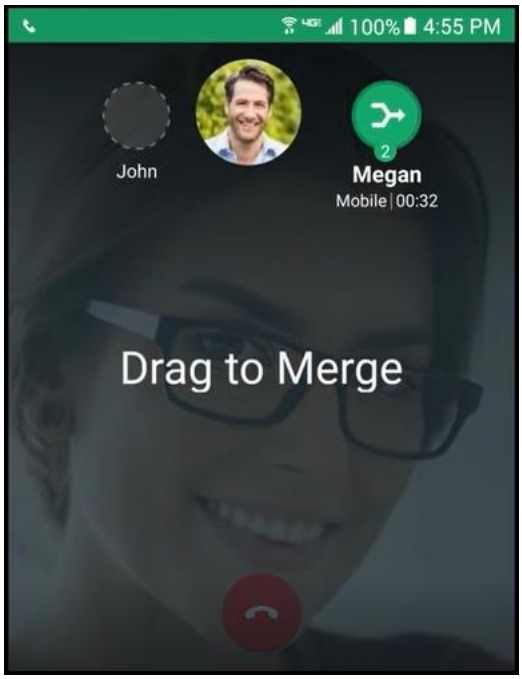

100% 4:55 PM
John
Megan
Mobile | 00:32
Drag to Merge

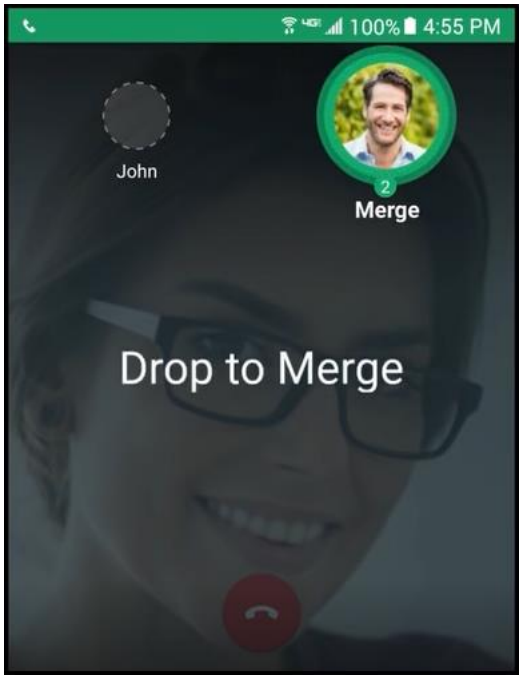




317. With respect to claim 11, Verizon's One Talk application determines that the at least one contact bubble overlaps the preset call area when location information of an edge point of the at least one contact bubble is location information of a point within the preset call area; and determines that the at least one contact bubble overlaps the preset call area when a distance

between location information of the at least one contact bubble and location information of the preset call area is within a preset value, wherein the location information is physical location data on the screen. *See, e.g.*, Tutorial Video at 0:39 ("To merge calls for a group conversation, just drag a call on hold over your currently active call"):





318. With respect to claims 15-17, a Verizon smartphones and/or tablet running Verizon's One Talk application is an electronic device comprising a screen, one or more processors, memory coupled to the one or more processors, wherein the processors are configured to perform the operations recited in paragraphs 310 through 317 above.

319. As such, on information and belief, Verizon has directly infringed at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent by at least, for example, performing testing of Verizon's One Talk application in the United States, in violation of 35 U.S.C. § 271(a).

320. On information and belief, Verizon has infringed at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent by inducing others, including users of Verizon's One Talk application that it sells and/or offers, to infringe at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent in violation of 35 U.S.C. § 271(b).

321. On information and belief, Verizon takes active steps to induce infringement of at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent by others, including its customers, and

Verizon takes such active steps knowing that those steps will induce, encourage and facilitate direct infringement by others. Such active steps include, but are not limited to, encouraging, advertising (including by internet websites, television, store displays, print advertisements, *etc.*), promoting, and instructing others to use and/or how to engage in conference call management using enhanced contact bubbles on a mobile terminal in the United States. For example, Verizon induces users of Verizon's One Talk application to use one or more claimed inventions of the '839 Patent by instructing users how to engage in conference call management using enhanced contact bubbles on a mobile terminal. *See, e.g.*, Tutorial Video. On information and belief, Verizon knows or should know that such activities induce others to directly infringe at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent.

322. On information and belief, Verizon contributes to the infringement of at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent by others, including its customers. Acts by Verizon that contribute to the infringement of others include, but are not limited to, the sale, offer for sale, and/or importation by Verizon of mobile terminals, such as cell phones and tablets, that operate Verizon's One Talk application. Such mobile terminals are especially made for or adapted for use to infringe at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent and are at least a material part of those claims, for example, as described above with respect to claim 7. Verizon's One Talk application, including the functionality contributing to infringement of the '839 Patent, is not suitable for substantial noninfringing use.

323. By way of at least this Complaint, Verizon knows of the '839 Patent and performs acts that it knows, or should know, induce the direct infringement of at least claims 1, 3, 5, 10-11, and 15-17 of the '839 Patent by third parties.

324. Verizon undertook and continues its infringing actions despite an objectively high likelihood that such activities infringed the '839 Patent, which is presumed valid. For example, Verizon has been aware of an objectively high likelihood that its actions constituted, and continue to constitute, infringement of the '839 Patent and that the '839 Patent is valid since at least the filing of this action. Verizon could not reasonably subjectively believe that its actions do not constitute infringement of the '839 Patent, nor could it reasonably subjectively believe that the '839 Patent is invalid. Despite that knowledge, subjective belief, and the objectively high likelihood that its actions constitute infringement, Verizon has continued its infringing activities. As such, Verizon willfully infringes the '839 Patent.

325. Huawei has been irreparably harmed by Verizon's infringement of the '839 Patent and will continue to be harmed unless and until Verizon's infringement is enjoined by this Court.

326. By its actions, Verizon has injured Huawei and is liable to Huawei for infringement of the '839 Patent pursuant to 35 U.S.C. § 271.

DEMAND FOR JURY TRIAL

327. Huawei hereby demands trial by jury on all claims and issues so triable.

PRAYER FOR RELIEF

328. Wherefore, Huawei respectfully requests that this Court enter judgment against Verizon for the Asserted Patents as follows:

A. Finding that each of the Asserted Patents has been infringed by Verizon;

B. Finding that Verizon's infringement of the Asserted Patents has been willful;

C. Awarding damages adequate to compensate Huawei for the patent infringement that has occurred, in accordance with 35 U.S.C. § 284, including an assessment of pre-judgment and post-judgment interest and costs, and an accounting as appropriate for infringing activity not captured within any applicable jury verdict;

D. Awarding Huawei an ongoing royalty for Verizon's post-verdict infringement, payable on each product or service offered by Verizon that is found to infringe one or more of the Asserted Patents, and on all future products and services that are not colorably different from those found to infringe, or – in the alternative if Verizon refuses the ongoing royalty – permanently enjoining Verizon from further infringement;

E. Providing an award of all other damages permitted by 35 U.S.C. § 284, including increased damages up to three times the amount of compensatory damages found;

F. Finding that this is an exceptional case and an award to Huawei of its costs, expenses, and reasonable attorneys' fees incurred in this action as provided by 35 U.S.C. § 285; and

G. Providing such other relief, including other monetary and equitable relief, as this Court deems just and proper.

Dated: February 5, 2020

Respectfully submitted,

By: */s/ Thomas H. Reger II*

Ruffin B. Cordell (*pro hac vice* to be filed)
cordell@fr.com
FISH & RICHARDSON P.C.
100 Maine Avenue, S.W.
Washington, D.C. 20024
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

David Barkan (*pro hac vice* to be filed)
California Bar No. 160825
barkan@fr.com
FISH & RICHARDSON P.C.
500 Arguello Street, Suite 500 Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Thomas H. Reger II
Texas Bar No. 24032992
reger@fr.com
FISH & RICHARDSON P.C.
1717 Main Street, Suite 5000
Dallas, TX 75201
Telephone: (214) 747-5070
Facsimile: (214) 747-2091

Brian G. Strand
Texas Bar No. 24081166
strand@fr.com
FISH & RICHARDSON P.C.
1221 McKinney Street, Suite 2800
Houston, TX 77010
Telephone: (713) 654-5300
Facsimile: (713) 652-0109

John P. Palmer
Texas Bar No. 15430600
palmer@namanhowell.com
NAMAN, HOWELL, SMITH & LEE, PLLC
400 Austin Ave., Suite 800
P.O. Box 1470
Waco, Texas 76703
Phone: (254) 755-4100
Fax: (254) 754-6331

COUNSEL FOR PLAINTIFFS HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD., AND HUAWEI DIGITAL TECHNOLOGIES (CHENGDU) CO., LTD