

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

DUNTI NETWORK TECHNOLOGIES, LLC,

Plaintiff,

v.

**HUAWEI DEVICE USA, INC., HUAWEI
ENTERPRISE USA, INC. AND HUAWEI
TECHNOLOGIES USA, INC.,**

Defendants.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Dunti Network Technologies, LLC (“Dunti”), is the owner and assignee of patents critical to the efficiency, security, and scalability of modern communications networks. In recent years, defendants Huawei Device USA, Inc., Huawei Enterprise USA, Inc., and Huawei Technologies USA, Inc. (collectively “Huawei”) have adopted Dunti’s patented technologies—developed more than a decade ago right here in Texas—*en masse*. Huawei has profited handsomely from its use of Dunti’s patented inventions, and Dunti deserves to be compensated for this use. But Huawei has not paid Dunti its fair share. This lawsuit, which alleges infringement of Dunti’s U.S. Patent Nos. 6,587,462 (“the ’462 patent”); 6,788,701 (“the ’701 patent”); 6,804,235 (“the ’235 patent”); 6,643,286 (“the ’286 patent”); 7,778,259 (“the ’259 patent”); 6,912,196 (“the ’196 patent”), and 6,754,214 (“the ’214 patent”) (collectively, “the patents-in-suit”), is brought to ensure that Huawei pays Dunti what it fairly owes.

THE PARTIES

1. Dunti, based in Longview, Texas, is committed to advancing the current state of innovation in the field of secure, optimized data transmission across communication networks. In addition to the ongoing efforts of the lead inventor, Dunti employs a resident of Longview,

Texas as a Technology Analyst. Dunti is a Texas limited liability company with its principal place of business at 911 NW Loop 281, Suite 211-44, Longview, TX 75604.



2. Dunti is a small, Texas-based company. Dunti depends on patent protection to effectively license its innovative technologies and build its business. Like Defendant Huawei, Dunti relies on its intellectual property.

3. On information and belief, Defendant Huawei Device USA, Inc. is a Texas corporation with its principal office at 5700 Tennyson Pkwy., Suite 600, Plano, TX 75024. Huawei Device USA, Inc. can be served through its registered agent, C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136.

4. On information and belief, Defendant Huawei Enterprise USA, Inc. is a California corporation with its principal office at 3965 Freedom Circle, 11th Floor, Santa Clara, CA 95054. Huawei Enterprise USA, Inc. can be served through its registered agent, C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136.

5. On information and belief, Defendant Huawei Technologies USA, Inc. is a Texas corporation with its principal office at 5700 Tennyson Pkwy., Suite 600, Plano, TX 75024. Huawei Technologies USA, Inc. can be served through its registered agent, C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136.

6. On information and belief, according to Huawei's website, Huawei offers infringing products for sale throughout the United States and Canada, including in the Eastern District of Texas. Further, Huawei advertises its infringing products throughout the Eastern District of Texas and claims financial benefits through its conducting of business in Texas.

JURISDICTION AND VENUE

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

8. Upon information and belief, this Court has personal jurisdiction over Huawei Device USA, Inc. in this action because Huawei Device USA, Inc. has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Huawei Device USA, Inc. would not offend traditional notions of fair play and substantial justice. Defendant Huawei Device USA, Inc., directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Huawei Device USA, Inc.'s principal office is located in Plano, Texas, it is registered to do business in the State of Texas, and it has appointed C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136, as its agent for service of process.

9. Upon information and belief, this Court has personal jurisdiction over Huawei Enterprise USA, Inc. in this action because Huawei Enterprise USA, Inc. has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Huawei Enterprise USA, Inc. would not offend traditional notions of fair play and substantial justice. Defendant Huawei Enterprise USA, Inc., directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Huawei Enterprise USA, Inc. is registered to do business in the State of Texas and has appointed C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136, as its agent for service of process.

10. Upon information and belief, this Court has personal jurisdiction over Huawei Technologies USA, Inc. in this action because Huawei Technologies USA, Inc. has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Huawei Technologies USA, Inc. would not offend traditional notions of fair play and substantial justice. Defendant Huawei Technologies USA, Inc., directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Huawei Technologies USA, Inc.'s principal office is located in Plano, Texas, it is registered to do business in the State of Texas, and it has appointed C T Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136, as its agent for service of process.

11. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Huawei Device USA, Inc. is registered to do business in Texas, has its principal office in Plano, Texas, and, upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

12. Defendant Huawei Enterprise USA, Inc. is registered to do business in Texas and, upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

13. Defendant Huawei Technologies USA, Inc. is registered to do business in Texas, has its principal office in Plano, Texas, and, upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

DUNTI'S LANDMARK NETWORK COMMUNICATION SYSTEMS

14. Dunti is the owner and assignee of ten patents on pioneering network technologies, including the seven patents-in-suit (collectively, “the Dunti patents”).

15. Electrical engineer and entrepreneur Rupaka Mahalingaiah is a named inventor on each of the Dunti Patents and the founder of Dunti Corp. and Dunti LLC. For more than 30 years, Rupaka has worked at the cutting edge of computing and networking technologies.

16. Even today, female engineers are rare in the American workforce, comprising just over ten percent of all engineers in recent government surveys.¹ When Rupaka began her career in the 1980s, female engineers were rarer still—and *foreign-born, female, computer* engineers were almost inconceivable. Yet through many years of hard work, creativity, and innovation, Rupaka did more than just defy the odds (and overcome large-scale industry pushback and skepticism)—she became an American engineering success story by any measure.

17. After earning a Bachelor’s Degree in Electronic Engineering from Bangalore University and a Master’s Degree in Electrical Engineering from Virginia Tech, Rupaka began working at Concurrent Computer Corporation, a company that specialized in multi-processing systems used for real-time computing (i.e., computer systems that are subject to strict time constraints and must respond to inputs within milliseconds). While real-time computing performance is common today, real-time systems were state of the art at that time.

18. After several years at Concurrent, Rupaka joined Teradata, a hardware/software company built around research conducted at the California Institute of Technology (Caltech) specializing in database and parallel processor computing. At Teradata, Rupaka was responsible for architecting a next-generation, database supercomputer.

19. After briefly working at a networking startup in Austin, Rupaka joined Advanced Micro Devices (“AMD”), where she was one of the lead architects on K7/K7+, which became

¹ According to the Bureau of Labor Statistics Current Population Survey, women comprised just 10.3% of American engineers in 2003, and 11.7% in 2011. See, e.g., http://www.nsf.gov/statistics/wmpd/2013/pdf/tab9-2_updated_2013_11.pdf (accessed Sept. 6, 2016).

AMD's wildly successful Athlon processor. The original Athlon processor was the first desktop processor to reach speeds of one gigahertz. The Athlon processor's revolutionary architecture and design made these unprecedented speeds possible by allowing the processor to achieve substantially higher clocking speeds and to keep the processing pipeline full. The result was a faster, more efficient chip design.

20. Although she was only at AMD for three years, her contributions during that time were enduring, helping to generate billions of dollars in revenue and resulting in over 30 patents.² Her innovations at AMD have inspired others and been cited by nearly one-thousand United States patents and published patent applications as prior art before the United States Patent and Trademark Office, including by:

- International Business Machines Corporation;
- Oracle Corporation;
- Fujitsu Ltd.;
- Sun Microsystems, Inc.;
- Intel Corporation;
- Qualcomm Inc.;
- Cisco Technology, Inc.;
- Texas Instruments Inc.;
- ARM Holdings, PLC;
- Samsung Electronics Co. Ltd.;
- Freescale Semiconductor, Inc.;
- SK Hynix, Inc.;
- Rambus, Inc.;
- Hitachi, Ltd.; and
- Apple, Inc.

21. Rupaka left AMD in 1997 to become an entrepreneur, shifting her focus from architecting fast, efficient processors to architecting fast, efficient networks. She recognized the inefficiencies, lack of fault tolerance, and security vulnerabilities in then-state-of-the-art network designs, so she set out to solve the separate but related problems of (1) network inefficiency and (2) the lack of network security. It was at this time that Rupaka began to develop the technologies that would be the foundation of Dunti's next-generation networking systems.

² In total, Rupaka is a named inventor on nearly 50 issued U.S. patents.

22. In early 1999, Rupaka and Viren Kapadia began working together to perfect and expand on her network security and efficiency innovations.

23. Combining Rupaka's expertise in processor design and Viren's expertise in network communications, they created a new holistic network architecture that solved many of the problems inherent to computer networks of that time and that would become widely used in modern data centers. This new architecture combined efficient addressing schemes with built-in security and priority mechanisms to allow for faster, more efficient, and more secure networks that were backwards compatible with the networks of the time.

24. Recognizing the importance of what they had developed, Rupaka set out to build and commercialize this new network architecture, hiring a team of engineers to create several operational prototypes of the Dunti network module—the Dunti Trupta.³

25. With the working module prototypes in hand, Rupaka hired PricewaterhouseCoopers ("PWC") to audit the Dunti Trupta system and design. PWC engineers used the prototypes to set up a metropolitan area network and spent days running tests on the Dunti Trupta module prototypes and the network to verify their designs. At the end of the audit, PWC provided an audit report verifying the viability of the new network architectures and the modules for implementing those architectures.

26. Unfortunately, Rupaka set out to fund her technical innovations at the worst possible time—at the height of the dot-com and telecom crashes in late 2000 and early 2001. With venture capital all but extinct marketwide, Rupaka was unable to widely commercialize her Dunti inventions in this period.

27. But Rupaka's groundbreaking innovations in network architecture and module design did not go unnoticed, gaining the attention of the Department of Defense, the Department of Energy, and the Department of Homeland Security—all of which awarded her Small Business Innovation Research ("SBIR") grants to develop other computing and networking technologies.

³ "Trupta" means "complete" in Sanskrit.

In addition, in 2005, the Department of Defense asked Rupaka to present her technological innovations to the Defense Advanced Research Projects Agency (“DARPA”) to further the agency’s mission—to transform revolutionary concepts and even seeming impossibilities into practical capabilities.

28. The Dunti patents and applications have been cited by 418 United States patents and published patent applications as prior art before the United States Patent and Trademark Office. Companies whose patents cite the Dunti patents include:

- Avaya, Inc.;
- Hitachi Ltd.;
- Advanced Micro Devices, Inc.;
- Microsoft Corporation;
- Hewlett Packard Enterprise Development LP.;
- Cisco Technology, Inc.;
- F5 Networks, Inc.;
- AT&T Corporation;
- CA, Inc.;
- Brocade Communication Systems, Inc.;
- Intel Corporation;
- International Business Machines Corporation;
- Alcatel Lucent S.A.;
- Apple, Inc.;
- Marvell International, Ltd.;
- ZTE Corporation;
- Broadcom Corporation;
- Vodafone Group PLC;
- Nokia Corporation;
- NEC Corporation;
- Terascale Supercomputing, Inc.;
- Siemens AG;
- British Telecommunications PLC;
- Fujitsu, Ltd.;
- Ciena Corporation; and
- Texas Instruments, Inc.

TECHNOLOGY BACKGROUND

29. A communication network is generally regarded as an interconnected set of subnetworks that uses various networking protocols at various networking layers to

communicate information—in the form of data packets—across the network. Each networking layer provides some particular functionality using layer-specific networking protocols, such as the well-known IP and Ethernet protocols.

30. For example, the IP protocol is generally considered a layer 3 protocol. The IP protocol uses IP addresses—which are 32-bit addresses—to send and receive data over the internet by delivering packets from a sending (i.e., source) device to a receiving (i.e., destination) device.

31. As another example, the Ethernet protocol is generally considered a layer 2 protocol. The Ethernet protocol uses MAC addresses—which are 48-bit addresses that are unique to every internet-connected device—to send and receive data over the physical network.

32. Data is, therefore, sent from a source device to a destination device using IP addresses at layer 3 and MAC addresses at layer 2. But before that data is sent, the various networking layers divide the data into packets and wrap the data by placing the packets into datagrams that include additional control information, such as a header containing IP and MAC addresses. Data can be wrapped multiple times before being sent across the network.

33. Links of a network are connected by various hardware components, such as routers and switches.

34. Traditionally, routers operate at layer 3 and direct traffic across the internet by looking at the destination IP address in the IP-addressed packet, determining the best route for the packet, and then sending the packet to the next hop along the path to the destination. To determine the best route for a packet, a router compares the destination address against an internal routing table. Routing tables are dynamic and can accommodate multiple modules having IP addresses that change as the network is reconfigured with new routers, switches, or other network components. Thus, routers can adapt to network conditions by using complex routing algorithms and by updating the routing tables accordingly.

35. Unlike routers, switches traditionally operate at layer 2 and use MAC addresses to forward packets to the next hop without first determining the best route. Switches receive data

packets on a particular input port and then send them to a particular output port (or ports). This operation can be quickly repeated each time a packet is received. Because of this, data travels faster through switches than it does through routers.

LIMITATIONS OF THEN-STATE-OF-THE-ART SYSTEMS

36. The next-generation technologies described in the Dunti patents addressed a number of limitations of then-state-of-the-art systems.

37. First, the next-generation technologies described in the Dunti patents addressed problems associated with using a single addressing domain, such as IP addressing, for all internet-connected devices.

38. For example, as explained in the Dunti patents, using a common IP addressing domain for every node in a network made up of hundreds, thousands, or even more sub-networks can pose several problems. The first major version of IP, called IPv4, uses 32-bit IP addresses; thus, the maximum number of possible IPv4 addresses in the IP addressing domain is approximately 4.3 billion. Given the explosive growth of the Internet and the constantly increasing number of internet-connected devices, the inventors of the Dunti patents recognized that the IPv4 addressing domain would soon become insufficient, and by 2011, this was indeed the case. They also recognized that simply increasing the size of the IP addressing domain (and therefore, the number of available IP addresses) by adding bits to the addressing domain would increase the amount of decoding required and, as a result, the amount of time required for routing.

39. Second, the next-generation technologies described in the Dunti patents addressed problems associated with slow routing-table lookups.

40. For example, a packet can travel through many hops before arriving at its destination, with each hop requiring a complex address-translation operation. As described above, because of the complex routing-table lookups required at each hop to make routing

decisions, routing can be a relatively slow process. Switches, on the other hand, are relatively fast, but, unlike routers, they are not able to adapt to changes in traffic conditions.

41. Third, the next-generation technologies described in the Dunti patents addressed problems associated with security and prioritization of data packets as they traverse a network.

42. For example, common network security mechanisms have traditionally included firewalls implemented in hardware and software, and authentication systems implemented in software, such as encryption and passwords. Firewalls, which analyze incoming packets to determine if a packet should be placed on the internal network, add latency at the interface between the external and internal networks and generally operate at a single point in the communication path rather than over the entire communication path. In addition, they can be difficult to configure because each firewall must be updated and configured separately as needs change.

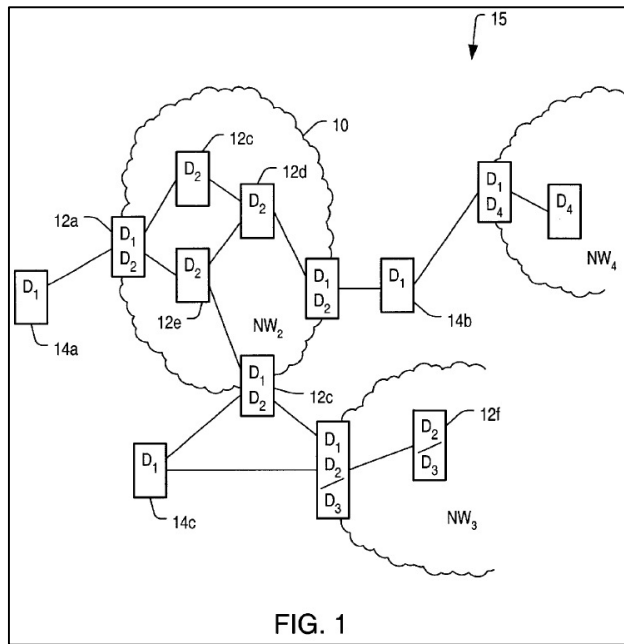
43. Encryption adds overhead to the packet and involves time-consuming decryption at the receiving end. Using passwords takes up less transmission bandwidth than encryption, but passwords can sometimes be broken either because of a user's improper choice of password or through a brute-force attack.

DUNTI'S NEXT-GENERATION NETWORKING SOLUTIONS

44. The next-generation networking technology described in the Dunti patents covers various aspects of networking systems that work together to provide networks that are faster, more efficient, more scalable, and more secure.

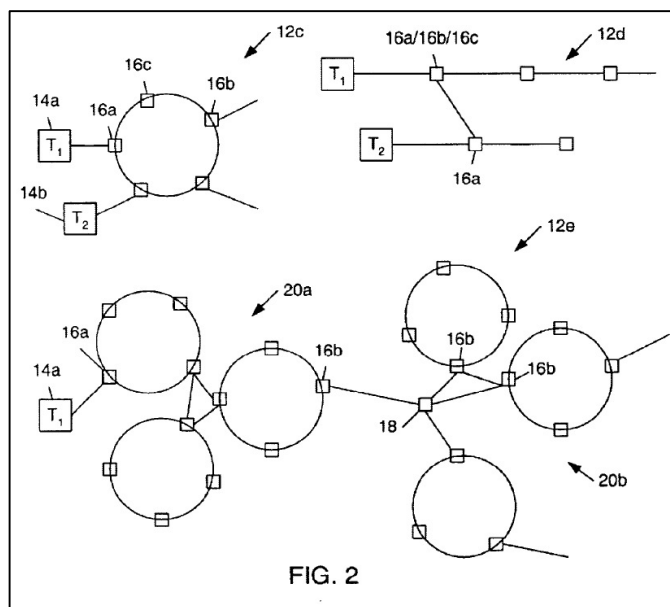
45. For example, some of the Dunti patents describe, among other things, using multiple separate and independent addressing domains to overcome the mathematical and practical limitations of the traditional IP packet addressing domains to allow for the transmission of data packets more quickly and efficiently than was possible with any prior art systems. They describe architectures, systems, and methods for transparently mapping addresses across multiple addressing domains, as shown, for example, in the figure below. Because an addressing domain in one network is separate from an addressing domain in another network, a module in the first

network and a module in the second network can each have the same identifier, which allows addressing (such as IP addresses) to be reused among networks. These new designs allow for the segmentation of a given network, permitting multiple networks and/or multiple services to share the same infrastructure.



'462 Patent, Fig. 1.

46. As another example, some of the Dunti patents describe using intelligent network infrastructure and hierarchical networks to more efficiently transfer data packets across a network, as shown, for example, in the figure below. By structuring a network and informing each module of its relative location within the network, modules internal to a particular network can operate as switches, quickly forwarding packets towards their final destination. As a result, only modules at the edges of a given network are required to analyze or decode the destination address of the packet.



'286 Patent, Fig. 2.

47. As another example, other Dunti patents describe using a packet-based security mechanism that prevents decryption techniques and password attacks. This packet-level security mechanism also enables hosts that are connected across a public network to be connected to form secure virtual networks by modifying the contents of packets in such a way that only the destined host that is part of the same secure virtual network will be able to restore the contents of the packet when it is received.

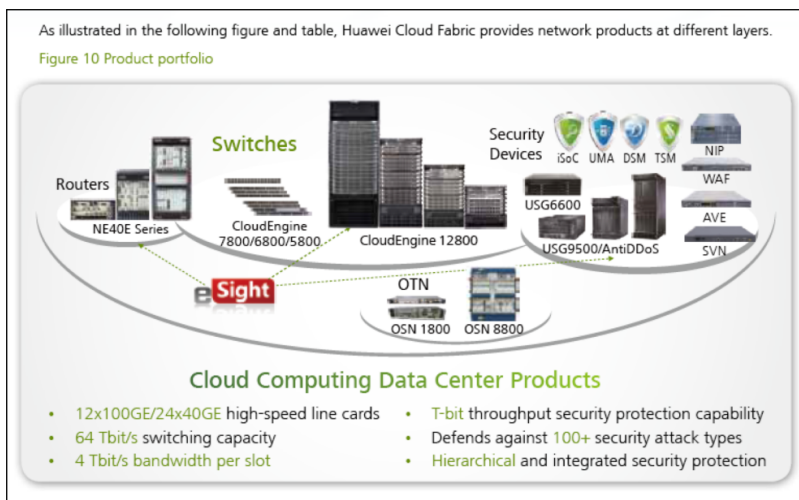
48. The continued growth of the number of internet-connected devices and internet-based services, as well as a recent shift toward cloud-based services, has led to wide adoption of Dunti's next-generation networking technology in the industry. For example, Dunti's next-generation networking technology has particular applicability to data-center networking and has been widely implemented by many major networking companies as part of their data center fabric solutions to provide faster, more efficient, more scalable, and more secure data centers. Dunti's next-generation networking technology also applies to the backbone ring networks that connect multiple data center physical locations into a single virtual data center.

HUAWEI’S INFRINGING PRODUCTS AND SERVICES

49. On information and belief, Huawei offers a high-performance data-center networking solution called the Cloud Fabric Data Center Solution (“Cloud Fabric”), which, as Huawei describes it, allows its customers “to build an elastic, simple, and open next-generation cloud data center network that supports sustainable cloud service development. Huawei Cloud Fabric uses Huawei’s flagship, high-performance CloudEngine (CE) series data center switches.” See *Huawei Cloud Fabric Data Center Solution*, HUAWEI SOLUTION BROCHURE (2014), at 3.

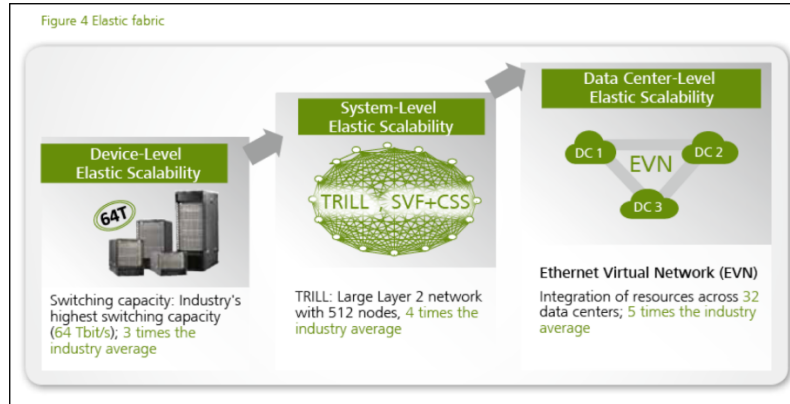
50. On information and belief, Cloud Fabric “implements full-scale network openness, providing an open fabric, an open controller, and an open ecosystem” in order to assist with customer adoption of the Cloud Fabric. *Huawei Cloud Fabric Data Center Solutions*, HUAWEI SOLUTION BROCHURE (2014), at 7. Huawei “is proactive in building a cloud computing data center ecosystem” and “has been cooperating with world-renowned IT vendors and standards organizations” to actively encourages the adoption of its products by enterprise customers. *Id.*

51. On information and belief, Huawei provides to its customers both hardware and software products as part of its Cloud Fabric solution, including, for example, the Huawei CloudEngine series data center switches, the Huawei Agile Controller, and the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8).



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.

52. On information and belief, the Cloud Fabric solution supports the Transparent Interconnection of Lots of Links (“TRILL”) protocol as a way of providing system-level scalability and efficiency.



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

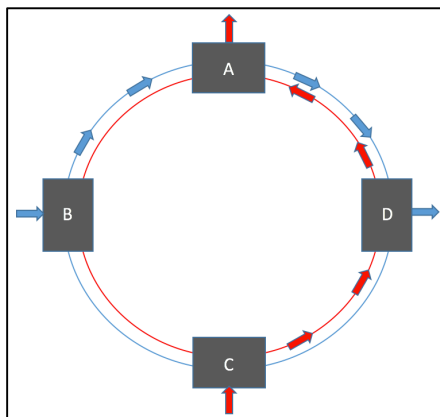
System-Level Elastic Scalability: Huawei Cloud Fabric seamlessly supports Transparent Interconnection of Lots of Links (TRILL), a standard IETF protocol. A typical TRILL network consisting of core and TOR switches is used to build a large Layer 2 network with over 512 nodes. Over 18,000 10GE servers can be deployed on a TRILL network. Huawei Cloud Fabric provides a combined solution of Huawei's proprietary Cluster Switch System (CSS) and Super Virtual Fabric (SVF). This combined solution virtualizes multiple homogeneous or heterogeneous physical switches into one logical switch, simplifying network management and improving network reliability. CSS is a core switch clustering technology that horizontally (east-west) virtualizes multiple core switches into one core switch. SVF expands heterogeneous core switches vertically (south-north). Multiple leaf switches are virtualized into remote line cards on a spine switch, which flexibly expands interfaces and simplifies cable layout and device management in equipment rooms. Huawei SVF is the only technology that implements local forwarding on leaf switches. Since the majority of the data center traffic is east-west traffic, SVF can maximize forwarding efficiency and reduce network latency.

Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

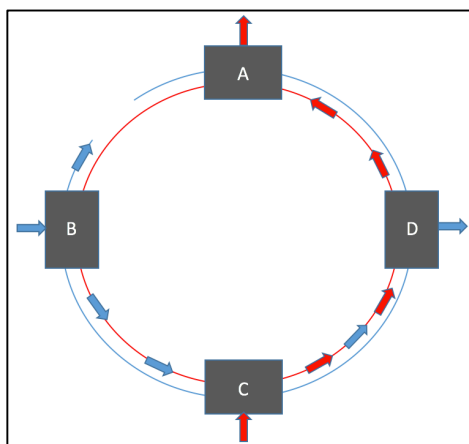
53. In addition to Cloud Fabric, on information and belief, Huawei also offers a number of products and services that implement IEEE 802.17 Resilient Packet Ring (“RPR”) networks. For example, the Huawei Enhanced OSN Series MSTP Product Series, including at least the Huawei OptiX OSN 1500, Huawei OptiX OSN 2500, Huawei OptiX OSN 3500, and Huawei OptiX OSN 7500, implement an RPR network.

54. RPR networks, which transport data traffic over widespread optical fiber rings, can be used to connect data centers that are spread across multiple physical locations or to connect smaller networks to larger and/or backbone networks.

55. RPR networks include dual, counter-rotating rings that are implemented using a series of switches located around the rings where traffic enters and exits the network.



56. The dual-ring topology provides robustness by including the capability of automatic reconfiguration after a link failure. If a node on the ring or a link between two nodes is disrupted or fails, traffic can be looped back around the ring in the opposite direction to the destination node and avoid the disruption/failure.



COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,587,462

57. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

58. U.S. Patent No. 6,587,462 (“the ’462 patent”), entitled “Address Mapping Mechanism Enabling Multi-Domain Addressing in Communication Networks, was filed on February 16, 2001. Dunti is the owner by assignment of the ’462 patent. A true and correct copy of the ’462 patent is attached hereto as Exhibit A. The ’462 patent claims a specific

architecture, systems, and methods for transparently mapping addresses across multiple addressing domains and/or protocols.

59. The '462 patent has been cited by at least fifteen United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '462 patent as relevant prior art:

- Hewlett Packard Enterprise Development LP;
- International Business Machines Corporation;
- Terascale Supercomputing, Inc.;
- NEC Corporation; and
- Microsoft Corporation.

60. The '462 patent teaches, for example, a networking system with multiple independent addressing domains. Because an addressing domain in a first network is separate from an addressing domain in a second network, the first and second networks need not have a common addressing mechanism in which each module of both the first and second networks requires a unique identification number. Instead, a module in the first network and a module in the second network can each have the same identifier, which allows addressing to be reused among networks.

61. The end modules and termination devices, however, must have a common addressing scheme, in which each end module and termination device has its own unique identifier. Thus, while the end modules and termination devices connected to the end modules have unique and corresponding lower layer addresses, the intermediate modules in the networks can have an independent set of identifiers separate from those of the end modules and termination devices.

62. Set up in this way, sending a data packet from a termination device to another termination device, separated by a network with an internal addressing domain that is different from external addressing domains, uses a simple mapping function. The entry end module adds to the data packet the separate addressing protocols unique to the internal modules, such that the packet includes the IP source and destination addresses, the Ethernet source and destination

addresses, and the internal source and destination addresses of the network. The internal addresses are added when the data packet enters the network and are stripped when the data packet leaves the network.

63. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

64. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, “the Huawei CE Switches”).

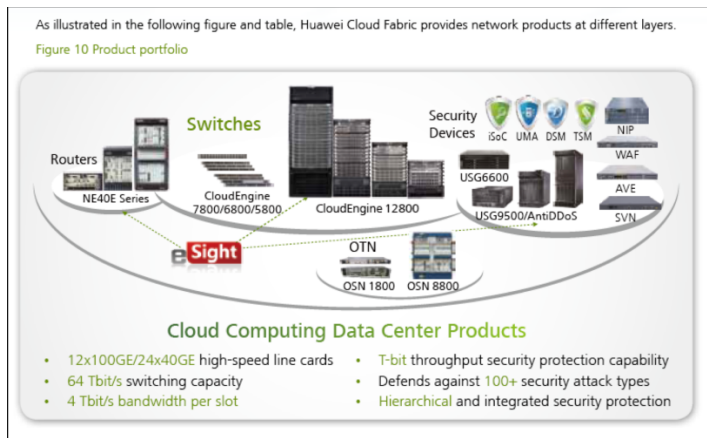
65. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Agile Controller.

66. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8), which runs on the Huawei CE Switches.

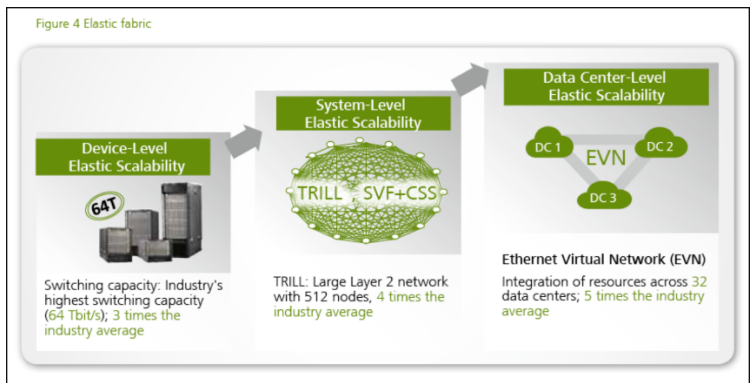
67. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE Switches, the Huawei Agile Controller, and the Huawei VRP8 Network Operating System (collectively, “the Huawei ’462 Accused Products”).

68. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei ’462 Accused Products (“a Huawei ’462 Accused Product Network”).

69. On information and belief, a Huawei ’462 Accused Product Network implements at least Huawei’s Cloud Fabric and/or the TRILL protocol.

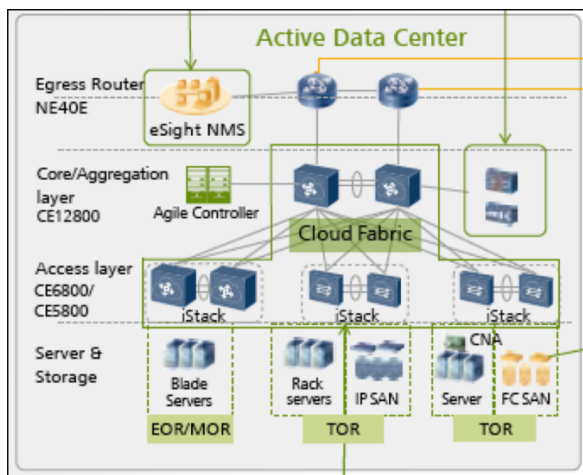


Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.



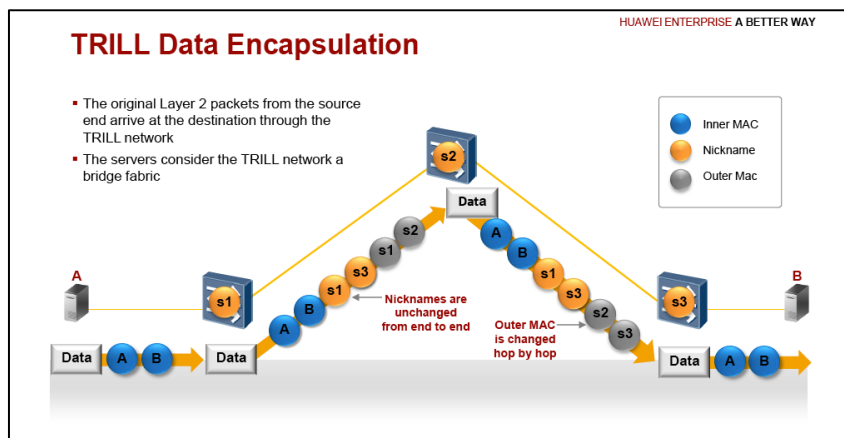
Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

70. On information and belief, a Huawei '462 Accused Product Network comprises a communication system.



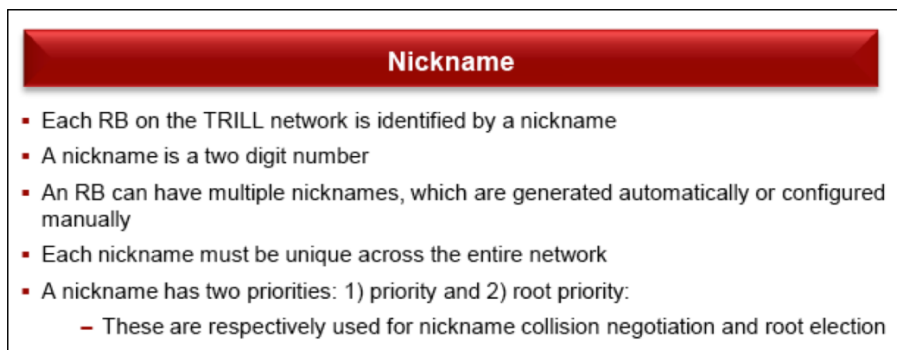
Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 4.

71. On information and belief, a Huawei '462 Accused Product Network comprises an entry end module, an exit end module, and at least one intermediate module between the entry end module and the exit end module. For example, the figure below shows an entry end module and an exit end module at the edges of a Cloud Fabric network and an intermediate module coupled between the entry and exit end modules. In a Cloud Fabric network, there can be multiple intermediate modules.



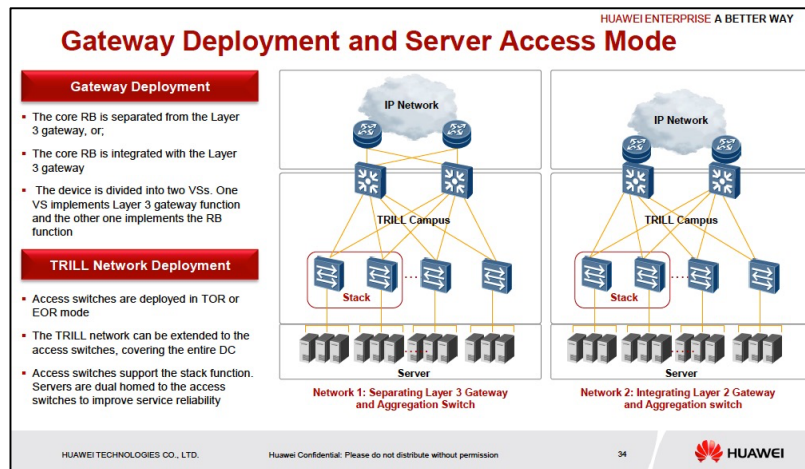
TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 7.

72. On information and belief, a Huawei '462 Accused Product Network comprises a first addressing domain for identifying each of the end modules and the intermediate module. For example, each RBridge within a Cloud Fabric network is assigned a unique RBridge Nickname.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 8.

73. On information and belief, a Huawei '462 Accused Product Network comprises a second addressing domain, separate and independent from the first addressing domain, for identifying each of the end modules exclusive of identifying the intermediate module. For example, edge switches in a Huawei '462 Accused Product Network can be addressed using IP addresses, but IP addresses are not used to address transit R Bridges when forwarding packets within a Cloud Fabric network.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 34.

74. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '462 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '462 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

75. On information and belief, Huawei also indirectly infringes the '462 patent by actively inducing infringement under 35 U.S.C. § 271(b).

76. On information and belief, Huawei has had knowledge of the '462 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '462 patent and knew of its infringement, including by way of this lawsuit.

77. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '462 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its

inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '462 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '462 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '462 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '462 patent, including at least claim 1, and Huawei further provides documentation and training materials that cause customers of the Huawei '462 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '462 patent. By providing instruction and training to customers on how to use the Huawei '462 Accused Products, Huawei specifically intended to induce infringement of the '462 patent, including at least claim 1. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '462 Accused Products and to actively induce its customers to infringe the '462 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '462 patent, knowing that such use constitutes infringement of the '462 patent.

78. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '462 patent.

79. As a result of Huawei's infringement of the '462 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,788,701

80. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

81. U.S. Patent No. 6,788,701 (“the ’701 patent”), entitled “Communication Network Having Modular Switches that Enhance Data Throughput,” was filed on May 14, 1999. Dunti is the owner by assignment of the ’701 patent. A true and correct copy of the ’701 patent is attached hereto as Exhibit B. The ’701 patent claims a specific architecture, system, and method for efficiently transferring packets of data across a communication network.

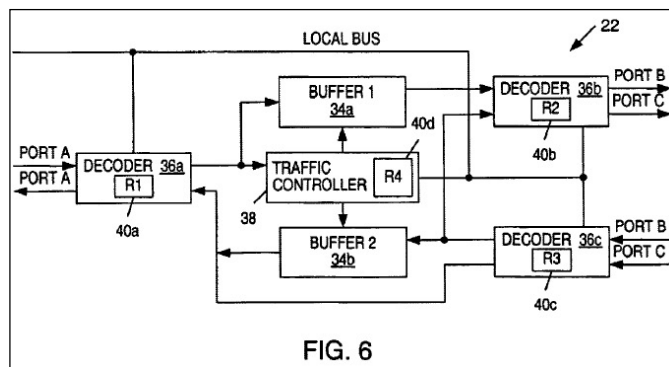
82. The ’701 patent has been cited by at least fifteen United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ’701 patent as relevant prior art:

- Alcatel Lucent S.A.;
- Terascale Supercomputing, Inc.;
- Arbor Networks, Inc.;
- Apple, Inc.;
- International Business Machines Corporation;
- Marvell International, Ltd.; and
- Ericsson.

83. The ’701 patent teaches, for example, an addressing and distributed routing mechanism used by forwarding modules (i.e., switches) that are topologically related to one another based on their position within a network. The modules, due to an awareness of their position or location with respect to the network, enable adaptive fast forwarding of packets across the network. Instead of statically routing packets in the same manner each time, as in conventional switches, the modules include some features of conventional routers, but without the detriments of routers. The modules can forward packets of data relatively quickly (similar to conventional switches), and can dynamically change the forwarding path based on activity within the network (similar to conventional routers).

84. The switches described in the ’701 patent can be used to forward or route incoming packets received on an input port to one or more output ports. Each switch within the network is assigned a unique identification number that is used for routing within the network. When a switch within the network receives an incoming packet on an input port, it decodes part of the packet to direct the packet to the appropriate output port, as shown in Figure 6 below. The

switches are aware of their position relative to the network and their neighboring modules, and they use that knowledge to determine which output port to use for forwarding the packet.



'701 Patent, Fig. 6.

85. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

86. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, "the Huawei CE Switches").

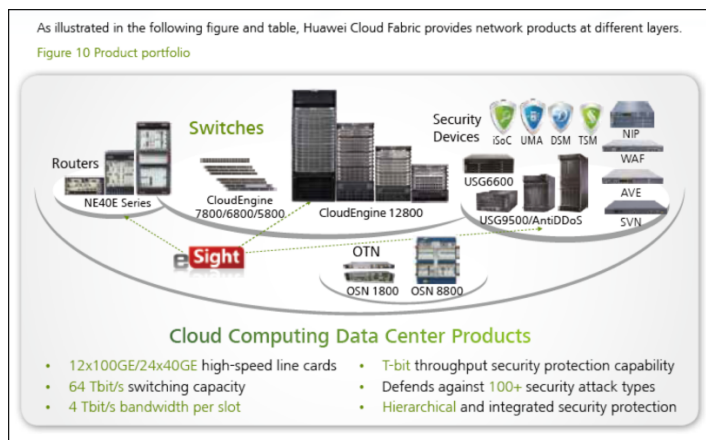
87. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Agile Controller.

88. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8), which runs on the Huawei CE Switches.

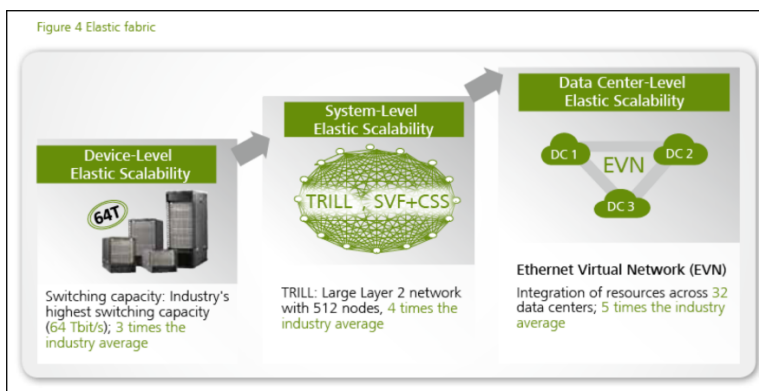
89. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE Switches, the Huawei Agile Controller, and the Huawei VRP8 Network Operating System (collectively, "the Huawei '701 Accused Products").

90. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei '701 Accused Products ("a Huawei '701 Accused Product Network").

91. On information and belief, a Huawei '701 Accused Product Network implements at least Huawei's Cloud Fabric and/or the TRILL protocol.

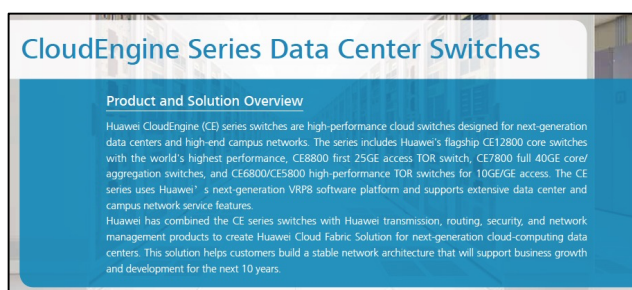


Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

92. On information and belief, the Huawei '701 Accused Products comprise a switch.



CloudEngine Series Data Center Switches, HUAWEI PRODUCT BROCHURE (2016), at 1.

93. On information and belief, the Huawei '701 Accused Products within a Cloud Fabric network comprise a traffic manager which dispatches a series of read operations to a memory coupled within a data flow path. For example, the Huawei '701 Accused Products include memory and at least one processor.

4T High-Density Line Cards

- The forwarding capacity of a line card can reach up to 3.6 Tbit/s.
- The CE12800 supports 36*40GE, 36*100GE, 144*25GE, and 144*10GE line cards, which provide line-rate forwarding.
- The CE12800 provides as many as 576*100GE, 576*40GE, 2,304*25GE, or 2,304*10GE line-rate ports.

Super-Large Buffer Size of 24 GB

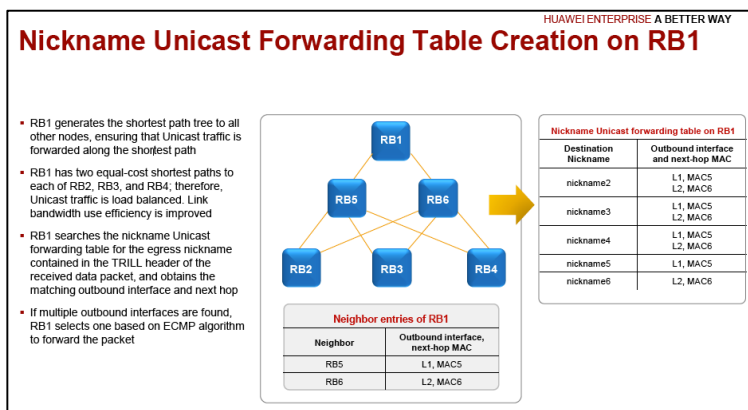
- All service ports (100GE/40GE/10GE/GE) provide a super high buffer capacity (up to 200 ms).
- The distributed buffer mechanism on inbound interfaces can effectively handle incast traffic loads in data centers.
- A line card provides up to 24 GB buffer, which is dynamically shared by interfaces to improve usage efficiency.

Back-to-Back Non-Blocking System

- The CE12816 is the industry's first data center core switch to support a non-blocking system. Two CE12816 switches can be upgraded to a CE12832 through back-to-back connection of Switch Fabric Units (SFUs). The new chassis provides 32 service slots.
- A CE12832 system is a non-blocking system using Clos multi-stage switching architecture. All traffic between two CE12816 chassis can be forwarded without occupying any service interface.
- The CE12832 can be upgraded through an in-service upgrade. This ensures continuous evolution and expansion of the customer service system.

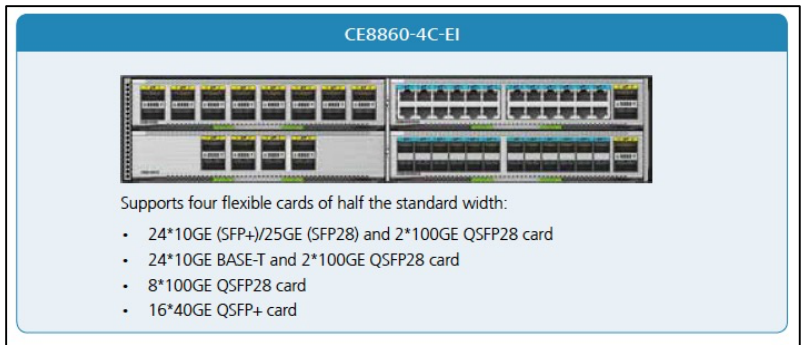
Data Sheet, *CloudEngine 12800 Series Data Center Core Switches*, HUAWEI TECHNICAL DOCUMENTATION (2016), at 2.

94. On information and belief, the Huawei '701 Accused Products within a Cloud Fabric network include a Nickname unicast forwarding table comprised in memory, which includes a source address and a destination address of a pair of network nodes routably coupled within the data flow path.



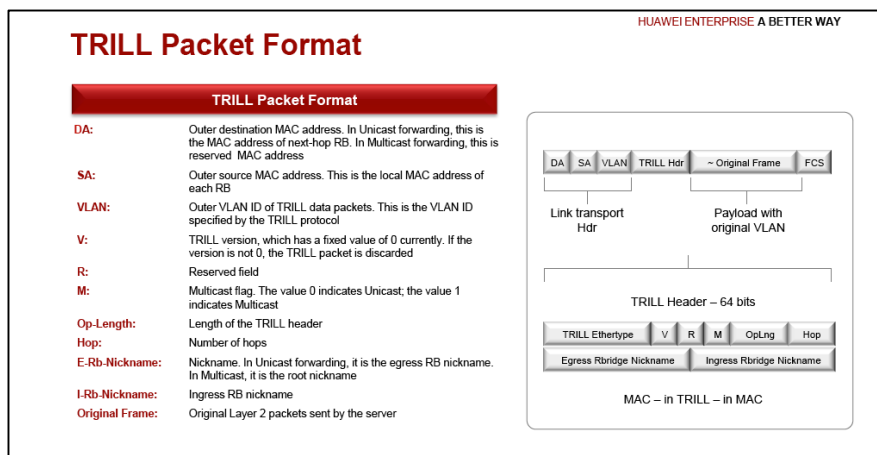
TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 18.

95. On information and belief, the Huawei '701 Accused Products comprise an input port and an output port.



CloudEngine Series Data Center Switches, HUAWEI PRODUCT BROCHURE (2016), at 2.

96. On information and belief, the memory in the Huawei '701 Accused Products comprises packets of data dispatched from the input port. For example, the Huawei '701 Accused Products encapsulate incoming data packets within a Link Transport Header and a TRILL Header. Incoming data packets are comprised in memory within an ingress RBridge as they are encapsulated in the Link Transport Header and the TRILL Header as forwarding decisions are made.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 6.

97. On information and belief, the Huawei '701 Accused Products comprise a decoder coupled to the input port for decoding only a single field of bits within a plurality of fields which comprise the destination address. For example, a TRILL Header includes an Egress Rbridge Nickname field and a Link Transport Header includes an RBridge outer destination

MAC address, both of which comprise a destination address. The Egress RBridge Nickname is decoded as forwarding decisions are made.

98. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '701 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '701 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

99. On information and belief, Huawei also indirectly infringes the '701 patent by actively inducing infringement under 35 U.S.C. § 271(b).

100. On information and belief, Huawei has had knowledge of the '701 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '701 patent and knew of its infringement, including by way of this lawsuit.

101. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '701 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '701 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '701 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '701 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '701 patent, including at least claim 1, and Huawei further provides documentation and training materials that cause customers of the Huawei '701 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '701 patent. By providing instruction and training to customers on how to use the Huawei '701 Accused Products, Huawei specifically intended to induce infringement of the '701 patent, including at least claim 1. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '701 Accused Products and to actively induce its customers to infringe the '701 patent. Accordingly,

Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '701 patent, knowing that such use constitutes infringement of the '701 patent.

102. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '701 patent.

103. As a result of Huawei's infringement of the '701 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 6,804,235

104. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

105. U.S. Patent No. 6,804,235 ("the '235 patent"), entitled "Address Mapping Mechanism Enabling Multi-Domain Addressing in Communication Networks," was filed on February 27, 2003 and claims priority as a continuation of U.S. Patent Application No. 09/785,899, filed on February 16, 2001. Dunti is the owner by assignment of the '235 patent. A true and correct copy of the '235 patent is attached hereto as Exhibit C.

106. The '235 patent has been cited by six United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '235 patent as relevant prior art:

- Texas Instruments, Inc.; and
- International Business Machines Corporation.

107. The '235 patent teaches, for example, a communication system that transparently maps addresses across multiple addressing domains and/or protocols. The communication system described in the '235 patent operates using a scalable addressing domain of an independent identification layer that is different from the addressing domain interfacing with the

network. This independent identification layer is an improvement to the OSI reference model and can be considered an even lower layer addressing domain within the OSI reference model because the existing lower-level layer addressing information is further wrapped with the independent identification layer addressing information.

108. The independent identification layer can be used to represent, for example, unique identification numbers of intermediate modules within the communication system of the '235 patent. The networking modules described in the '235 patent can be classified as either end modules (i.e., entry and exit end modules) or as intermediate modules. End modules are coupled to other networks, addressing domains, or devices outside of the network. Entry end modules perform protocol wrapping functions as data packets enter the network, and exit end modules strip protocol used by the network as data packets exit the network. Identification addresses for the intermediate modules and end modules of a given network can utilize that network's unique and independent identification layer.

109. As described in the '235 patent, sending a data packet from a source device to a destination device, where the devices are separated by a network with an internal addressing domain that is different from the external addressing domains, requires only a simple mapping function. One addressing domain can be used to forward data from a source device to a unique entry end module and from an exit end module to the destination device. Within the network, among the intermediate modules, a separate and independent addressing domain can be used.

110. When data packets enter a network from a device external to the network, the IP address and Ethernet address within the network layer and the lower-level data/physical layer addressing domains are further wrapped with the independent identification layer source address and corresponding destination addresses unique to that addressing domain. The wrapped information indicates where the data came from external to the network and, due to the wrapped independent identification layer, where within the network the data enters the network and exits the network. When data packets exit the network, an end module strips the wrapped information from the packets.

111. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

112. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, “the Huawei CE Switches”).

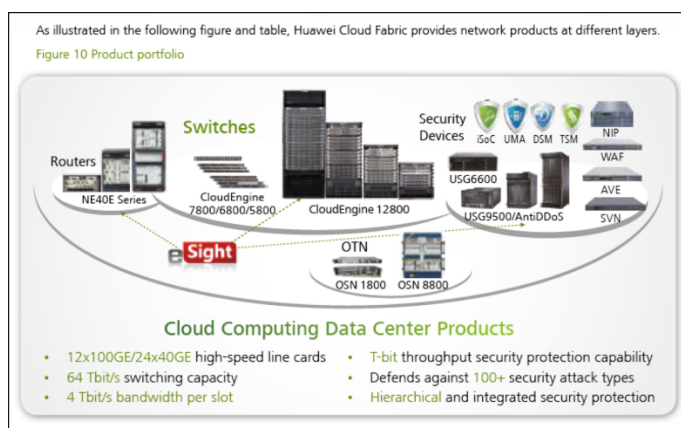
113. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Agile Controller.

114. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8), which runs on the Huawei CE Switches.

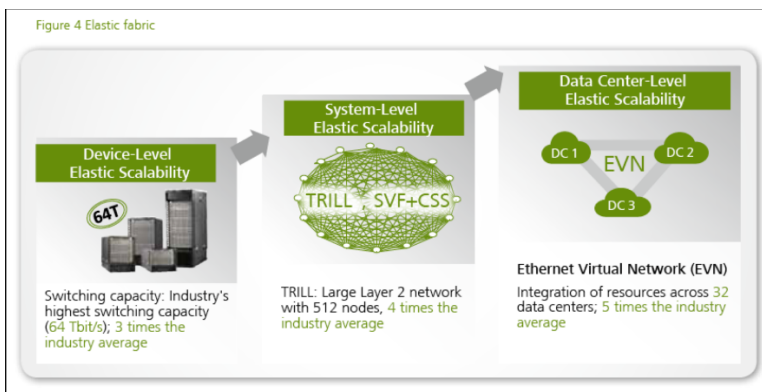
115. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE Switches, the Huawei Agile Controller, and the Huawei VRP8 Network Operating System (collectively, “the Huawei ’235 Accused Products”).

116. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei ’235 Accused Products (“a Huawei ’235 Accused Product Network”).

117. On information and belief, a Huawei ’235 Accused Product Network implements at least Huawei’s Cloud Fabric and/or the TRILL protocol.



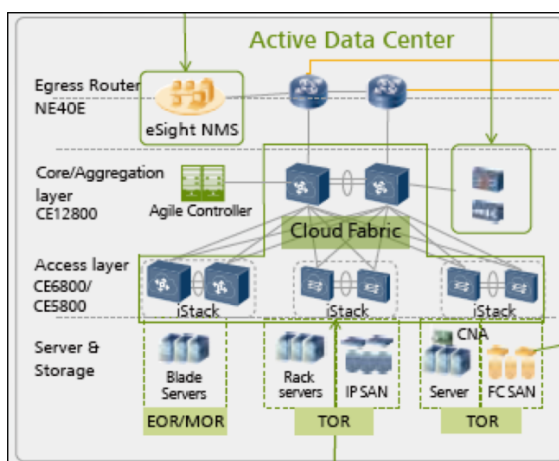
Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

118. On information and belief, a Huawei '235 Accused Product Network comprises a communication network.

119. On information and belief, a Huawei '235 Accused Product Network comprises a plurality of interconnected modules adapted to direct packets of data through the network.



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 4.

120. On information and belief, modules within a Huawei '235 Accused Product Network are identified according to identification numbers contained within a first addressing domain of a first model layer independent and separate from a second addressing domain of a second model layer used to identify modules which forward and receive the packets of data outside the network. For example, each RBridge within a Cloud Fabric network is assigned a unique RBridge Nickname, which is a unique identification number that is independent of the MAC address, and can be assigned to different TRILL network topologies.

Nickname

- Each RB on the TRILL network is identified by a nickname
- A nickname is a two digit number
- An RB can have multiple nicknames, which are generated automatically or configured manually
- Each nickname must be unique across the entire network
- A nickname has two priorities: 1) priority and 2) root priority:
 - These are respectively used for nickname collision negotiation and root election

TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 8.

121. On information and belief, the first model layer used in a Huawei '235 Accused Product Network is an improvement to, and is lower than, a physical layer of the OSI reference model. For example, data packets entering a Cloud Fabric network, which already include headers from higher layers, are further wrapped/encapsulated within a TRILL header that includes the RBridge Nickname of the egress RBridge.

HUAWEI ENTERPRISE A BETTER WAY

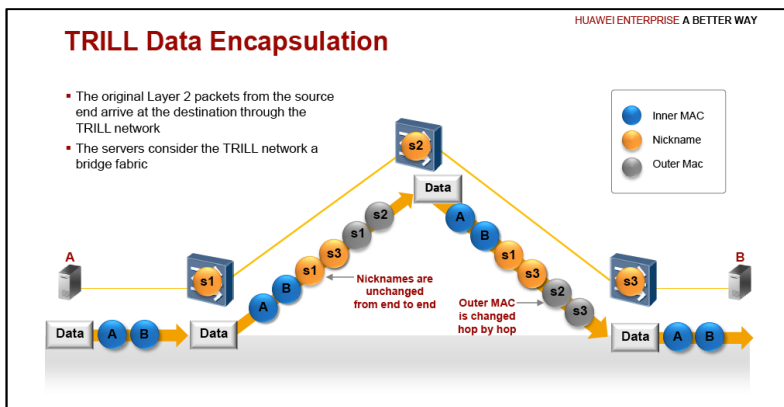
TRILL Packet Format

TRILL Packet Format

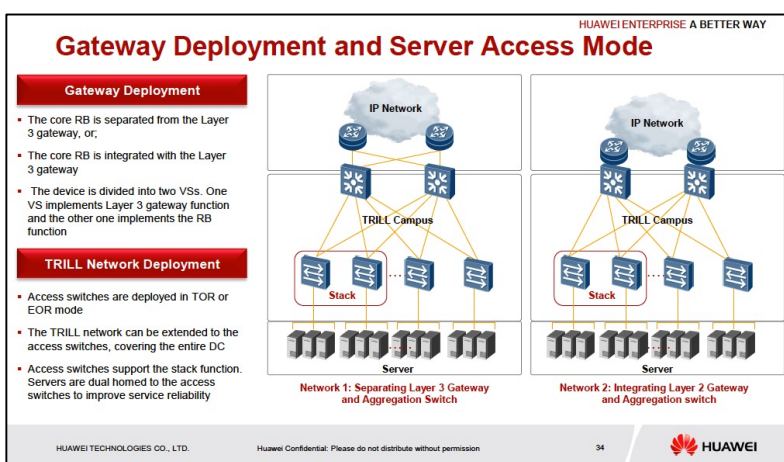
DA:	Outer destination MAC address. In Unicast forwarding, this is the MAC address of next-hop RB. In Multicast forwarding, this is reserved MAC address
SA:	Outer source MAC address. This is the local MAC address of each RB
VLAN:	Outer VLAN ID of TRILL data packets. This is the VLAN ID specified by the TRILL protocol
V:	TRILL version, which has a fixed value of 0 currently. If the version is not 0, the TRILL packet is discarded
R:	Reserved field
M:	Multicast flag. The value 0 indicates Unicast, the value 1 indicates Multicast
Op-Length:	Length of the TRILL header
Hop:	Number of hops
E-Rb-Nickname:	Nickname. In Unicast forwarding, it is the egress RB nickname. In Multicast, it is the root nickname
I-Rb-Nickname:	Ingress RB nickname
Original Frame:	Original Layer 2 packets sent by the server

TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 6.

122. On information and belief, the second model layer used in a Huawei '235 Accused Product Network is higher than a physical layer of the OSI reference model. For example, the edge RBridges in a Huawei '235 Accused Product Network can use IP addresses to route data packets outside of a Cloud Fabric network, and the IP address layer is higher than a physical layer of the OSI model.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 7.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 34.

123. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '235 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '235 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

124. On information and belief, Huawei also indirectly infringes the '235 patent by actively inducing infringement under 35 U.S.C. § 271(b).

125. On information and belief, Huawei has had knowledge of the '235 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '235 patent and knew of its infringement, including by way of this lawsuit.

126. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '235 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '235 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '235 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '235 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '235 patent, including at least claim 1, and Huawei further provides documentation and training materials that cause customers of the Huawei '235 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '235 patent. By providing instruction and training to customers on how to use the Huawei '235 Accused Products, Huawei specifically intended to induce infringement of the '235 patent, including at least claim 1. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '235 Accused Products and to actively induce its customers to infringe the '235 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '235 patent, knowing that such use constitutes infringement of the '235 patent.

127. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '235 patent.

128. As a result of Huawei's infringement of the '235 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 6,643,286

129. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

130. U.S. Patent No. 6,643,286 (“the ’286 patent”), entitled “Modular Switches Interconnected Across a Communication Network to Achieve Minimal Address Mapping or Translation Between Termination Devices,” was filed on May 14, 1999. Dunti is the owner by assignment of the ’286 patent. A true and correct copy of the ’286 patent is attached hereto as Exhibit D. The ’286 patent claims a specific architecture, system, and method for efficiently transferring packets of data across a communication network with hierarchical levels of high speed switches throughout the network.

131. The ’286 patent has been cited by fourteen issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ’286 patent as relevant prior art.

- Google, Inc.;
- Ciena Corporation;
- Advanced Micro Devices, Inc.; and
- Fujitsu Ltd.

132. The ’286 patent teaches, for example, an addressing and distributed routing mechanism used by forwarding modules within a network that perform fast decoding to forward data packets, thereby reducing the number of full network address mapping/translation operations as the packet traverses the network. It claims a technical solution to a problem unique to computer networks—quickly and efficiently transmitting data packets through a computer network without needing to perform a full network address mapping/translation operation at every intermediate node.

133. The forwarding modules of the ’286 patent are topologically related to one another based on their position within the network and can perform adaptive fast forwarding of

packets across the network due to an awareness of their position or location with respect to the network.

134. The adaptive fast forwarding occurs through decoding operations using a series of comparisons within only select switches. An entry end switch wraps entering data packets with internal control information that includes an originating identification number of the entry end switch and an identification number of the exit end switch. The wrapped packet can then be forwarded through the structured network without performing full network address translation operations at each hop. When the packet arrives at the exit end switch, the internal control information of the network is stripped from the packet, and a mapping table is used to forward the packet to a destination termination device connected to the exit end switch. This full network address translation at the exit end switch bridges the gap between the structured network and any external protocol or domain.

135. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

136. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, “the Huawei CE Switches”).

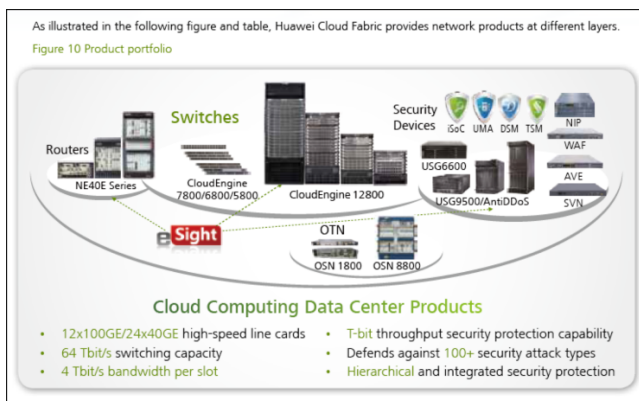
137. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Agile Controller.

138. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8), which runs on the Huawei CE Switches.

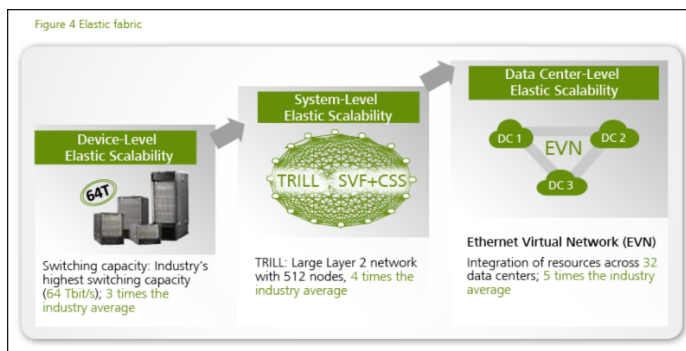
139. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE Switches, the Huawei Agile Controller, and the Huawei VRP8 Network Operating System (collectively, “the Huawei ’286 Accused Products”).

140. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei ’286 Accused Products (“a Huawei ’286 Accused Product Network”).

141. On information and belief, a Huawei '286 Accused Product Network implements at least Huawei's Cloud Fabric and/or the TRILL protocol.

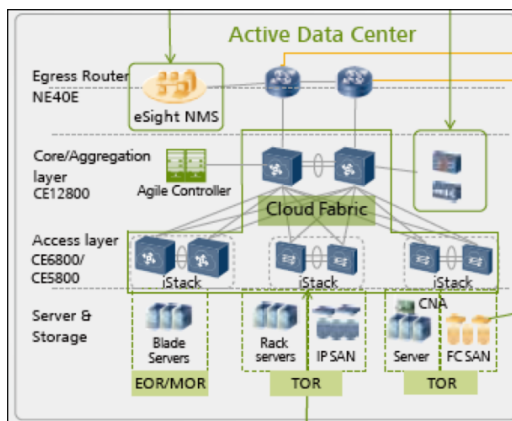


Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.



Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

142. On information and belief, a Huawei '286 Accused Product Network comprises a communication network.

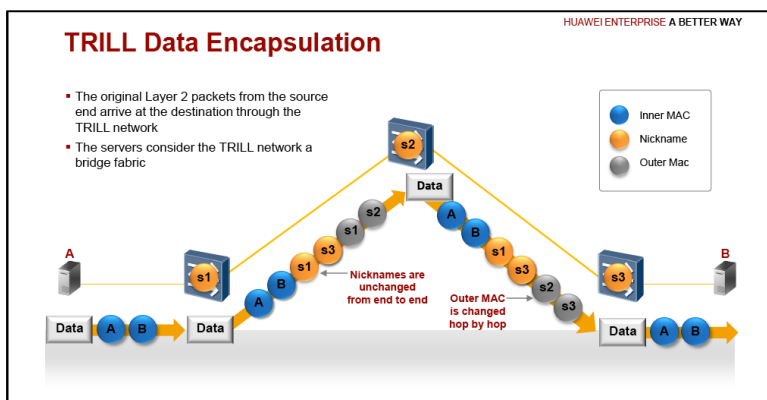


Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 4.

143. On information and belief, a Huawei '286 Accused Product Network comprises an entry end switch.

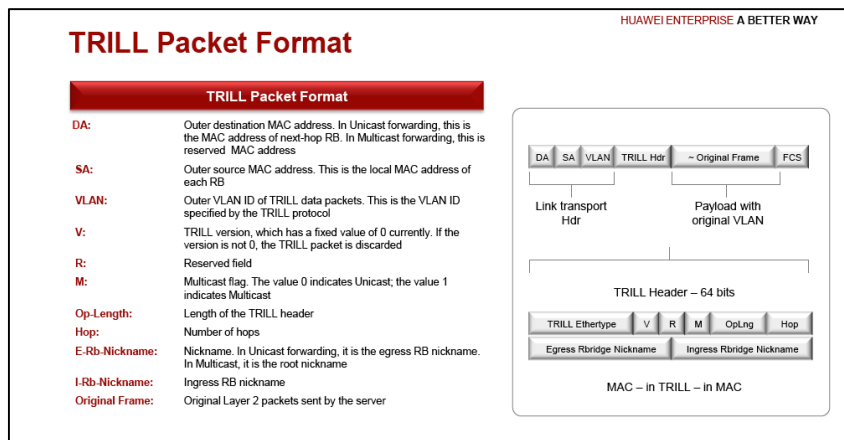
144. On information and belief, a Huawei '286 Accused Product Network comprises an exit end switch, which is selectably coupled to multiple termination devices including at least one exit termination device.

145. On information and belief, a Huawei '286 Accused Product Network comprises multiple intermediate switches coupled between the entry end switch and the exit end switch. For example, the figure below shows an entry end switch (i.e., ingress RBridge s1), an exit end switch (i.e., egress RBridge s3), and an intermediate switch (i.e., transit RBridge s2) in between them. A Cloud Fabric network can include multiple transit RBridges and multiple hosts (e.g., B) connected to an egress RBridge.



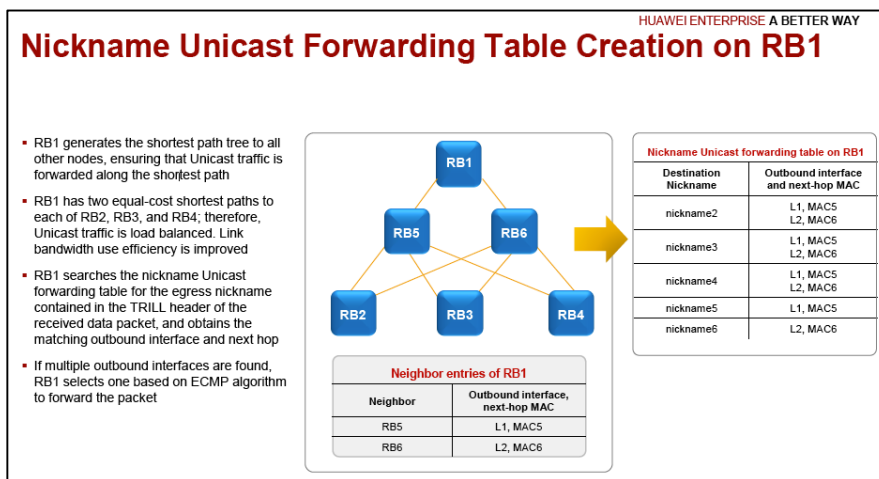
TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 7.

146. On information and belief, an entry end switch in a Huawei '286 Accused Product Network compiles a packet that contains a destination address of the exit end switch. For example, an entry end switch (i.e., ingress RBridge) encapsulates an incoming data packet within a TRILL Header and a Link Transport Header. The TRILL Header includes an “Egress RBridge Nickname” field, which contains the unique RBridge Nickname of the exit end switch (i.e., egress RBridge).



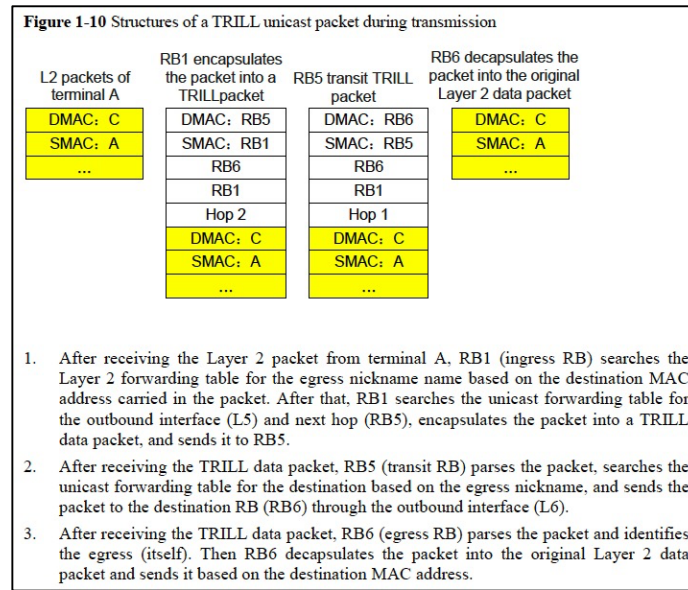
TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 6.

147. On information and belief, in a Huawei '286 Accused Product Network, the packet is forwarded through the plurality of intermediate switches with each intermediate switch having an identification number which points the packet to a successive one of the plurality of intermediate switches and finally to the exit end switch which performs the entirety of all translation needed by the communication network to route the packet from the exit end switch to the exit termination device. For example, each intermediate switch (i.e., transit RBridge) uses the Egress RBridge Nickname within the TRILL Header to point the packet to the next RBridge.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 18.

148. In addition, on information and belief, the exit end switch (i.e., egress RBridge) performs the entirety of all translation needed by the Cloud Fabric network to route the packet from the egress RBridge to the exit termination device (i.e., the packet's final destination).



Technology White Paper – TRILL, HUAWEI TECHNICAL DOCUMENTATION (Mar. 31, 2013), at 1-18.

149. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '286 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '286 patent, including at least claim 6, pursuant to 35 U.S.C. § 271(a).

150. On information and belief, Huawei also indirectly infringes the '286 patent by actively inducing infringement under 35 U.S.C. § 271(b).

151. On information and belief, Huawei has had knowledge of the '286 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '286 patent and knew of its infringement, including by way of this lawsuit.

152. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '286 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '286 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement,

with the knowledge of the '286 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '286 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '286 patent, including at least claim 6, and Huawei further provides documentation and training materials that cause customers of the Huawei '286 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '286 patent. By providing instruction and training to customers on how to use the Huawei '286 Accused Products, Huawei specifically intended to induce infringement of the '286 patent, including at least claim 6. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '286 Accused Products and to actively induce its customers to infringe the '286 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '286 patent, knowing that such use constitutes infringement of the '286 patent.

153. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '286 patent.

154. As a result of Huawei's infringement of the '286 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,778,259

155. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

156. U.S. Patent No. 7,778,259 ("the '259 patent"), entitled "Network Packet Transmission Mechanism," was filed on June 11, 2004. Dunti is the owner by assignment of the '259 patent. A true and correct copy of the '259 patent is attached hereto as Exhibit E.

157. The '259 patent has been cited by ten United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '259 patent as relevant prior art:

- International Business Machines Corporation;
- Toshiba Corporation;
- Nicira, Inc.; and
- The University of Zurich.

158. The '259 patent teaches, for example, a communication network that efficiently transfers data packets by using an independent numbering mechanism with distinct identification addresses, referred to as transport IDs, for transporting packets across a network. This solution eliminates complex lookup operations at intermediate modules, resulting in faster transmission across the network.

159. Each packet in the network of the '259 patent is embedded with unique destination transport ID information when the packet enters the network and carries this routing information along with the data. This transport ID-based packet transmission mechanism utilizes the logical structure in the network, which enables simple distributed packet direction operations as the packet traverses the network.

160. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

161. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, "the Huawei CE Switches").

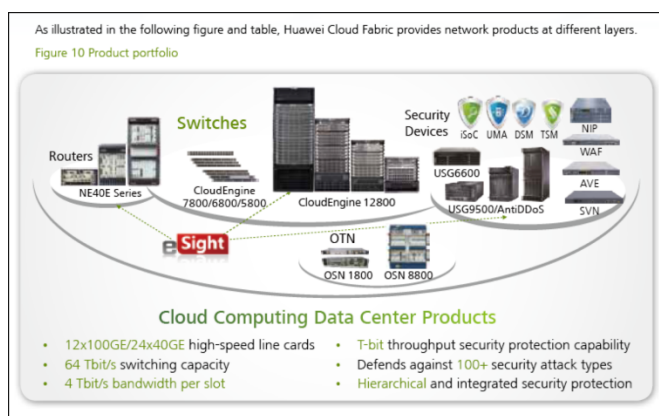
162. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Agile Controller.

163. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Next-Generation Network Operating System Versatile Routing Platform (VRP8), which runs on the Huawei CE Switches.

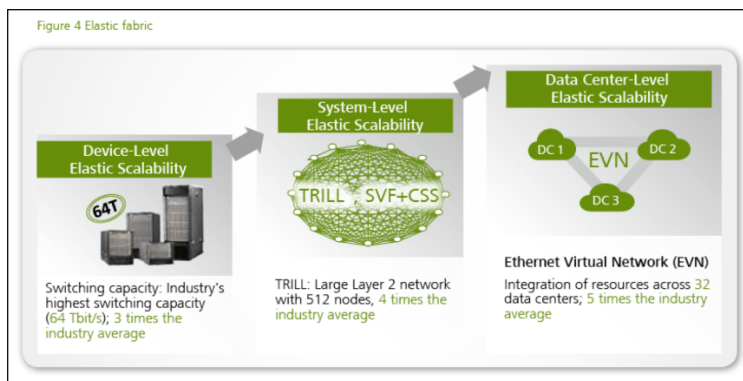
164. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CE Switches, the Huawei Agile Controller, and the Huawei VRP8 Network Operating System (collectively, “the Huawei ’259 Accused Products”).

165. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei ’259 Accused Products (“a Huawei ’259 Accused Product Network”).

166. On information and belief, a Huawei ’259 Accused Product Network implements at least Huawei’s Cloud Fabric and/or the TRILL protocol.

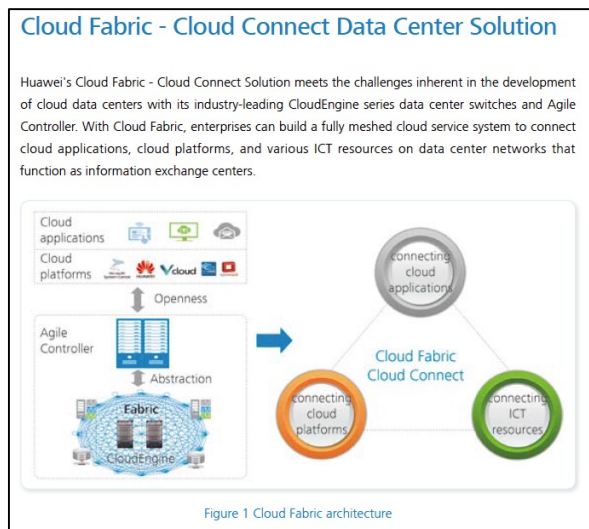


Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 9.



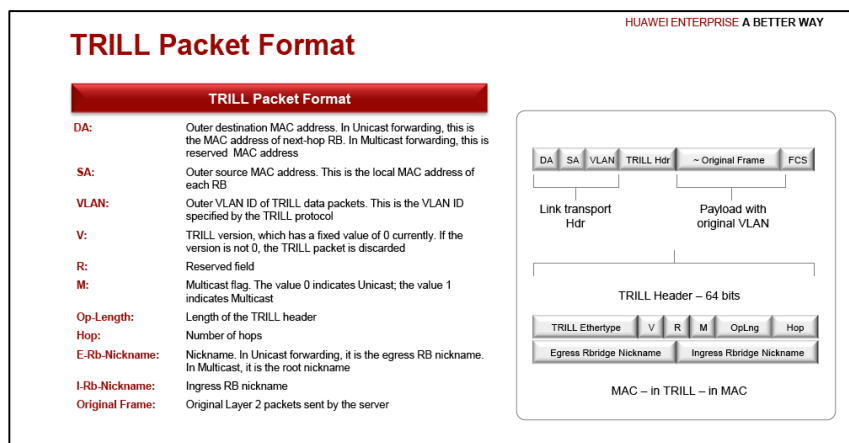
Huawei Cloud Fabric Data Center Solutions, HUAWEI SOLUTION BROCHURE (2014), at 5.

167. On information and belief, the Huawei ’259 Accused Products perform a method of transporting packets across a network.

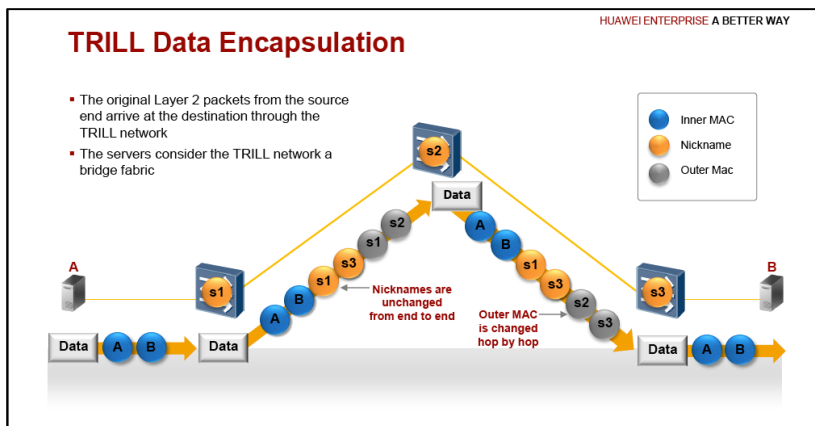


Data Sheet, *Huawei Cloud Fabric-Cloud Connect Data Center Solution*, HUAWEI TECHNICAL DOCUMENTATION (2014), at 3.

168. On information and belief, the Huawei '259 Accused Products embed a destination transport identification to a data packet when the data packet enters the network. For example, data packets entering a Cloud Fabric network are encapsulated within a TRILL Header and Link Transport Header, which include, for example, a “Egress RBridge Nickname” field that contains the RBridge Nickname of the exit end switch.

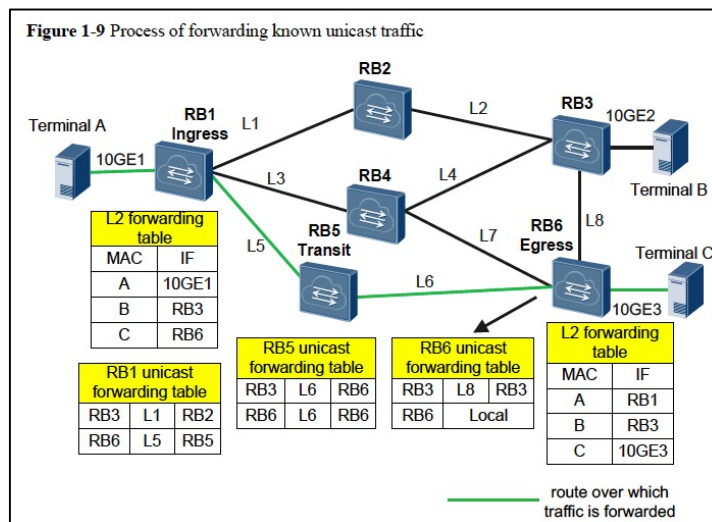


TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 6.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 7.

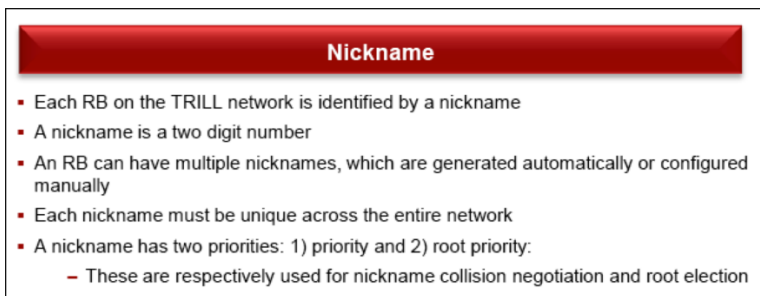
169. On information and belief, the Huawei '259 Accused Products connect a plurality of routing switches within a network with the routing switches grouped into two or more groups within the network based on network topology. For example, in a Cloud Fabric network, the Huawei '259 Accused Products are grouped into ingress R Bridges, transit R Bridges, and egress R Bridges based on whether they are entry switches, intermediate switches, or exit switches.



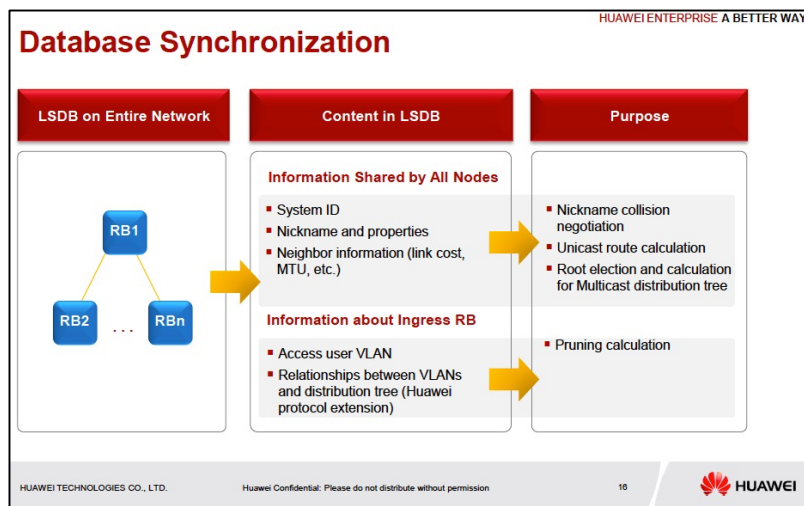
Technology White Paper – TRILL, HUAWEI TECHNICAL DOCUMENTATION (Mar. 31, 2013), at 1-17.

170. On information and belief, the Huawei '259 Accused Products assign a unique transport identification number to each routing switch indicative, at least in part, of the network topology. For example, each R Bridge includes a unique R Bridge Nickname, which includes a

nickname priority value and a root priority value that are used in determining the topology of distribution trees within a Cloud Fabric network and are indicative, at least in part, of the network topology. In addition, the RBridge Nickname is part of a network topology database and adjacency tables that are built and maintained by the IS-IS protocol and, when used with the topology database and/or adjacency tables, indicates, at least in part, the network topology.



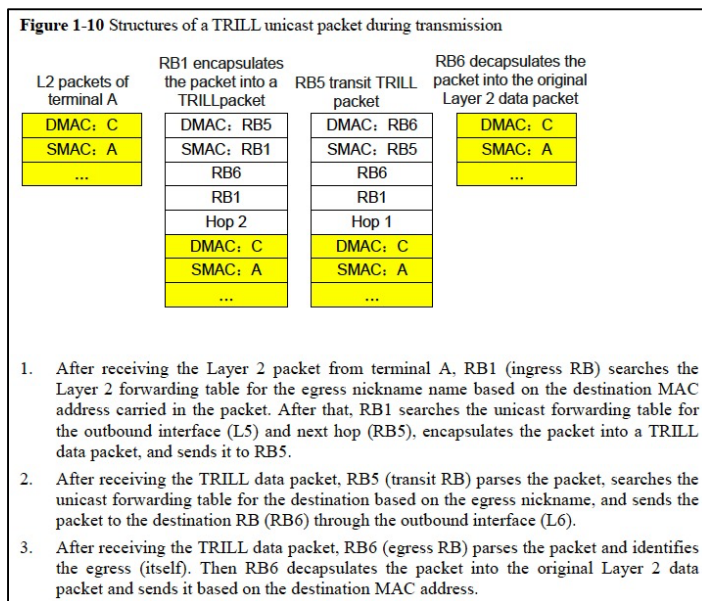
TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 8.



TRILL for Data Center Networks, HUAWEI ENTERPRISE PRESENTATION, at 7.

171. On information and belief, the Huawei '259 Accused Products compare the destination transport identification of a packet with the transport identification of a routing switch. For example, data packets entering a Cloud Fabric network are encapsulated within a TRILL Header, which includes the “Egress RBridge Nickname” field that contains the RBridge Nickname of the egress RBridge. Switches running Huawei’s Cloud Fabric technology, such as

the Huawei '259 Accused Products, compare the value in the Egress RBridge Nickname field to values in the switches' memory.



Technology White Paper – TRILL, HUAWEI TECHNICAL DOCUMENTATION (Mar. 31, 2013), at 1-18.

172. On information and belief, the Huawei '259 Accused Products forward data packets through a network based on the comparison of destination transport identification. For example, switches running Huawei's Cloud Fabric technology, such as the Huawei '259 Accused Products, forward encapsulated data packets using the Egress RBridge Nickname.

173. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '259 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '259 patent, including at least claim 9, pursuant to 35 U.S.C. § 271(a).

174. On information and belief, Huawei also indirectly infringes the '259 patent by actively inducing infringement under 35 U.S.C. § 271(b).

175. On information and belief, Huawei has had knowledge of the '259 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '259 patent and knew of its infringement, including by way of this lawsuit.

176. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '259 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '259 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '259 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '259 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '259 patent, including at least claim 9, and Huawei further provides documentation and training materials that cause customers of the Huawei '259 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '259 patent. By providing instruction and training to customers on how to use the Huawei '259 Accused Products, Huawei specifically intended to induce infringement of the '259 patent, including at least claim 9. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '259 Accused Products and to actively induce its customers to infringe the '259 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '259 patent, knowing that such use constitutes infringement of the '259 patent.

177. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '259 patent.

178. As a result of Huawei's infringement of the '259 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 6,912,196

179. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

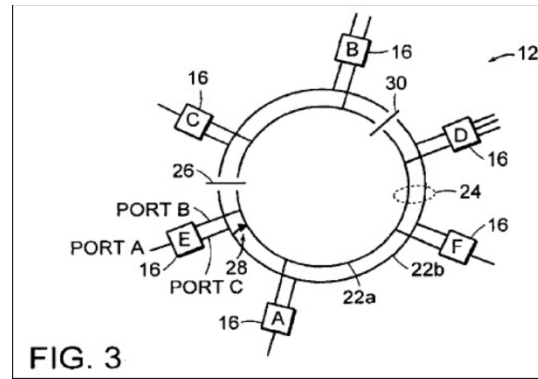
180. U.S. Patent No. 6,912,196 (“the ’196 patent”), entitled “Communication Network and Protocol Which Can Efficiently Maintain Transmission Across a Disrupted Network,” was filed on May 15, 2000. Dunti is the owner by assignment of the ’196 patent. A true and correct copy of the ’196 patent is attached hereto as Exhibit F. The ’196 patent claims a specific packet architecture, communication system, and method for determining the location at which a network is disrupted, disabled, and/or severed.

181. The ’196 patent has been cited by thirty-seven United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ’196 patent as relevant prior art:

- Alcatel Lucent S.A.;
- Fujitsu, Ltd.;
- Google, Inc.;
- International Business Machines Corporation;
- Samsung Electronics Co., Ltd.;
- Terascale Supercomputing, Inc.;
- Siemens AG; and
- NEC Corporation.

182. The ’196 patent teaches, for example, an improved packet protocol and communication system that can determine where within a network a transmission error exists.

183. Figure 3 of the ’196 patent, shown below, depicts a ring topology with multiple modules labeled “A” through “F” that communicate over two transmission channels that form a single transmission path. One channel is used for counter-clockwise data transmission, while the other channel is used for clockwise data transmission.



'196 Patent, Fig. 3.

184. Figure 3 shows an example where the transmission path has been severed between modules C and E. In an attempted transmission from module A to module C (clockwise through module E), module E will detect the severance and notify the other modules by employing a loop-back path of the packet sent from module A back to module A. When module E detects the downstream severance, it sends control bits to the originating module A indicating the downstream error. Since receiving module E was the last module in the path before the severance, module E sends both control bits and error identification bits. The control bits are set to indicate a disruption immediately downstream of receiving module E. The error identification bits identify the receiving module E by the identification number assigned to that module.

185. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to network communications.

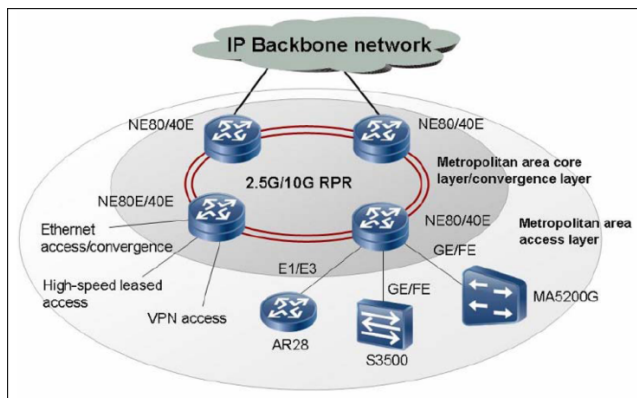
186. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Enhanced OSN Series MSTP Product Series, including but not limited to the Huawei OptiX OSN 1500, Huawei OptiX OSN 2500, Huawei OptiX OSN 3500, Huawei OptiX OSN 7500 (collectively, “the Huawei OptiX Products”). *See* Huawei MSTP Product Series Product Brochure (2013).

187. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei OptiX Products (collectively, “the Huawei '196 Accused Products”).

188. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei '196 Accused Products (“a Huawei '196 Accused Product Network”).

189. On information and belief, a Huawei '196 Accused Product Network implements at least the IEEE 802.17 Resilient Packet Ring (“RPR”) protocol.

190. On information and belief, a Huawei '196 Accused Product Network comprises a communication system.

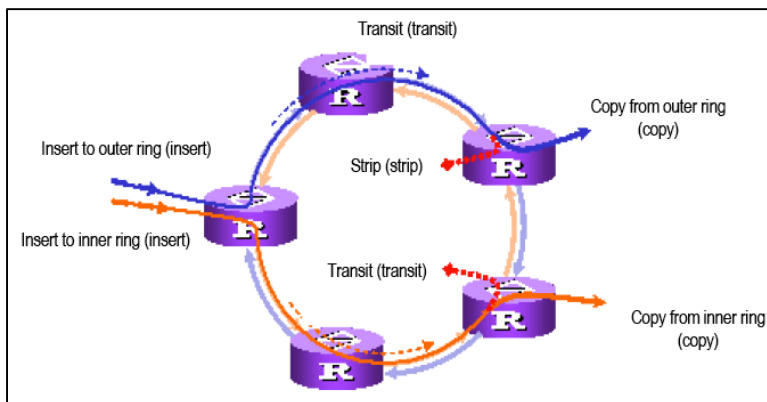


Technical White Paper for Resilient Packet Ring (RPR), HUAWEI TECHNICAL DOCUMENTATION (2007), at 16.

Integrating the intelligent features of IP network, economical feature of Ethernet, and high bandwidth utilization and availability of optical fiber ring network, RPR (Resilient Packet Ring) is an ideal networking solution for IP MAN. RPR makes it possible for a carrier to provide carrier-class services in a MAN at a low cost, offering network reliability of SDH level but at a much lower transmission cost. RPR is different from traditional MAC with its most appealing feature of carrier-class reliability. This feature allows it to address data-oriented service transmission requirements and to form an integrated transmission solution capable of multi-service processing.

Technical White Paper for Resilient Packet Ring (RPR), HUAWEI TECHNICAL DOCUMENTATION (2007), at 1.

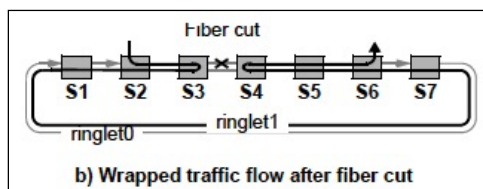
191. On information and belief, a Huawei '196 Accused Product Network comprises at least two transmission channels. For example, an RPR ring is made up of dual counter-rotating rings that are used to transmit data, as shown below.



Technical White Paper for Resilient Packet Ring (RPR), HUAWEI TECHNICAL DOCUMENTATION (2007), at 4.

192. On information and belief, a Huawei '196 Accused Product Network comprises a receiving module connected to the transmission channels, which can be seen, for example, in the figure shown directly above.

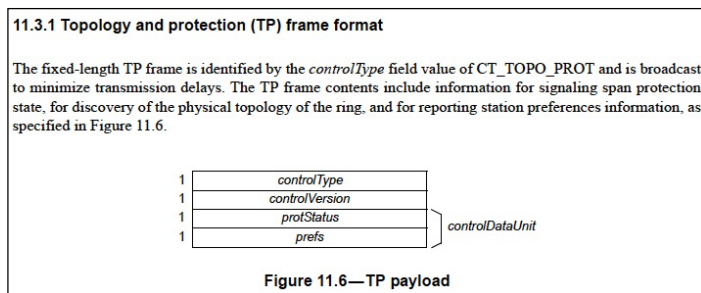
193. On information and belief, a receiving module in a Huawei '196 Accused Product Network includes a loop-back conductor that connects the two transmission channels. For example, each receiving module can receive packets on either the west or the east interface and can transmit packets out of either the west or the east interface, such that a packet received on the east interface can be looped back and sent out on the east interface. RPR networks use wrapping protection to avoid disrupted links.



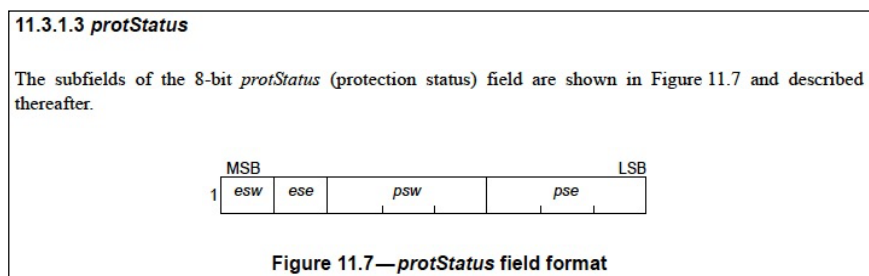
IEEE Std 802.17-2011, *Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications*, IEEE STANDARDS ASSOCIATION (Sept. 20, 2011), at 279.

194. On information and belief, a receiving module in a Huawei '196 Accused Product Network returns a packet containing error bits if one or more of the transmission channels downstream of the receiving module is disturbed. For example, when a span is determined to be an edge (i.e., the transmission channel downstream of the module is disturbed), topology and

protection (“TP”) frames, which are control frames, are sent to report the edge. The payload of a TP frame includes two fields that indicate whether an edge is present on either the west span or the east span of a station.



IEEE Std 802.17-2011, *Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications*, IEEE STANDARDS ASSOCIATION (Sept. 20, 2011), at 292.

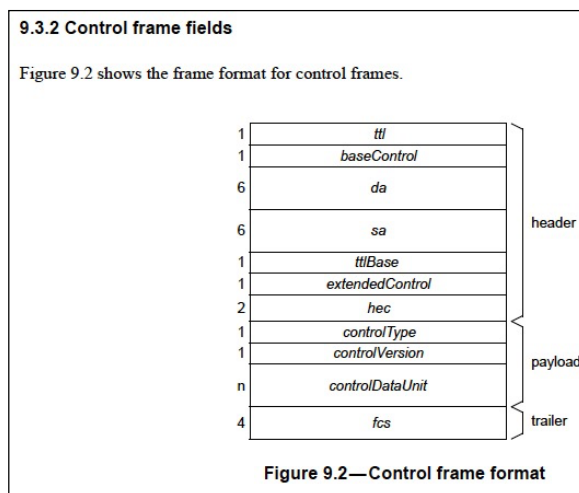


11.3.1.3.1 *esw*: A (edge state, west) bit that indicates whether an edge is present on the west span of a station. A value of 0 indicates that there is no edge, whereas a value of 1 indicates that an edge is present.

11.3.1.3.2 *ese*: A (edge state, east) bit that indicates whether an edge is present on the east span of a station. A value of 0 indicates that there is no edge, whereas a value of 1 indicates that an edge is present.

IEEE Std 802.17-2011, *Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications*, IEEE STANDARDS ASSOCIATION (Sept. 20, 2011), at 292-93.

195. On information and belief, the error bits sent by a receiving module in a Huawei ’196 Accused Product Network comprise a unique identification number assigned to the receiving module to note the receiving module was the last of a plurality of modules that received the packet destined for a destination module dissimilar from and located downstream of the receiving module. For example, a control frame in an RPR network includes the source address of the originating module, which is a unique identifier that identifies the module sending the error bits indicating that an edge is present at the module.



IEEE Std 802.17-2011, *Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications*, IEEE STANDARDS ASSOCIATION (Sept. 20, 2011), at 206.

196. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '196 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '196 patent, including at least claim 10, pursuant to 35 U.S.C. § 271(a).

197. On information and belief, Huawei also indirectly infringes the '196 patent by actively inducing infringement under 35 U.S.C. § 271(b).

198. On information and belief, Huawei has had knowledge of the '196 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '196 patent and knew of its infringement, including by way of this lawsuit.

199. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '196 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '196 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '196 patent and with the knowledge that the induced acts would

constitute infringement. For example, Huawei provides the Huawei '196 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '196 patent, including at least claim 10, and Huawei further provides documentation and training materials that cause customers of the Huawei '196 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '196 patent. By providing instruction and training to customers on how to use the Huawei '196 Accused Products, Huawei specifically intended to induce infringement of the '196 patent, including at least claim 10. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '196 Accused Products and to actively induce its customers to infringe the '196 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '196 patent, knowing that such use constitutes infringement of the '196 patent.

200. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '196 patent.

201. As a result of Huawei's infringement of the '196 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty for the use made of the invention by Huawei together with interest and costs as fixed by the Court.

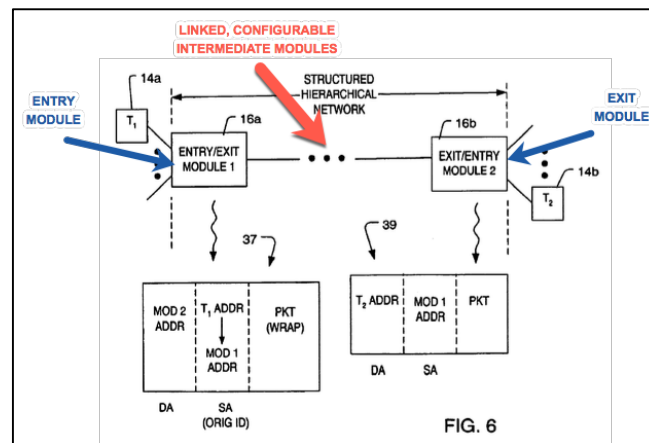
COUNT VII
INFRINGEMENT OF U.S. PATENT NO. 6,754,214

202. Dunti restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

203. U.S. Patent No. 6,754,214 ("the '214 patent"), entitled "Communication Network Having Packetized Security Codes and a System for Detecting Security Breach Locations Within the Network," was filed on July 19, 1999. Dunti is the owner by assignment of the '214 patent. A true and correct copy of the '214 patent is attached hereto as Exhibit G.

204. The '214 patent discloses and claims a specific architecture and system for securing and prioritizing packets of data sent through a communication network. By assigning security and priority codes to packets as they enter the network through a specially configured entry module, maximum bandwidth allocation can be achieved among linked, configurable entry, exit, and intermediate modules in a hierarchical, packet-switched environment. Advantageously over prior art networks and conventional solutions, the communication network claimed in the '214 patent dynamically ensures dynamic data path security, QoS-related packet forwarding priority in the presence of congestion at a shared network resource, and modular configurability. As described in the foregoing and in the paragraphs below, the '214 patent claims a technical solution to a problem unique to computer networks.

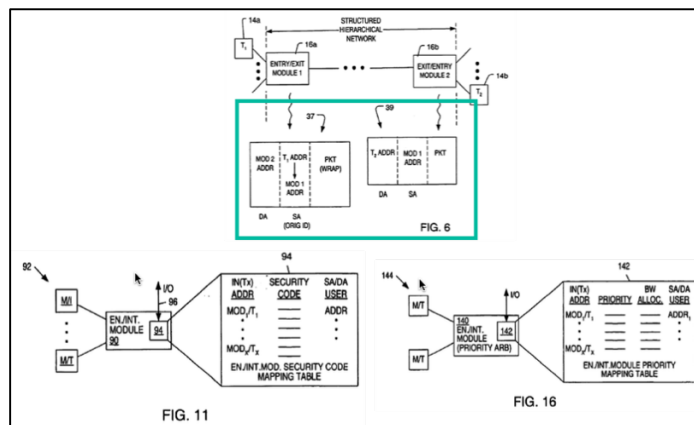
205. In the communication network of the '214 patent, distinct entry and exit modules are coupled in a structured, hierarchical network by linked, configurable intermediate modules, as shown below in Figure 6 from the '214 patent. Modules 16a and 16b are the distinct entry and exit modules of the claimed communication network, while the intermediate ellipses represent the configurable nature of linked intermediate modules.



'214 Patent, Fig. 6 (blue and red illustrations added).

206. The entry module of the communication network claimed in the '214 patent is coupled to assign and transfer a security code and an identification number to a packet of data. The exit module (through an included exit compare unit) is coupled to compare this security

code and identification number before transferring the packet from the claimed communication network. As shown below, the green-boxed portion of Fig. 6 of the '214 patent, as well as Figs. 11 and 16 of the '214 patent, illustrate exemplary security code and identification number labels assigned, used, and compared by the configurable modules (including distinct entry and exit modules) of the communication network claimed in the '214 patent.



'214 Patent, Figs. 6, 11, and 16 (green illustration added).

207. Advantageously, the entry module claimed in the '214 patent comprises a decoder, a specially-configured storage device, and a coupled entry compare unit configured to evaluate and route entering packets according to (among other things) the aforementioned security code and identification number.

208. A packet traversing the communication network claimed in the '214 patent can be transferred as a “secured packet”—a concrete and specific technical concept within the '214 patent claims. A claimed “secured packet” is concretely structured with at least (1) the aforementioned security code and identification number; (2) a first grouping of trailer bits reserved for a count of traversed intermediate modules; and (3) a second grouping of trailer bits reserved for an identifier of traversed intermediate modules.

209. The '214 patent has been cited by at least one hundred and four United States patents and patent applications as relevant prior art. For example, patents issued to the following companies have cited the '214 patent as relevant prior art.

- Bank of America Corporation;
- Hitachi, Ltd.;
- Nokia Corporation;
- IBM Corporation;
- Ntt Docomo, Inc.;
- Cisco Technology, Inc.
- EMC Corporation;
- AT&T Mobility II, LLC; and
- AT&T Intellectual Property I, L.P.

210. Huawei makes, uses, sells, and/or offers for sale in the United States products and/or services relating to secure, prioritized network communications.

211. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei Enterprise S Series Switch Products, including but not limited to the Huawei Enterprise Sx700 Series Switch Products (e.g., S12700 Series Agile Switches, S9700 Series Terabit Routing Switches, S7700 Series Smart Routing Switches, S6700 Series 10G Switches, S5700 Series Gigabit Enterprise Switches, S3700 Series Enterprise Switches, S2700 Series Enterprise Switches, and S1700 Series Enterprise Switches)⁴ (collectively, “the Huawei S Switches”).

212. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei CloudEngine Series data center switches, including but not limited to Model Nos. CE5800, CE6800, CE7800, and CE12800 (collectively, “the Huawei CE Switches”).

213. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei USG6000v series Virtual Service Gateway product and platform (“the Huawei VSG Products”).

214. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei FusionSphere Cloud OS and the Huawei Versatile Routing Platform (“VRP”) software.

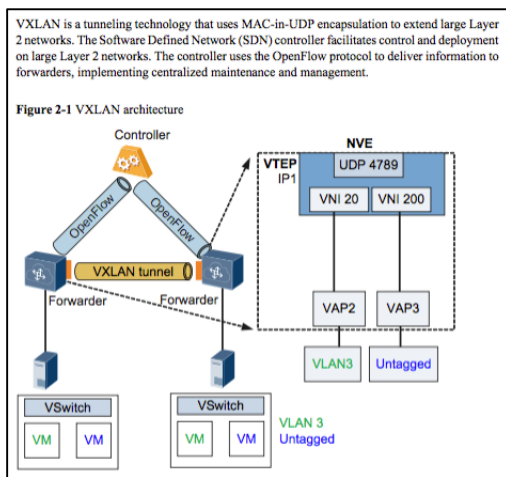
215. Huawei makes, uses, sells, offers to sell, and/or imports the Huawei S Switches, the Huawei CE Switches, the Huawei VSG Products, the Huawei FusionSphere Cloud OS, and the Huawei VRP software (collectively, “the Huawei ’214 Accused Products”).

⁴ See generally, e.g., *Huawei Enterprise Sx700 Series Switch Product Quick Reference Guide*, HUAWEI TECHNICAL DOCUMENTATION (2013), at 3-121.

216. Huawei makes, uses, sells, and/or offers to sell networks comprised of the Huawei '214 Accused Products (a "Huawei '214 Accused Product Network").

217. On information and belief, a Huawei '214 Accused Product Network implements at least Huawei CloudEngine Virtual Extensible LAN (VXLAN) technology—for example, using the Huawei CE Switches running Huawei FusionSphere and VRP software to perform VXLAN bridging and gateway functions.

218. On information and belief, Huawei CloudEngine VXLAN is an overlay technology for network virtualization. It provides Layer-2 extension over a shared Layer-3 underlay infrastructure network by using MAC address in IP User Datagram Protocol (MAC in IP/UDP) tunneling encapsulation. The purpose of obtaining Layer-2 extension in the overlay network is to overcome the limitations of physical server racks and geographical location boundaries and achieve flexibility for workload placement within a data center or between different data centers.



CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 5.

219. On information and belief, Huawei CloudEngine VXLAN technology differs from both conventional communication network technology and from VLAN network segmentation technology, standardized under the IEEE 802.1Q group. For example, traditional VLAN network segmentation under IEEE 802.1Q provides logical segmentation of Layer 2

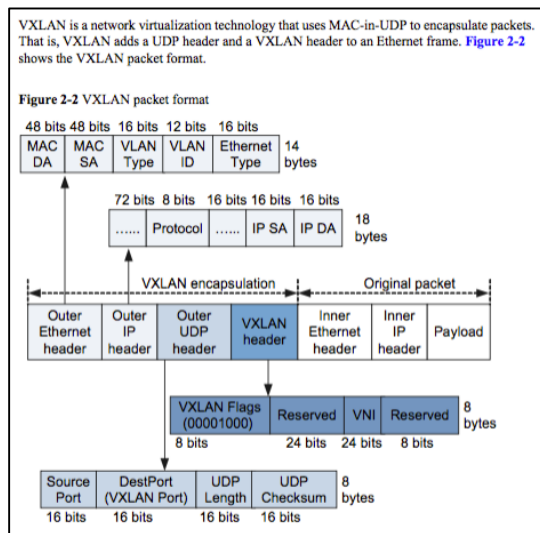
boundaries or broadcast domains. Due to the inefficient use of available network links with VLAN use, rigid requirements on device placements in the data center network, and the limited scalability of VLAN technology, in recent years VLAN technology (itself an improvement over “traditional” communication networks) has become a limiting factor to IT departments and cloud providers as they build large multitenant data centers.

VXLAN addresses the above problems on large Layer 2 networks as follows:

- VM scale limitations imposed by network performance**
 VXLAN encapsulates data packets sent from VMs into UDP packets and encapsulates IP and MAC addresses used on the physical network into outer headers. The network is only aware of the encapsulated parameters. This greatly reduces the number of MAC address entries required on large Layer 2 networks.
- Limited network isolation capabilities**
 VXLAN uses a VXLAN network identifier (VNI) field similar to the VLAN ID field defined in IEEE 802.1Q. The VNI field has 24 bits and can identify a maximum of 16M $[(2^{24}-1)/1024^2]$ VXLAN segments.
- VM migration scope limitations imposed by network architecture**
 When VXLAN is used to construct a large Layer 2 network, VM IP and MAC addresses can remain unchanged after VM migration.

CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 3.

220. On information and belief, the Huawei CloudEngine VXLAN defines a structured, hierarchical MAC-in-UDP encapsulation scheme where the original Layer 2 frame has a VXLAN header added and is then placed in a UDP-IP packet. With the MAC-in-UDP encapsulation, Huawei CloudEngine VXLAN tunnels Layer 2 network over Layer 3 network.



CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 7.

221. The structured, hierarchical MAC-in-UDP encapsulated packet structure and Layer 2-over-Layer 3 network tunneling technology defined and used in Huawei CloudEngine VXLAN enables secure, prioritized packet forwarding over dynamic, configurable networks through Huawei's integration of technologies such as MPLS-IP VPN and Huawei Versatile Routing Platform (VRP) into the base VXLAN network architecture. On information and belief, a Huawei '214 Accused Product Network with Huawei CloudEngine VXLAN implements each of the aforementioned technologies, including Huawei's VRP-based MPLS VPN ("VRP-MPLS VPN").

222. On information and belief, a Huawei '214 Accused Product Network configured for Huawei CloudEngine VXLAN and Huawei VRP-MPLS supports secure, prioritized packet forwarding through VRP-MPLS VPN. A VRP-MPLS VPN consists of a set of sites that are interconnected by means of a Huawei VRP-MPLS provider core network.

223. On information and belief, a VPN delivers private network services over a public infrastructure, allowing a set of sites to communicate with each other privately over the Internet or other public networks. In contrast to conventional VPNs, MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without the customer's involvement.

224. On information and belief, a Huawei '214 Accused Product Network comprises a communication network. For example, a Huawei '214 Accused Product Network comprises a packetized communication network that securely routes packets in a dynamic, configurable, QoS-aware manner using specially configured, Huawei VRP-aware VXLAN MPLS-VPN entry, exit, and intermediate forwarding modules.

225. On information and belief, a Huawei '214 Accused Product Network comprises an entry module; an exit module; and at least one intermediate module.

1.3 Configuring Tunnel Interfaces

Tunnel interfaces are point-to-point virtual interfaces that are used for encapsulating packets. Similar to loopback interfaces, tunnel interfaces are logical interfaces.

Applicable Environment

Tunnels such as MPLS TE tunnels, and IPv6 over IPv4 tunnels all use virtual interfaces, namely, tunnel interfaces, to forward packets. Before setting up these types of tunnels, you need to create tunnel interfaces.

Tunnel interfaces can be configured with different encapsulation modes as required, for example, mpls te, and ipv6-ipv4.

Huawei NetEngine5000E Core Router Configuration Guide - VPN, HUAWEI TECHNICAL DOCUMENTATION (Oct. 15, 2011), at 2.

Table 2-1 Controller-related concepts

Concept	Description
Controller	A controller is an OpenFlow server running on the control plane. An independent controller performs all path calculation and management operations. In general, a blade server can function as the controller.
Forwarder	A forwarder is an OpenFlow device running on the forwarding plane dedicated to data forwarding only.

CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 5.

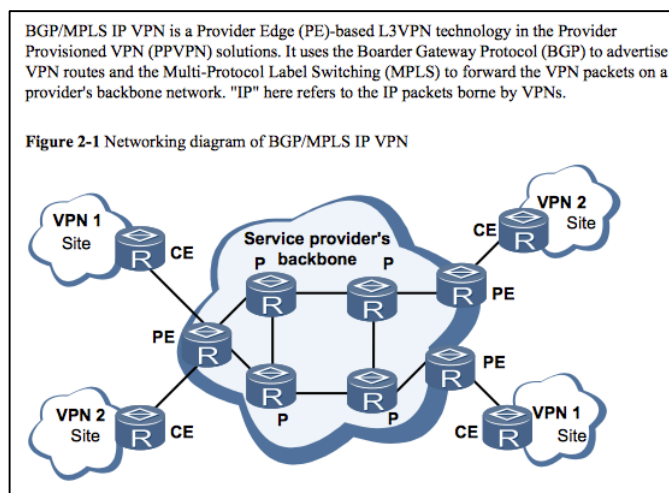
226. On information and belief, a Huawei '214 Accused Product Network entry module is coupled to assign and transfer a security code and an identification number to a packet of data. For example, the entry VXLAN/MPLS-VPN virtual tunnel interface Huawei CE Switch is configured to assign VXLAN/MPLS VPN security (e.g., VPN identifier) and priority (e.g., QoS/TE) labels to the MAC-in-UDP encapsulated header that the entry virtual tunnel interface assigns to a data packet entering the Huawei '214 Accused Product Network.

BGP/MPLS IP VPN features flexible networking modes, excellent extensibility and convenient support for Quality of Service (QoS) and MPLS Traffic Engineering (MPLS TE) features. It is now widely used.

In BGP/MPLS IP VPN, three types of devices are involved:

- Customer Edge (CE): It is an edge device on the user network. A CE is directly connected to a Service Provider (SP) network. CEs can be routers, switches, or hosts. Usually, CEs cannot sense the existence of VPNs and need not support MPLS.
- Provider Edge (PE): It is an edge device on an SP network. A PE is directly connected to a CE. On the MPLS network, PEs are responsible for processing all VPN services.
- Provider (P): is a backbone device on the SP network. A P is not directly connected to a CE. Ps only need to possess basic MPLS forwarding capabilities and do not need to maintain information about VPNs.

Huawei NetEngine5000E Core Router Configuration Guide - VPN, HUAWEI TECHNICAL DOCUMENTATION (Oct. 15, 2011), at 2-3.



Huawei NetEngine5000E Core Router Configuration Guide - VPN, HUAWEI TECHNICAL DOCUMENTATION (Oct. 15, 2011), at 28.

227. On information and belief, the '214 Accused Product Network entry module (e.g., in the entry VXLAN/MPLS-VPN virtual tunnel interface Huawei CE Switch) comprises a decoder (e.g., a VXLAN/MPLS-VPN-aware Huawei CloudEngine/VRF hardware and/or software decoder coupled to an entry port) and a storage device configured with a set of bits (e.g., a Huawei CloudEngine hardware, virtual appliance, and/or software configuration register storing base and/or context-specific Huawei VXLAN/MPLS-VPN settings and identifiers for the entry VXLAN/MPLS-VPN virtual tunnel interface Huawei CloudEngine Series Enterprise Switch).

228. On information and belief, an entry compare unit (e.g., a VTEP/MPLS-VPN virtual tunnel interface gateway subsystem) is coupled between the decoder and storage device within the Huawei '214 Accused Product Network entry module in order to facilitate targeted traffic inspection and lookup/testing of packets received at the entry module (e.g., inspection and/or logging of VPN/QoS-related MAC-in-UDP header fields of received packets and lookup/comparison/testing against known/stored values via, for example, logical testing of received/detected bit strings in identifiable MAC-in-UDP header subfield against an array of known/stored bit strings), thereby allowing for reliable, extensible traffic

classification/shaping/engineering on the basis of security and priority labels/identifiers within the Huawei '214 Accused Product Network.

On the network as shown in [Figure 2-9](#), VXLAN QoS implements mapping between QoS priorities in original packets, internal priorities, and priorities of encapsulated packets according to the following process:

1. An original packet arrives at a Layer 2 sub-interface on Switch_1. Switch_1 maps the 802.1p priority of the original packet to the internal priority (PHB and color) based on the DiffServ profile bound to the specified VLAN on the sub-interface, and then sends the packet to the specified queue.
2. Before the packet enters the VXLAN tunnel from Switch_1, Switch_1 encapsulates the packet with a VXLAN header, UDP header, IP header, and Ethernet header in turn, and then maps the packet's internal priority to the 802.1p priority or DSCP priority based on the default profile in the DiffServ domain. The packet is then transmitted over the VXLAN tunnel based on the 802.1p priority or DSCP priority.
3. When the packet leaves the tunnel, its 802.1p priority or DSCP priority (depending on which priority is trusted on the tunnel interface) is mapped to the internal priority based on the default profile in the DiffServ domain. The packet then enters the queue matching the internal priority. An Ethernet interface working in Layer 3 mode only trusts the DSCP priority.

CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 19-20.

229. On information and belief, secure traffic management and packet tunneling in the Huawei '214 Accused Product Network is achieved through (among other things) packet classification on the basis of security.

Common VPN Tunnels

The common VPN tunnels are as follows:

- LSP
Label Switched Paths (LSPs) are used as tunnels for VPN data forwarding over the Multi-Protocol Label Switch (MPLS) VPN public network. In this mode, only the PE rather than each device that a VPN packet passes needs to analyze IP packet headers. Thus, the time to process VPN packets shortens and the delay of packet transmission decreases. In addition, MPLS labels are supported any link-layer protocol. An LSP is similar to an Asynchronous Transfer Mode (ATM) virtual circuit (VC) or a Frame Relay (FR) VC in function and security.
- MPLS TE
Generally, carriers are required to provide VPN users with end-to-end Quality of Service (QoS) for various services, such as the voice service, video service, mission-critical service, and common online service. MPLS Traffic Engineering (TE) tunnels can optimize network resources and offer users QoS guaranteed services.

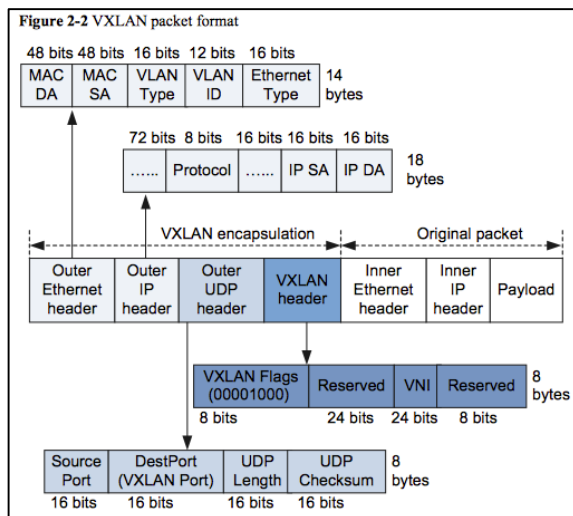
Tunnel Configuration Management

The setup and management of tunnels vary with the tunnel type. For example, MPLS TE tunnels (CR-LSP tunnels) are set up and managed through tunnel interfaces, whereas Label Distribution Protocol (LDP) LSPs tunnels are automatically set up as long as corresponding protocols are configured.

This section describes the configurations of tunnel interfaces and general tunnel management.

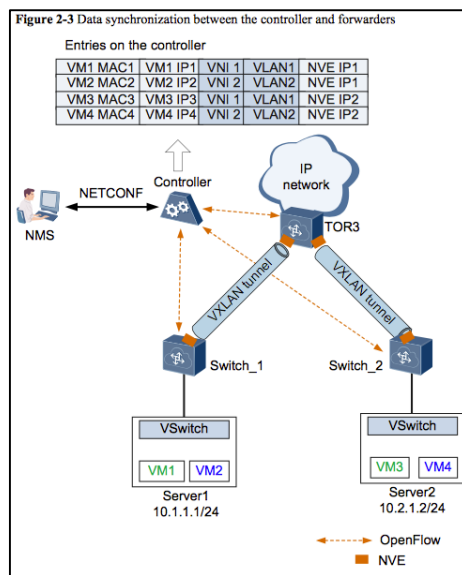
- Tunnel interface configuration: You can specify different tunnel types on different tunnel interfaces. Configurations of tunnels vary with the tunnel type.
- Tunnel management: This function notifies the tunnel status to applications that use the tunnel and provides tunnel query policies for tunnel selection. The commonly used function is to set tunnel policies.

Huawei NetEngine5000E Core Router Configuration Guide - VPN, HUAWEI TECHNICAL DOCUMENTATION (Oct. 15, 2011), at 2.

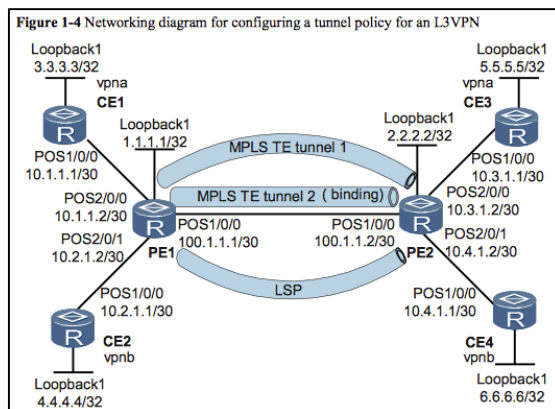


CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 7.

230. On information and belief, this classification uses at least the identification number and security code described in the foregoing paragraphs, as well as trailer bit groupings identifying a count number for intermediate modules traversed by a packet and an identification of traversed intermediate modules.



CloudEngine Series Switches VXLAN Technical White Paper, HUAWEI TECHNICAL DOCUMENTATION (Oct. 9, 2014), at 9.



Huawei NetEngine5000E Core Router Configuration Guide - VPN, HUAWEI TECHNICAL DOCUMENTATION (Oct. 15, 2011), at 14.

231. On information and belief, a Huawei '214 Accused Product Network exit module comprises an exit compare unit coupled to compare the security code and identification number before transferring the packet of data from the Huawei '214 Accused Product Network. For example, the Huawei CloudEngine Series Enterprise Switch configured as an exit VXLAN/MPLS-VPN virtual tunnel interface module for the '214 Accused Product Network is coupled to compare the aforementioned VXLAN/MPLS-VPN security and priority labels of the encapsulated MAC-in-UDP data packet (e.g., detected/sniffed values in defined subfields of the structured, hierarchical MAC-in-UDP VXLAN encapsulation header that are known/defined to correspond to security/priority in the Huawei VXLAN/MPLS-VPN network) with known/stored values before transferring the (now-decapsulated) packet from the exit VLAN/MPLS-VPN virtual tunnel interface device (e.g., configured Huawei CloudEngine Series Enterprise Switch) and out of the Huawei '214 Accused Product Network.

232. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Huawei '214 Accused Products, Huawei has injured Dunti and is liable to Dunti for directly infringing one or more claims of the '214 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

233. On information and belief, Huawei also indirectly infringes the '214 patent by actively inducing infringement under 35 U.S.C. § 271(b).

234. On information and belief, Huawei has had knowledge of the '214 patent since at least the date of service of this Complaint or shortly thereafter, and on information and belief, Huawei knew of the '214 patent and knew of its infringement, including by way of this lawsuit.

235. On information and belief, Huawei intended to induce patent infringement by third-party customers and users of the Huawei '214 Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Huawei specifically intended and was aware that the normal and customary use of the accused products would infringe the '214 patent. Huawei performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '214 patent and with the knowledge that the induced acts would constitute infringement. For example, Huawei provides the Huawei '214 Accused Products, which are capable of operating in a manner that infringes one or more claims of the '214 patent, including at least claim 1, and Huawei further provides documentation and training materials that cause customers of the Huawei '214 Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '214 patent. By providing instruction and training to customers on how to use the Huawei '214 Accused Products, Huawei specifically intended to induce infringement of the '214 patent, including at least claim 1. On information and belief, Huawei engaged in such inducement to promote the sales of the Huawei '214 Accused Products and to actively induce its customers to infringe the '214 patent. Accordingly, Huawei has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '214 patent, knowing that such use constitutes infringement of the '214 patent.

236. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '214 patent.

237. As a result of Huawei's infringement of the '214 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Dunti respectfully requests that this Court enter:

- A. A judgment in favor of Plaintiff Dunti that Huawei has infringed, either literally and/or under the doctrine of equivalents, the '462 patent, the '701 patent, the '235 patent, the '286 patent, the '259 patent, the '196 patent, and/or the '214 patent;
- B. An award of damages resulting from Huawei's acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order requiring Huawei to provide accountings and to pay supplemental damages to Dunti, including, without limitation, prejudgment and post-judgment interest; and
- D. Any and all other relief to which Dunti may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Dunti requests a trial by jury of any issues so triable by right.

Dated: September 19, 2016

Respectfully submitted,

/s/ Matt Olavi

Elizabeth L. DeRieux (TX Bar No.
05770585)

D. Jeffrey Rambin (TX Bar No. 00791478)

CAPSHAW DERIEUX, LLP

114 E. Commerce Ave.

Gladewater, Texas 75647

Telephone: 903-845-5770

E-mail: ederieux@capshawlaw.com

E-mail: jrambin@capshawlaw.com

Matt Olavi (TX Bar No. 24095777)

Brian J. Dunne (CA SB No. 275689)

Douglas W. Meier (TX Bar No. 24100889)

OLAVI DUNNE LLP

816 Congress Ave., Ste. 1620

Austin, Texas 78701

Telephone: 512-717-4485

Facsimile: 512-717-4495

E-mail: molavi@olavidunne.com

E-mail: bdunne@olavidunne.com

E-mail: dmeier@olavidunne.com

*Attorneys for Dunti Network Technologies,
LLC*