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

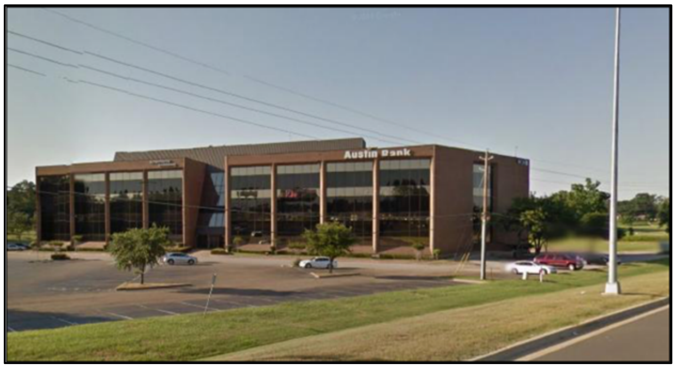
DUNTI NETWORK TECHNOLOGIES, LLC,	
Plaintiff,	**Civil Action No._________**
v.	
EXTREME NETWORKS, INC.,	**JURY TRIAL DEMANDED**
Defendant.	

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, defendant Extreme Networks, Inc. ("Extreme Networks") has adopted Dunti's patented technologies—developed more than a decade ago right here in Texas—*en masse*. Extreme Networks has profited handsomely from its use of Dunti's patented inventions, and Dunti deserves to be compensated for this use. But Extreme Networks 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"); and 7,778,259 ("the '259 patent") (collectively, "the patents-in-suit"), is brought to ensure that Extreme Networks 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 Extreme Networks, Dunti relies on its intellectual property.

3. On information and belief, Defendant Extreme Networks, Inc. is a Delaware corporation with its principal office at 145 Rio Robles, San Jose, CA 95134. Extreme Networks, Inc. can be served through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136.

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

5. In addition, on information and belief, Extreme Networks maintains a number of sales and technical employees in Texas and targets large enterprises, including broadband infrastructure providers, universities, and data center operators throughout Texas.[1]

[1] *See, e.g.*, http://investor.extremenetworks.com/releasedetail.cfm?releaseid=405505 (accessed Sept. 6, 2016); http://www.baylor.edu/mediacommunications/news.php?action=story&story=145543 (accessed Sept. 6, 2016); http://www.citynap.com/news/citynaps-virtualized-data-center-powered-by-extreme-networks/index.html (accessed Sept. 6, 2016).

JURISDICTION AND VENUE

6. 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).

7. Upon information and belief, this Court has personal jurisdiction over Extreme Networks, Inc. in this action because it 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 Extreme Networks, Inc. would not offend traditional notions of fair play and substantial justice. Defendant Extreme Networks, 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, Extreme Networks, Inc. is registered to do business in the State of Texas and has appointed CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136, as its agent for service of process.

8. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Extreme Networks, 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.

DUNTI'S LANDMARK NETWORK COMMUNICATION SYSTEMS

9. Dunti is the owner and assignee of ten patents on pioneering network technologies, including the five patents-in-suit (collectively, "the Dunti patents").

10. 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.

11. Even today, female engineers are rare in the American workforce, comprising just over ten percent of all engineers in recent government surveys.[2] 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.

12. 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.

13. 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.

14. 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 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.

[2] 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).

15. 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.[3] 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.

16. 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.

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

18. 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

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

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.

19. 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.[4]

20. 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.

21. 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.

22. 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. 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.

[4] "Trupta" means "complete" in Sanskrit.

23. 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

24. 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.

25. 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.

26. 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.

27. 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.

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

29. 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.

30. 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

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

32. 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.

33. 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.

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

35. 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.

36. 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.

37. 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.

38. 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

39. 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.

40. 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.

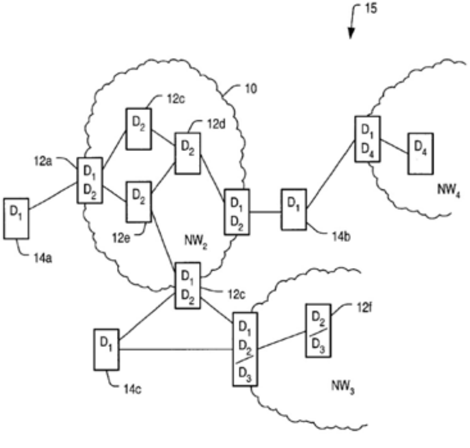


FIG. 1

’462 Patent, Fig. 1.

41. 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.

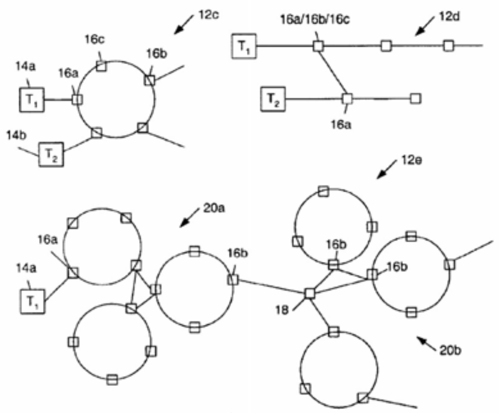


FIG. 2

’286 Patent, Fig. 2.

42. 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.

EXTREME NETWORKS' INFRINGING PRODUCTS AND SERVICES

43. On information and belief, Extreme Networks offers a high-performance data center networking solution that leverages Extreme Networks' OneFabric Connect and Software-Defined Architecture to provide a "unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure." Data Center Solutions Guide, *A Solution White Paper*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 5. The Extreme Data Center solution provides a "***secure, scalable infrastructure*** with the ability to expand or shrink resources based on business needs." *Id.* at 6 (emphasis added).

44. On information and belief, Extreme Networks' OneFabric architecture provides a complete data center solution that incorporates Extreme Networks' hardware and software products.

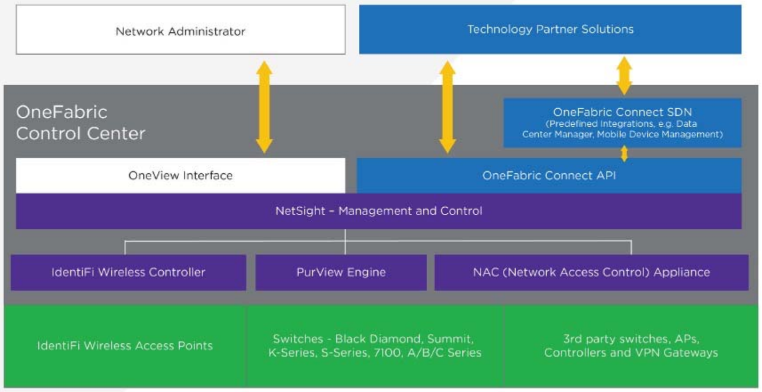
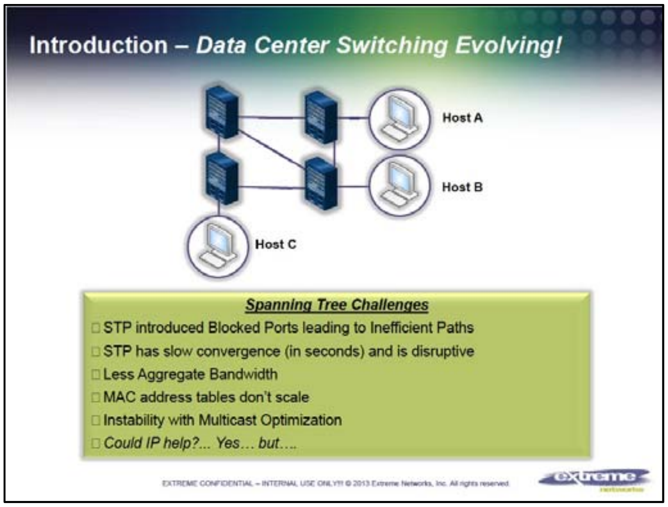

Network Administrator
Technology Partner Solutions
OneFabric Control Center
OneFabric Connect SDN
(Predefined Integrations, e.g. Data Center Manager, Mobile Device Management)
OneView Interface
OneFabric Connect API
NetSight – Management and Control
IdentiFi Wireless Controller
PurView Engine
NAC (Network Access Control) Appliance
IdentiFi Wireless Access Points
Switches - Black Diamond, Summit, K-Series, S-Series, 7100, A/B/C Series
3rd party switches, APs, Controllers and VPN Gateways

Figure X – OneFabric Solution Architecture

Data Center Solutions Guide, *A Solution White Paper*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 9.

45. On information and belief, Extreme Networks' OneFabric solution implements the Transparent Interconnection of Lots of Links ("TRILL") protocol, which "allows for improved scaling of data center servers and virtual machine interconnections by combining bridged networks with network topology control and routing management." Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13. As explained by Extreme Networks, the TRILL functionality implemented in its data center solution solves some of the problems associated with previous data center technology, such as "inefficient paths" and the fact that "MAC address tables don't scale," as shown below.


Introduction – *Data Center Switching Evolving!*

Host A
Host B
Host C

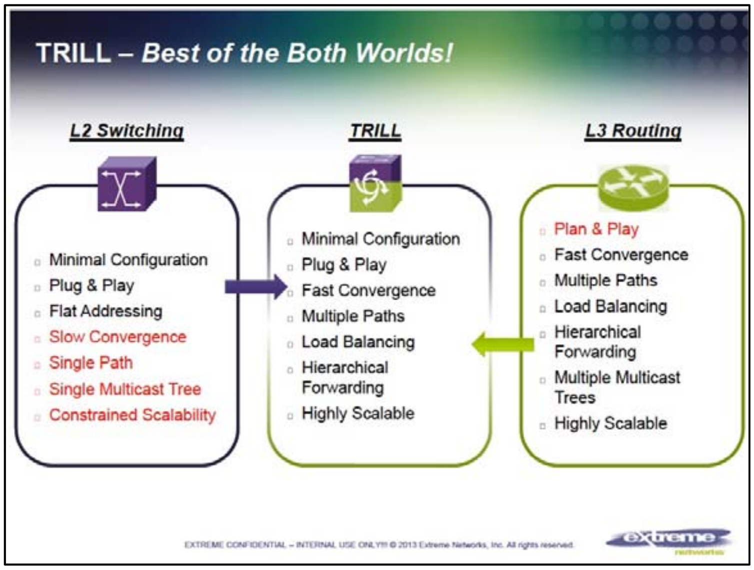
Spanning Tree Challenges

- □ STP introduced Blocked Ports leading to Inefficient Paths
- □ STP has slow convergence (in seconds) and is disruptive
- □ Less Aggregate Bandwidth
- □ MAC address tables don't scale
- □ Instability with Multicast Optimization
- □ *Could IP help?... Yes… but….*

EXTREME CONFIDENTIAL – INTERNAL USE ONLY!!! © 2013 Extreme Networks, Inc. All rights reserved

Pete Williams, *How to Scale the Data Centre with TRILL (and Other Technology)*, EXTREME NETWORKS PRESENTATION (2013), at 4.

46. On information and belief, and according to Extreme Networks, the TRILL functionality, as implemented in the Extreme Networks data center solutions, provides the "best of both worlds" between layer 2 switching and layer 3 routing.



TRILL – *Best of the Both Worlds!*

L2 Switching

- Minimal Configuration
- Plug & Play
- Flat Addressing
- Slow Convergence
- Single Path
- Single Multicast Tree
- Constrained Scalability

TRILL

- Minimal Configuration
- Plug & Play
- Fast Convergence
- Multiple Paths
- Load Balancing
- Hierarchical Forwarding
- Highly Scalable

L3 Routing

- Plan & Play
- Fast Convergence
- Multiple Paths
- Load Balancing
- Hierarchical Forwarding
- Multiple Multicast Trees
- Highly Scalable

EXTREME CONFIDENTIAL – INTERNAL USE ONLY!!! © 2013 Extreme Networks, Inc. All rights reserved.

Pete Williams, *How to Scale the Data Centre with TRILL (and Other Technology)*, EXTREME NETWORKS PRESENTATION (2013), at 5.

47. On information and belief, the Extreme Networks BlackDiamond-X series switches, Summit X670 series switches, and Summit X770 series switches implement TRILL functionality as part of the Extreme Networks OneFabric solution architecture. *See, e.g.*, Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

48. On information and belief, the Extreme Networks ExtremeXOS ("EXOS") is the operating system that runs on the Extreme Networks BlackDiamond-X, Summit X670, and Summit X770 series switches. *See, e.g.*, Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

49. On information and belief, Extreme Networks offers both on-site and remote installation of the Extreme Networks OneFabric Connect architecture. *See, e.g.*, Data Sheet, *OneFabric Connect*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 11.

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

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

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

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

57. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BlackDiamond-X series switches, including but not limited to the Extreme Networks X8 Series switches (collectively, “the Extreme Networks BD-X Switches”).

58. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X670 series switches, including but not limited to the Extreme Networks Summit X670-48x, the Summit X670V-48x, and the Summit X670V-48t switches (collectively, “the Extreme Networks Summit X670 Switches”).

59. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X770 series switches, including but not limited to the Extreme Networks Summit X770-32q switch (collectively, “the Extreme Networks Summit X770 Switches”).

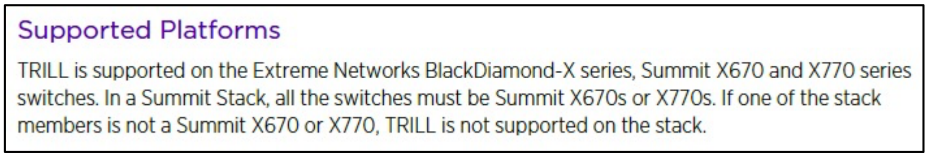
60. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks EXOS operating system.

61. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BD-X Switches, the Extreme Networks Summit X670 Switches, the Extreme

Networks Summit X770 Switches, and the Extreme Networks EXOS operating system (collectively, "the Extreme Networks '462 Accused Products").

62. Extreme Networks makes, uses, sells, and/or offers to sell networks comprised of the Extreme Networks '462 Accused Products ("an Extreme Networks '462 Accused Product Network").

63. On information and belief, an Extreme Networks '462 Accused Product Network implements at least the TRILL protocol.

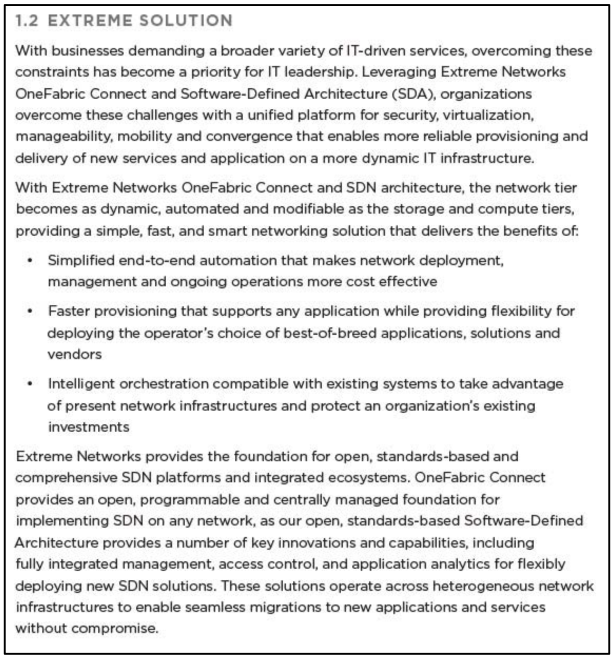


Supported Platforms

TRILL is supported on the Extreme Networks BlackDiamond-X series, Summit X670 and X770 series switches. In a Summit Stack, all the switches must be Summit X670s or X770s. If one of the stack members is not a Summit X670 or X770, TRILL is not supported on the stack.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

64. On information and belief, an Extreme Networks '462 Accused Product Network comprises a communication system.



1.2 EXTREME SOLUTION

With businesses demanding a broader variety of IT-driven services, overcoming these constraints has become a priority for IT leadership. Leveraging Extreme Networks OneFabric Connect and Software-Defined Architecture (SDA), organizations overcome these challenges with a unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure.

With Extreme Networks OneFabric Connect and SDN architecture, the network tier becomes as dynamic, automated and modifiable as the storage and compute tiers, providing a simple, fast, and smart networking solution that delivers the benefits of:

- Simplified end-to-end automation that makes network deployment, management and ongoing operations more cost effective
- Faster provisioning that supports any application while providing flexibility for deploying the operator's choice of best-of-breed applications, solutions and vendors
- Intelligent orchestration compatible with existing systems to take advantage of present network infrastructures and protect an organization's existing investments

Extreme Networks provides the foundation for open, standards-based and comprehensive SDN platforms and integrated ecosystems. OneFabric Connect provides an open, programmable and centrally managed foundation for implementing SDN on any network, as our open, standards-based Software-Defined Architecture provides a number of key innovations and capabilities, including fully integrated management, access control, and application analytics for flexibly deploying new SDN solutions. These solutions operate across heterogeneous network infrastructures to enable seamless migrations to new applications and services without compromise.

Data Center Solutions Guide, A Solution White Paper, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 5.

65. On information and belief, an Extreme Networks ’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 TRILL network and an intermediate module coupled between the entry and exit end modules. In a TRILL network, there can be multiple intermediate modules.

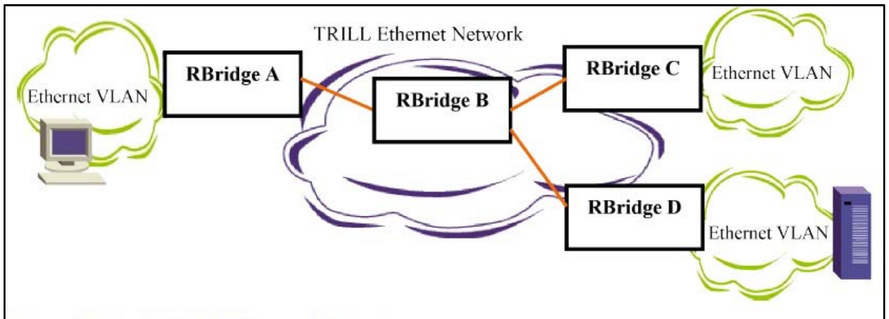
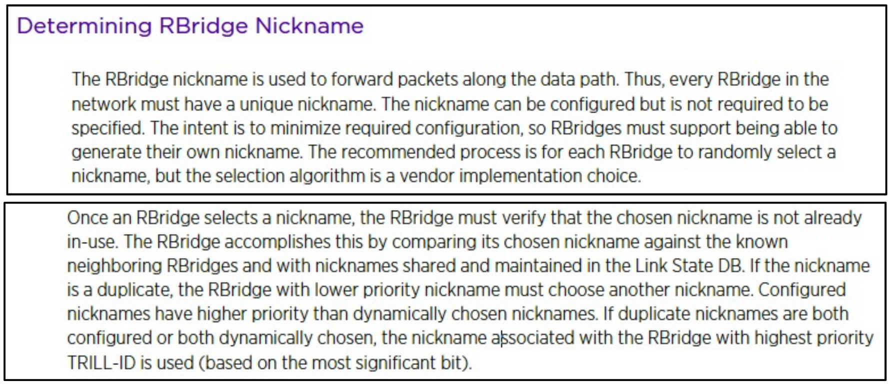


Figure 9: Simple TRILL Reference Network

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 23.

66. On information and belief, an Extreme Networks ’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 TRILL network is assigned a unique RBridge Nickname.



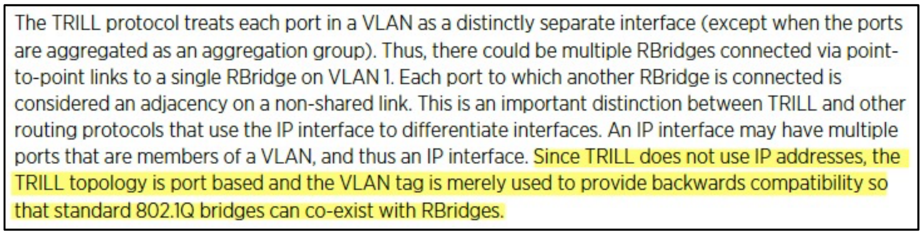
Determining RBridge Nickname

The RBridge nickname is used to forward packets along the data path. Thus, every RBridge in the network must have a unique nickname. The nickname can be configured but is not required to be specified. The intent is to minimize required configuration, so RBridges must support being able to generate their own nickname. The recommended process is for each RBridge to randomly select a nickname, but the selection algorithm is a vendor implementation choice.

Once an RBridge selects a nickname, the RBridge must verify that the chosen nickname is not already in-use. The RBridge accomplishes this by comparing its chosen nickname against the known neighboring RBridges and with nicknames shared and maintained in the Link State DB. If the nickname is a duplicate, the RBridge with lower priority nickname must choose another nickname. Configured nicknames have higher priority than dynamically chosen nicknames. If duplicate nicknames are both configured or both dynamically chosen, the nickname associated with the RBridge with highest priority TRILL-ID is used (based on the most significant bit).

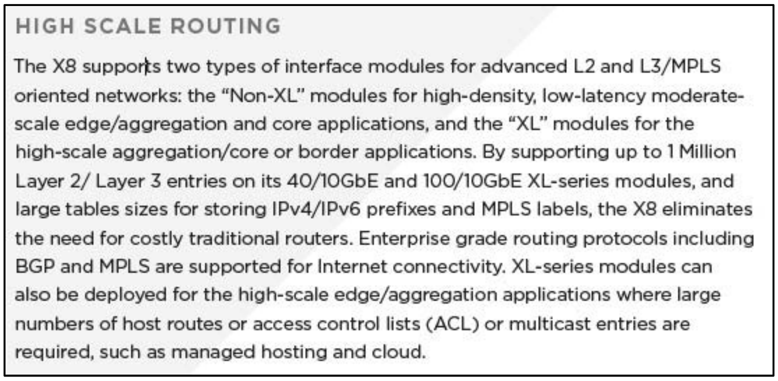
Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 31-32.

67. On information and belief, an Extreme Networks ’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 an Extreme Networks ’462 Accused Product Network can be addressed using IP addresses, but IP addresses are not used to address intermediate RBridges when forwarding packets within a TRILL network.



The TRILL protocol treats each port in a VLAN as a distinctly separate interface (except when the ports are aggregated as an aggregation group). Thus, there could be multiple RBridges connected via point-to-point links to a single RBridge on VLAN 1. Each port to which another RBridge is connected is considered an adjacency on a non-shared link. This is an important distinction between TRILL and other routing protocols that use the IP interface to differentiate interfaces. An IP interface may have multiple ports that are members of a VLAN, and thus an IP interface. Since TRILL does not use IP addresses, the TRILL topology is port based and the VLAN tag is merely used to provide backwards compatibility so that standard 802.1Q bridges can co-exist with RBridges.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 14 (highlighting added).



HIGH SCALE ROUTING

The X8 supports two types of interface modules for advanced L2 and L3/MPLS oriented networks: the “Non-XL” modules for high-density, low-latency moderate-scale edge/aggregation and core applications, and the “XL” modules for the high-scale aggregation/core or border applications. By supporting up to 1 Million Layer 2/ Layer 3 entries on its 40/10GbE and 100/10GbE XL-series modules, and large tables sizes for storing IPv4/IPv6 prefixes and MPLS labels, the X8 eliminates the need for costly traditional routers. Enterprise grade routing protocols including BGP and MPLS are supported for Internet connectivity. XL-series modules can also be deployed for the high-scale edge/aggregation applications where large numbers of host routes or access control lists (ACL) or multicast entries are required, such as managed hosting and cloud.

Data Sheet, *ExtremeSwitching X8*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2016), at 7.

68. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Extreme Networks ’462 Accused Products, Extreme Networks 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).

69. On information and belief, Extreme Networks also indirectly infringes the ’462 patent by actively inducing infringement under 35 U.S.C. § 271(b).

70. On information and belief, Extreme Networks 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, Extreme Networks knew of the ’462 patent and knew of its infringement, including by way of this lawsuit.

71. On information and belief, Extreme Networks intended to induce patent infringement by third-party customers and users of the Extreme Networks ’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. Extreme Networks specifically intended and was aware that the normal and customary use of the accused products would infringe the ’462 patent. Extreme Networks 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, Extreme Networks provides the Extreme Networks ’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 Extreme Networks further provides documentation and training materials that cause customers of the Extreme Networks ’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 Extreme Networks ’462 Accused Products, Extreme Networks specifically intended to induce infringement of the ’462 patent, including at least claim 1. On information and belief, Extreme Networks engaged in such inducement to promote the sales of the Extreme Networks ’462 Accused Products and to actively induce its customers to infringe the ’462 patent. Accordingly, Extreme Networks 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.

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

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

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

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

75. 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.

76. 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.

77. 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).

78. 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.

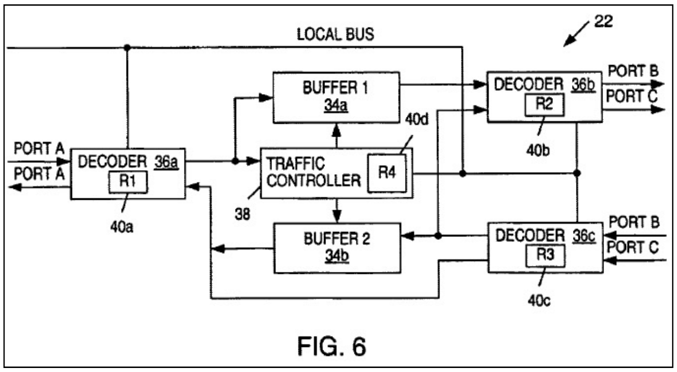


FIG. 6

’701 Patent, Fig. 6.

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

80. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BlackDiamond-X series switches, including but not limited to the Extreme Networks X8 Series switches (collectively, “the Extreme Networks BD-X Switches”).

81. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X670 series switches, including but not limited to the Extreme Networks Summit X670-48x, the Summit X670V-48x, and the Summit X670V-48t switches (collectively, “the Extreme Networks Summit X670 Switches”).

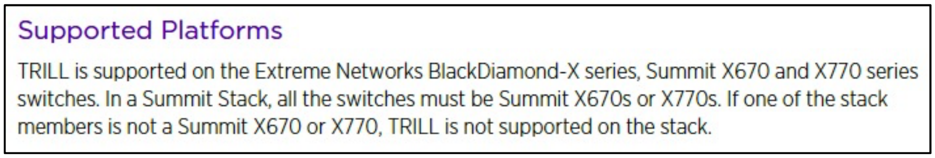
82. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X770 series switches, including but not limited to the Extreme Networks Summit X770-32q switch (collectively, "the Extreme Networks Summit X770 Switches").

83. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks EXOS operating system.

84. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BD-X Switches, the Extreme Networks Summit X670 Switches, the Extreme Networks Summit X770 Switches, and the Extreme Networks EXOS operating system (collectively, "the Extreme Networks '701 Accused Products").

85. Extreme Networks makes, uses, sells, and/or offers to sell networks comprised of the Extreme Networks '701 Accused Products ("an Extreme Networks '701 Accused Product Network").

86. On information and belief, an Extreme Networks '701 Accused Product Network implements at least the TRILL protocol.

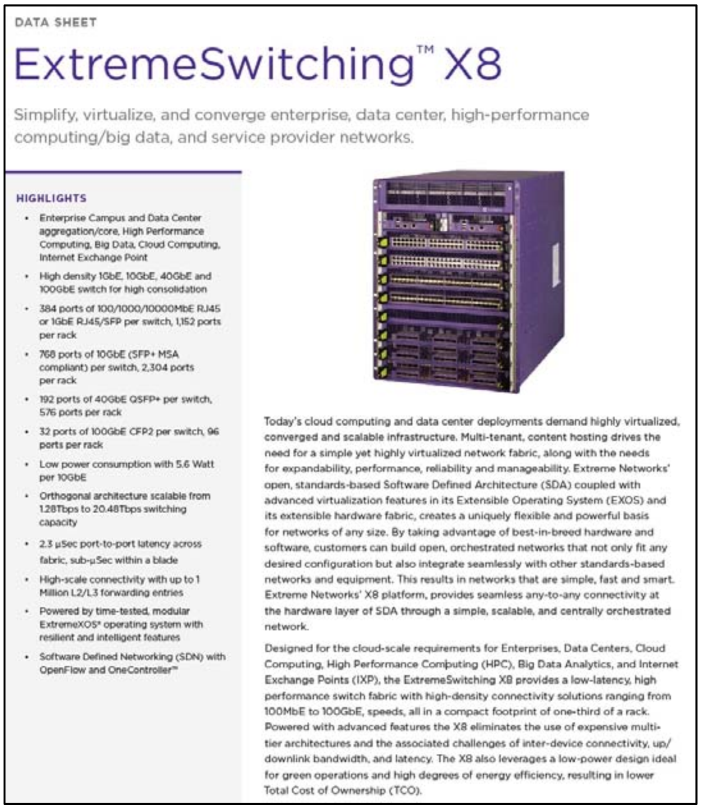


Supported Platforms

TRILL is supported on the Extreme Networks BlackDiamond-X series, Summit X670 and X770 series switches. In a Summit Stack, all the switches must be Summit X670s or X770s. If one of the stack members is not a Summit X670 or X770, TRILL is not supported on the stack.

Advanced Features, *ExtremeXOS 15.5 User Guide*, Extreme Networks Technical Documentation (June 2014), at 13.

87. On information and belief, the Extreme Networks '701 Accused Products comprise a switch.



DATA SHEET

ExtremeSwitching™ X8

Simplify, virtualize, and converge enterprise, data center, high-performance computing/big data, and service provider networks.

HIGHLIGHTS

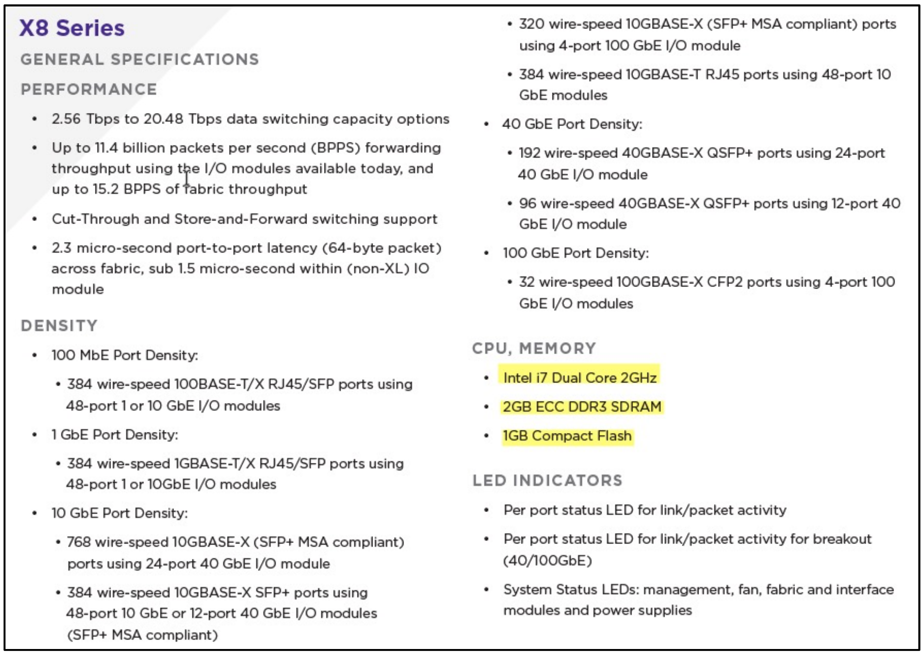
- Enterprise Campus and Data Center aggregation/core, High Performance Computing, Big Data, Cloud Computing, Internet Exchange Point
- High density 1GbE, 10GbE, 40GbE and 100GbE switch for high consolidation
- 384 ports of 100/1000/10000MbE RJ45 or 1GbE RJ45/SFP per switch, 1,152 ports per rack
- 768 ports of 10GbE (SFP+ MSA compliant) per switch, 2,304 ports per rack
- 192 ports of 40GbE QSFP+ per switch, 576 ports per rack
- 32 ports of 100GbE CFP2 per switch, 96 ports per rack
- Low power consumption with 5.6 Watt per 10GbE
- Orthogonal architecture scalable from 1.28Tbps to 20.48Tbps switching capacity
- 2.3 µSec port-to-port latency across fabric, sub-µSec within a blade
- High-scale connectivity with up to 1 Million L2/L3 forwarding entries
- Powered by time-tested, modular ExtremeXOS® operating system with resilient and intelligent features
- Software Defined Networking (SDN) with OpenFlow and OneController™

Today's cloud computing and data center deployments demand highly virtualized, converged and scalable infrastructure. Multi-tenant, content hosting drives the need for a simple yet highly virtualized network fabric, along with the needs for expandability, performance, reliability and manageability. Extreme Networks' open, standards-based Software Defined Architecture (SDA) coupled with advanced virtualization features in its Extensible Operating System (EXOS) and its extensible hardware fabric, creates a uniquely flexible and powerful basis for networks of any size. By taking advantage of best-in-breed hardware and software, customers can build open, orchestrated networks that not only fit any desired configuration but also integrate seamlessly with other standards-based networks and equipment. This results in networks that are simple, fast and smart. Extreme Networks' X8 platform, provides seamless any-to-any connectivity at the hardware layer of SDA through a simple, scalable, and centrally orchestrated network.

Designed for the cloud-scale requirements for Enterprises, Data Centers, Cloud Computing, High Performance Computing (HPC), Big Data Analytics, and Internet Exchange Points (IXP), the ExtremeSwitching X8 provides a low-latency, high performance switch fabric with high-density connectivity solutions ranging from 100MbE to 100GbE, speeds, all in a compact footprint of one-third of a rack. Powered with advanced features the X8 eliminates the use of expensive multi-tier architectures and the associated challenges of inter-device connectivity, up/downlink bandwidth, and latency. The X8 also leverages a low-power design ideal for green operations and high degrees of energy efficiency, resulting in lower Total Cost of Ownership (TCO).

Data Sheet, *ExtremeSwitching X8*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2016), at 1.

88. On information and belief, the Extreme Networks ’701 Accused Products within a TRILL network comprise a traffic manager which dispatches a series of read operations to a memory coupled within a data flow path. For example, the Extreme Networks ’701 Accused Products include memory and at least one processor.



X8 Series

GENERAL SPECIFICATIONS

PERFORMANCE

- 2.56 Tbps to 20.48 Tbps data switching capacity options
- Up to 11.4 billion packets per second (BPPS) forwarding throughput using the I/O modules available today, and up to 15.2 BPPS of fabric throughput
- Cut-Through and Store-and-Forward switching support
- 2.3 micro-second port-to-port latency (64-byte packet) across fabric, sub 1.5 micro-second within (non-XL) IO module

DENSITY

- 100 MbE Port Density:
  - 384 wire-speed 100BASE-T/X RJ45/SFP ports using 48-port 1 or 10 GbE I/O modules
- 1 GbE Port Density:
  - 384 wire-speed 1GBASE-T/X RJ45/SFP ports using 48-port 1 or 10GbE I/O modules
- 10 GbE Port Density:
  - 768 wire-speed 10GBASE-X (SFP+ MSA compliant) ports using 24-port 40 GbE I/O module
  - 384 wire-speed 10GBASE-X SFP+ ports using 48-port 10 GbE or 12-port 40 GbE I/O modules (SFP+ MSA compliant)
  - 320 wire-speed 10GBASE-X (SFP+ MSA compliant) ports using 4-port 100 GbE I/O module
  - 384 wire-speed 10GBASE-T RJ45 ports using 48-port 10 GbE modules
- 40 GbE Port Density:
  - 192 wire-speed 40GBASE-X QSFP+ ports using 24-port 40 GbE I/O module
  - 96 wire-speed 40GBASE-X QSFP+ ports using 12-port 40 GbE I/O module
- 100 GbE Port Density:
  - 32 wire-speed 100GBASE-X CFP2 ports using 4-port 100 GbE I/O modules

CPU, MEMORY

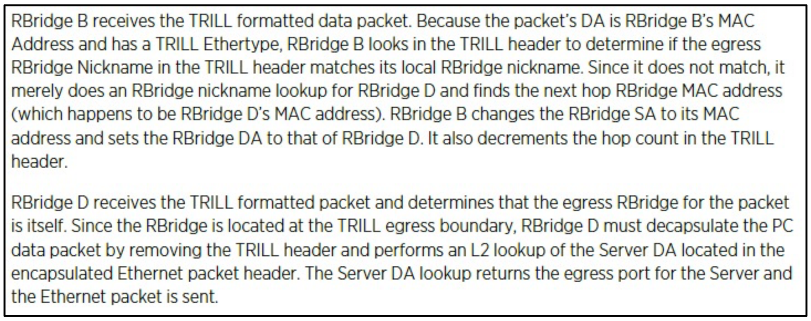
- Intel i7 Dual Core 2GHz
- 2GB ECC DDR3 SDRAM
- 1GB Compact Flash

LED INDICATORS

- Per port status LED for link/packet activity
- Per port status LED for link/packet activity for breakout (40/100GbE)
- System Status LEDs: management, fan, fabric and interface modules and power supplies

Data Sheet, *ExtremeSwitching X8*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2016), at 7 (highlighting added).

89. On information and belief, the Extreme Networks ’701 Accused Products within a TRILL network include a 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.

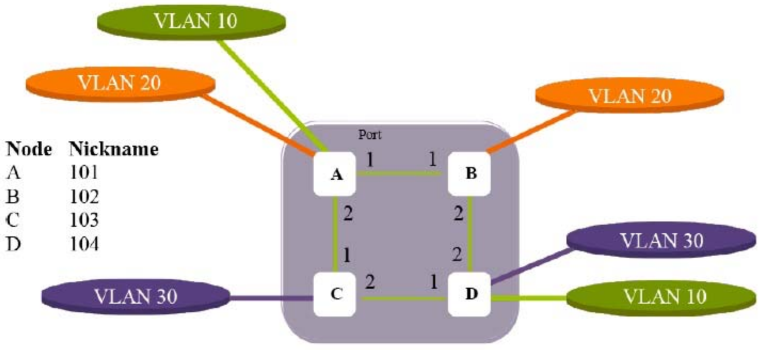


RBridge B receives the TRILL formatted data packet. Because the packet's DA is RBridge B's MAC Address and has a TRILL Ethertype, RBridge B looks in the TRILL header to determine if the egress RBridge Nickname in the TRILL header matches its local RBridge nickname. Since it does not match, it merely does an RBridge nickname lookup for RBridge D and finds the next hop RBridge MAC address (which happens to be RBridge D's MAC address). RBridge B changes the RBridge SA to its MAC address and sets the RBridge DA to that of RBridge D. It also decrements the hop count in the TRILL header.

RBridge D receives the TRILL formatted packet and determines that the egress RBridge for the packet is itself. Since the RBridge is located at the TRILL egress boundary, RBridge D must decapsulate the PC data packet by removing the TRILL header and performs an L2 lookup of the Server DA located in the encapsulated Ethernet packet header. The Server DA lookup returns the egress port for the Server and the Ethernet packet is sent.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 25.

90. On information and belief, the Extreme Networks ’701 Accused Products comprise an input port and an output port.

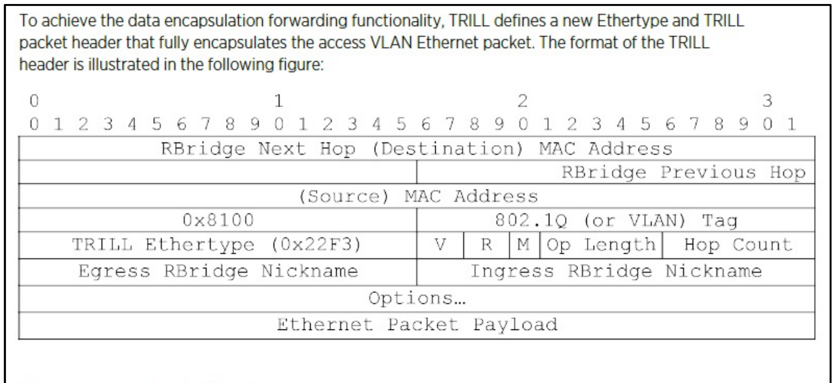


Node	Nickname
A	101
B	102
C	103
D	104

Figure 23: TRILL Network Configuration

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 37.

91. On information and belief, the memory in the Extreme Networks ’701 Accused Products comprises packets of data dispatched from the input port. For example, the Extreme Network ’701 Accused Products encapsulate incoming data packets within a TRILL header. The incoming data packets are comprised in memory within an ingress RBridge as they are encapsulated within a TRILL header as forwarding decisions are made.



To achieve the data encapsulation forwarding functionality, TRILL defines a new Ethertype and TRILL packet header that fully encapsulates the access VLAN Ethernet packet. The format of the TRILL header is illustrated in the following figure:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

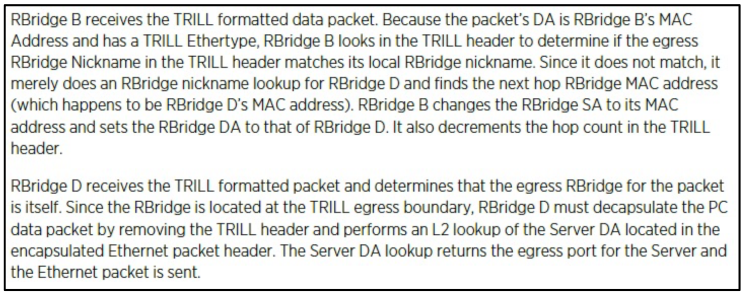
<table>
<tr><td colspan="6">RBridge Next Hop (Destination) MAC Address</td></tr>
<tr><td></td><td colspan="5">RBridge Previous Hop</td></tr>
<tr><td colspan="6">(Source) MAC Address</td></tr>
<tr><td>0x8100</td><td colspan="5">802.1Q (or VLAN) Tag</td></tr>
<tr><td>TRILL Ethertype (0x22F3)</td><td>V</td><td>R</td><td>M</td><td>Op Length</td><td>Hop Count</td></tr>
<tr><td>Egress RBridge Nickname</td><td colspan="5">Ingress RBridge Nickname</td></tr>
<tr><td colspan="6">Options...</td></tr>
<tr><td colspan="6">Ethernet Packet Payload</td></tr>
</table>

Figure 8: Data Packet Header

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 23.

92. On information and belief, the Extreme Networks ’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, the TRILL header includes an Egress RBridge Nickname field and the Outer Ethernet Header includes an RBridge

Next Hop (Destination) MAC Address field, both of which comprise a destination address. The Egress RBridge Nickname is decoded as forwarding decisions are made.



RBridge B receives the TRILL formatted data packet. Because the packet's DA is RBridge B's MAC Address and has a TRILL Ethertype, RBridge B looks in the TRILL header to determine if the egress RBridge Nickname in the TRILL header matches its local RBridge nickname. Since it does not match, it merely does an RBridge nickname lookup for RBridge D and finds the next hop RBridge MAC address (which happens to be RBridge D's MAC address). RBridge B changes the RBridge SA to its MAC address and sets the RBridge DA to that of RBridge D. It also decrements the hop count in the TRILL header.

RBridge D receives the TRILL formatted packet and determines that the egress RBridge for the packet is itself. Since the RBridge is located at the TRILL egress boundary, RBridge D must decapsulate the PC data packet by removing the TRILL header and performs an L2 lookup of the Server DA located in the encapsulated Ethernet packet header. The Server DA lookup returns the egress port for the Server and the Ethernet packet is sent.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 25.

93. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Extreme Networks ’701 Accused Products, Extreme Networks 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).

94. On information and belief, Extreme Networks also indirectly infringes the ’701 patent by actively inducing infringement under 35 U.S.C. § 271(b).

95. On information and belief, Extreme Networks 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, Extreme Networks knew of the ’701 patent and knew of its infringement, including by way of this lawsuit.

96. On information and belief, Extreme Networks intended to induce patent infringement by third-party customers and users of the Extreme Networks ’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. Extreme Networks specifically intended and was aware that the normal and customary use of the accused products would infringe the ’701 patent. Extreme Networks 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, Extreme

Networks provides the Extreme Networks ’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 Extreme Networks further provides documentation and training materials that cause customers of the Extreme Networks ’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 Extreme Networks ’701 Accused Products, Extreme Networks specifically intended to induce infringement of the ’701 patent, including at least claim 1. On information and belief, Extreme Networks engaged in such inducement to promote the sales of the Extreme Networks ’701 Accused Products and to actively induce its customers to infringe the ’701 patent. Accordingly, Extreme Networks 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.

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

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

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

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

100. 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.

101. 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.

102. 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.

103. 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.

104. 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.

105. 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.

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

107. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BlackDiamond-X series switches, including but not limited to the Extreme Networks X8 Series switches (collectively, “the Extreme Networks BD-X Switches”).

108. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X670 series switches, including but not limited to the Extreme Networks Summit X670-48x, the Summit X670V-48x, and the Summit X670V-48t switches (collectively, “the Extreme Networks Summit X670 Switches”).

109. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X770 series switches, including but not limited to the Extreme Networks Summit X770-32q switch (collectively, “the Extreme Networks Summit X770 Switches”).

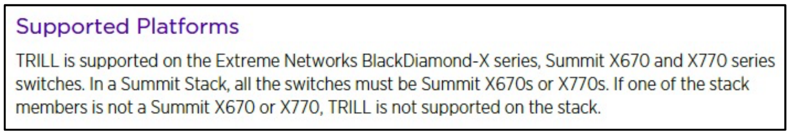
110. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks EXOS operating system.

111. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BD-X Switches, the Extreme Networks Summit X670 Switches, the Extreme

Networks Summit X770 Switches, and the Extreme Networks EXOS operating system (collectively, "the Extreme Networks '235 Accused Products").

112. Extreme Networks makes, uses, sells, and/or offers to sell networks comprised of the Extreme Networks '235 Accused Products ("an Extreme Networks '235 Accused Product Network").

113. On information and belief, an Extreme Networks '235 Accused Product Network implements at least the TRILL protocol.



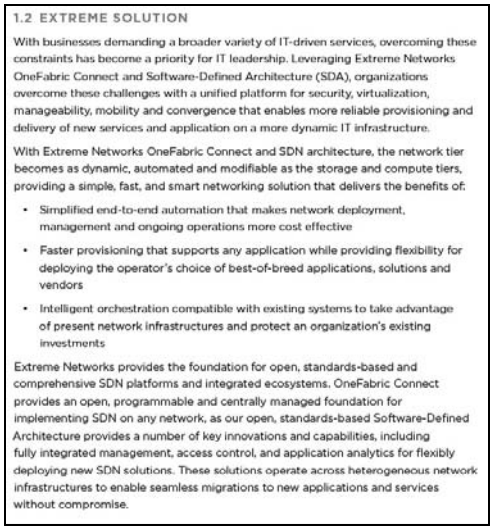
Supported Platforms

TRILL is supported on the Extreme Networks BlackDiamond-X series, Summit X670 and X770 series switches. In a Summit Stack, all the switches must be Summit X670s or X770s. If one of the stack members is not a Summit X670 or X770, TRILL is not supported on the stack.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

114. On information and belief, an Extreme Networks '235 Accused Product Network comprises a communication network.

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



1.2 EXTREME SOLUTION

With businesses demanding a broader variety of IT-driven services, overcoming these constraints has become a priority for IT leadership. Leveraging Extreme Networks OneFabric Connect and Software-Defined Architecture (SDA), organizations overcome these challenges with a unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure.

With Extreme Networks OneFabric Connect and SDN architecture, the network tier becomes as dynamic, automated and modifiable as the storage and compute tiers, providing a simple, fast, and smart networking solution that delivers the benefits of:

- Simplified end-to-end automation that makes network deployment, management and ongoing operations more cost effective
- Faster provisioning that supports any application while providing flexibility for deploying the operator's choice of best-of-breed applications, solutions and vendors
- Intelligent orchestration compatible with existing systems to take advantage of present network infrastructures and protect an organization's existing investments

Extreme Networks provides the foundation for open, standards-based and comprehensive SDN platforms and integrated ecosystems. OneFabric Connect provides an open, programmable and centrally managed foundation for implementing SDN on any network, as our open, standards-based Software-Defined Architecture provides a number of key innovations and capabilities, including fully integrated management, access control, and application analytics for flexibly deploying new SDN solutions. These solutions operate across heterogeneous network infrastructures to enable seamless migrations to new applications and services without compromise.

Data Center Solutions Guide, A Solution White Paper, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 5.

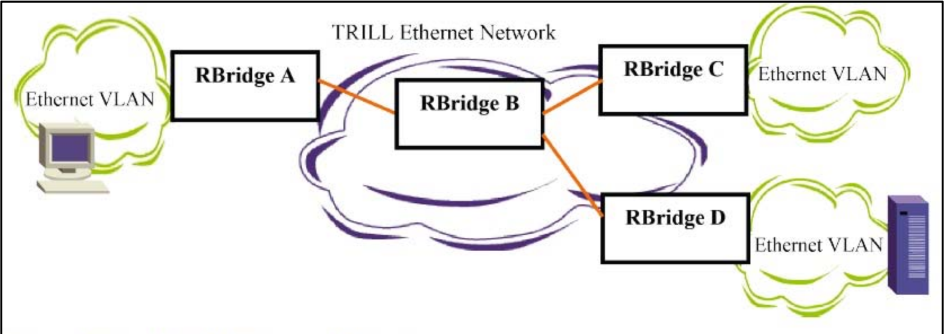
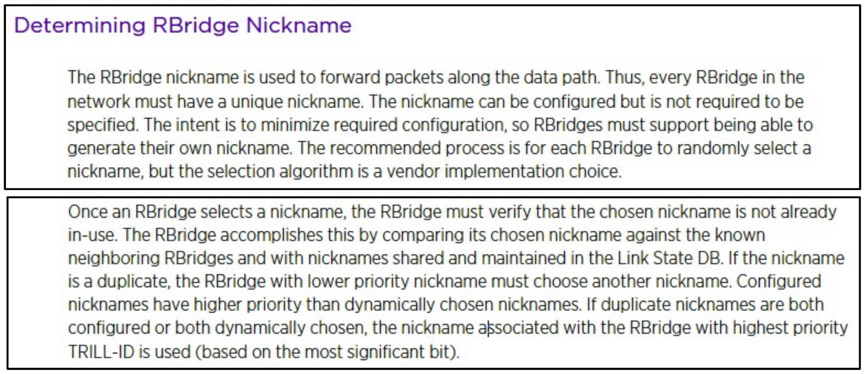


Figure 9: Simple TRILL Reference Network

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 24.

116. On information and belief, modules within an Extreme Networks ’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 TRILL 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 topologies.



Determining RBridge Nickname

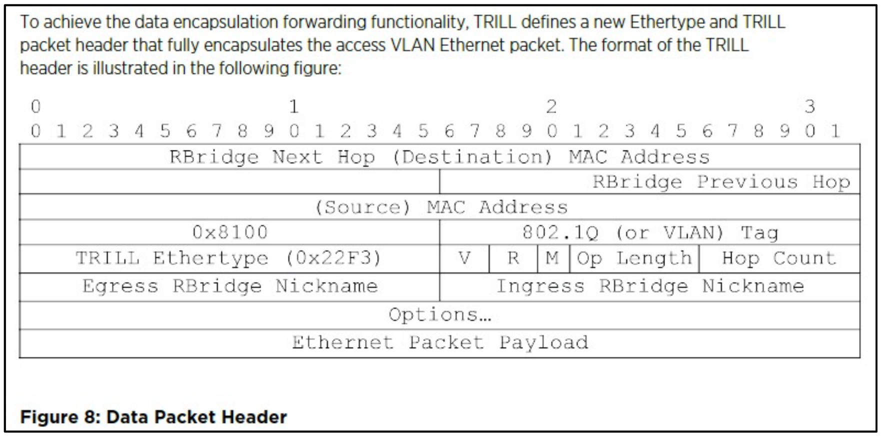
The RBridge nickname is used to forward packets along the data path. Thus, every RBridge in the network must have a unique nickname. The nickname can be configured but is not required to be specified. The intent is to minimize required configuration, so RBridges must support being able to generate their own nickname. The recommended process is for each RBridge to randomly select a nickname, but the selection algorithm is a vendor implementation choice.

Once an RBridge selects a nickname, the RBridge must verify that the chosen nickname is not already in-use. The RBridge accomplishes this by comparing its chosen nickname against the known neighboring RBridges and with nicknames shared and maintained in the Link State DB. If the nickname is a duplicate, the RBridge with lower priority nickname must choose another nickname. Configured nicknames have higher priority than dynamically chosen nicknames. If duplicate nicknames are both configured or both dynamically chosen, the nickname associated with the RBridge with highest priority TRILL-ID is used (based on the most significant bit).

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 31-32.

117. On information and belief, the first model layer used in an Extreme Networks ’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 TRILL 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.



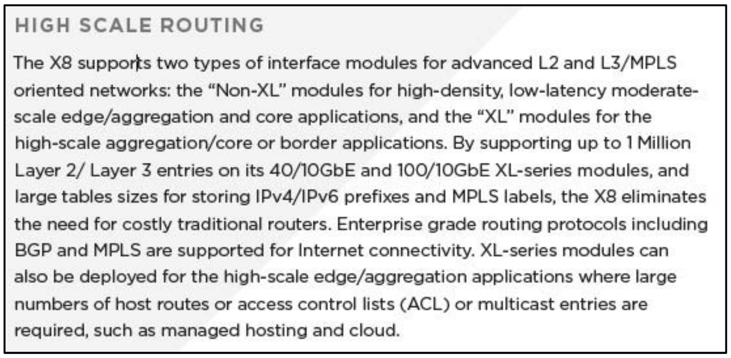
To achieve the data encapsulation forwarding functionality, TRILL defines a new Ethertype and TRILL packet header that fully encapsulates the access VLAN Ethernet packet. The format of the TRILL header is illustrated in the following figure:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|          RBridge Next Hop (Destination) MAC Address           |
+-------------------------------+-------------------------------+
|                               |          RBridge Previous Hop |
+-------------------------------+-------------------------------+
|                      (Source) MAC Address                     |
+-------------------------------+-------------------------------+
|            0x8100             |      802.1Q (or VLAN) Tag     |
+-------------------------------+---+---+-+---------+-----------+
|    TRILL Ethertype (0x22F3)   | V | R |M|Op Length| Hop Count |
+-------------------------------+---+---+-+---------+-----------+
|     Egress RBridge Nickname   |    Ingress RBridge Nickname   |
+-------------------------------+-------------------------------+
|                           Options…                            |
+---------------------------------------------------------------+
|                    Ethernet Packet Payload                    |
+---------------------------------------------------------------+
```

Figure 8: Data Packet Header

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 23.

118. On information and belief, the second model layer used in an Extreme Networks ’235 Accused Product Network is higher than a physical layer of the OSI reference model. For example, the edge switches in an Extreme Networks ’235 Accused Product Network can use IP addresses to route data packets outside of a TRILL network, and the IP address layer is higher than a physical layer of the OSI model.



HIGH SCALE ROUTING

The X8 supports two types of interface modules for advanced L2 and L3/MPLS oriented networks: the "Non-XL" modules for high-density, low-latency moderate-scale edge/aggregation and core applications, and the "XL" modules for the high-scale aggregation/core or border applications. By supporting up to 1 Million Layer 2/ Layer 3 entries on its 40/10GbE and 100/10GbE XL-series modules, and large tables sizes for storing IPv4/IPv6 prefixes and MPLS labels, the X8 eliminates the need for costly traditional routers. Enterprise grade routing protocols including BGP and MPLS are supported for Internet connectivity. XL-series modules can also be deployed for the high-scale edge/aggregation applications where large numbers of host routes or access control lists (ACL) or multicast entries are required, such as managed hosting and cloud.

Data Sheet, *ExtremeSwitching X8*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2016), at 7.

119. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Extreme Networks ’235 Accused

Products, Extreme Networks 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).

120. On information and belief, Extreme Networks also indirectly infringes the ’235 patent by actively inducing infringement under 35 U.S.C. § 271(b).

121. On information and belief, Extreme Networks 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, Extreme Networks knew of the ’235 patent and knew of its infringement, including by way of this lawsuit.

122. On information and belief, Extreme Networks intended to induce patent infringement by third-party customers and users of the Extreme Networks ’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. Extreme Networks specifically intended and was aware that the normal and customary use of the accused products would infringe the ’235 patent. Extreme Networks 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, Extreme Networks provides the Extreme Networks ’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 Extreme Networks further provides documentation and training materials that cause customers of the Extreme Networks ’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 Extreme Networks ’235 Accused Products, Extreme Networks specifically intended to induce infringement of the ’235 patent, including at least claim 1. On information and belief, Extreme Networks engaged in such inducement to promote the sales of the Extreme Networks ’235 Accused Products and to actively induce its customers to infringe the ’235 patent. Accordingly, Extreme Networks 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.

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

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

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

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

126. 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.

127. 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.

128. 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.

129. 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.

130. 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.

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

132. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BlackDiamond-X series switches, including but not limited to the Extreme Networks X8 Series switches (collectively, “the Extreme Networks BD-X Switches”).

133. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X670 series switches, including but not limited to the Extreme Networks

Summit X670-48x, the Summit X670V-48x, and the Summit X670V-48t switches (collectively, “the Extreme Networks Summit X670 Switches”).

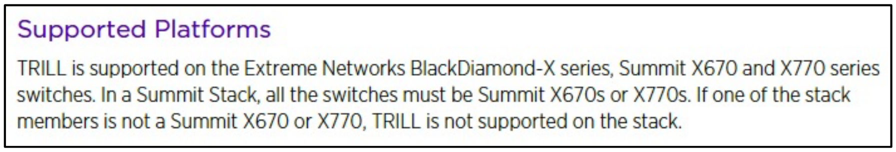
134. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X770 series switches, including but not limited to the Extreme Networks Summit X770-32q switch (collectively, “the Extreme Networks Summit X770 Switches”).

135. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks EXOS operating system.

136. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BD-X Switches, the Extreme Networks Summit X670 Switches, the Extreme Networks Summit X770 Switches, and the Extreme Networks EXOS operating system (collectively, “the Extreme Networks ’286 Accused Products”).

137. Extreme Networks makes, uses, sells, and/or offers to sell networks comprised of the Extreme Networks ’286 Accused Products (“an Extreme Networks ’286 Accused Product Network”).

138. On information and belief, an Extreme Networks ’286 Accused Product Network implements at least the TRILL protocol.

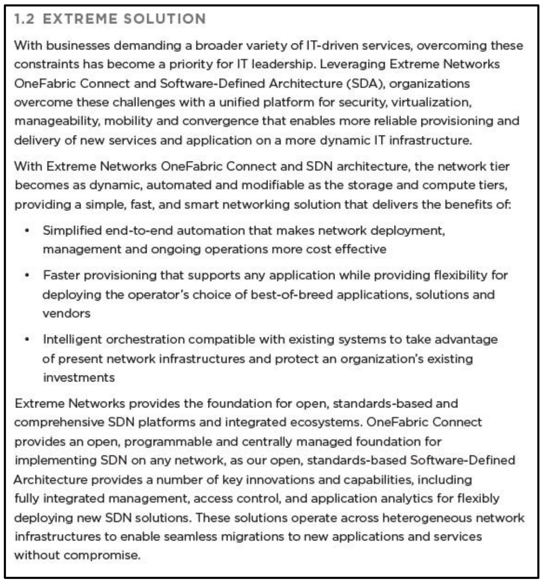


Supported Platforms

TRILL is supported on the Extreme Networks BlackDiamond-X series, Summit X670 and X770 series switches. In a Summit Stack, all the switches must be Summit X670s or X770s. If one of the stack members is not a Summit X670 or X770, TRILL is not supported on the stack.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

139. On information and belief, an Extreme Networks ’286 Accused Product Network comprises a communication network.



1.2 EXTREME SOLUTION

With businesses demanding a broader variety of IT-driven services, overcoming these constraints has become a priority for IT leadership. Leveraging Extreme Networks OneFabric Connect and Software-Defined Architecture (SDA), organizations overcome these challenges with a unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure.

With Extreme Networks OneFabric Connect and SDN architecture, the network tier becomes as dynamic, automated and modifiable as the storage and compute tiers, providing a simple, fast, and smart networking solution that delivers the benefits of:

- Simplified end-to-end automation that makes network deployment, management and ongoing operations more cost effective
- Faster provisioning that supports any application while providing flexibility for deploying the operator's choice of best-of-breed applications, solutions and vendors
- Intelligent orchestration compatible with existing systems to take advantage of present network infrastructures and protect an organization's existing investments

Extreme Networks provides the foundation for open, standards-based and comprehensive SDN platforms and integrated ecosystems. OneFabric Connect provides an open, programmable and centrally managed foundation for implementing SDN on any network, as our open, standards-based Software-Defined Architecture provides a number of key innovations and capabilities, including fully integrated management, access control, and application analytics for flexibly deploying new SDN solutions. These solutions operate across heterogeneous network infrastructures to enable seamless migrations to new applications and services without compromise.

Data Center Solutions Guide, A Solution White Paper, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 5.

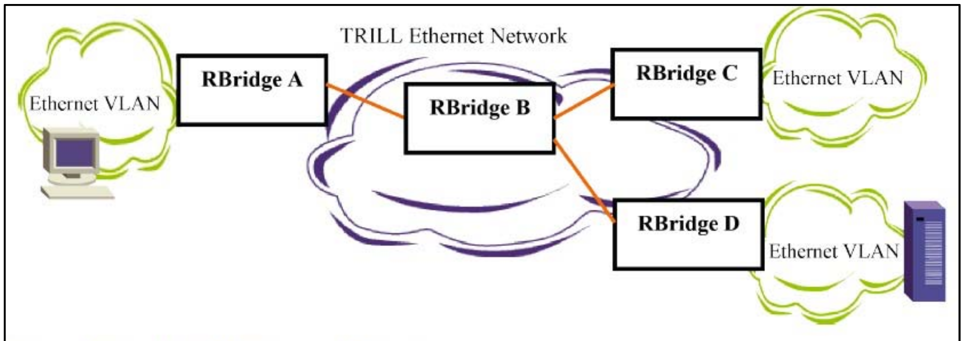


Figure 9: Simple TRILL Reference Network

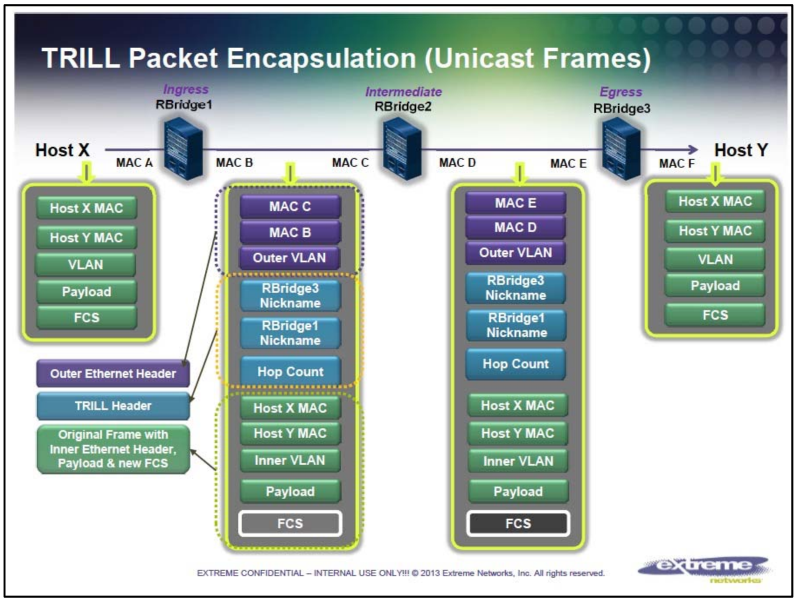
Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 24.

140. On information and belief, an Extreme Networks '286 Accused Product Network comprises an entry end switch.

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

142. On information and belief, an Extreme Networks '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 RBridge1), an exit end switch (i.e., Egress RBridge3), and an intermediate switch (i.e., Intermediate RBridge2) in between them. A TRILL network can include multiple intermediate RBridges and multiple hosts (e.g., Host Y) connected to an egress RBridge.



TRILL Packet Encapsulation (Unicast Frames)

Ingress RBridge1
Intermediate RBridge2
Egress RBridge3
Host X
Host Y
MAC A
MAC B
MAC C
MAC D
MAC E
MAC F

Host X MAC
Host Y MAC
VLAN
Payload
FCS

Outer Ethernet Header
TRILL Header
Original Frame with Inner Ethernet Header, Payload & new FCS

MAC C
MAC B
Outer VLAN
RBridge3 Nickname
RBridge1 Nickname
Hop Count
Host X MAC
Host Y MAC
Inner VLAN
Payload
FCS

MAC E
MAC D
Outer VLAN
RBridge3 Nickname
RBridge1 Nickname
Hop Count
Host X MAC
Host Y MAC
Inner VLAN
Payload
FCS

Host X MAC
Host Y MAC
VLAN
Payload
FCS

EXTREME CONFIDENTIAL – INTERNAL USE ONLY!!! © 2013 Extreme Networks, Inc. All rights reserved.

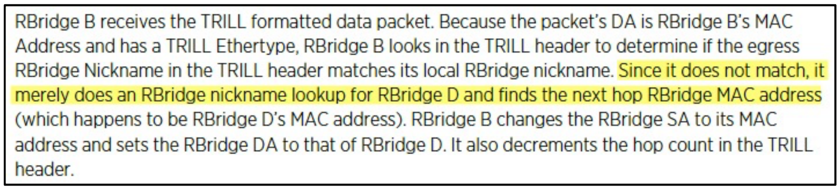
extreme networks

Pete Williams, *How to Scale the Data Centre with TRILL (and Other Technology)*, EXTREME NETWORKS PRESENTATION (2013), at 9.

143. On information and belief, an entry end switch in an Extreme Networks ’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 an Outer Ethernet 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).

144. On information and belief, in an Extreme Networks ’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

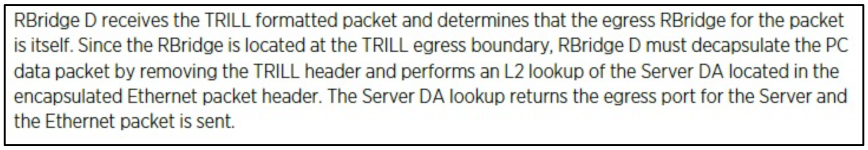
end switch to the exit termination device. For example, each intermediate switch (i.e., intermediate RBridge) uses the Egress RBridge Nickname within the TRILL header to point the packet to the next RBridge.



RBridge B receives the TRILL formatted data packet. Because the packet's DA is RBridge B's MAC Address and has a TRILL Ethertype, RBridge B looks in the TRILL header to determine if the egress RBridge Nickname in the TRILL header matches its local RBridge nickname. Since it does not match, it merely does an RBridge nickname lookup for RBridge D and finds the next hop RBridge MAC address (which happens to be RBridge D's MAC address). RBridge B changes the RBridge SA to its MAC address and sets the RBridge DA to that of RBridge D. It also decrements the hop count in the TRILL header.

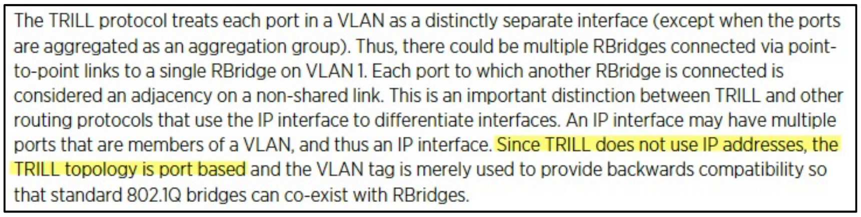
Advanced Features, *ExtremeXOS 15.5 User Guide*, Extreme Networks Technical Documentation (June 2014), at 25 (highlighting added).

145. In addition, on information and belief, the exit end switch (i.e., egress RBridge) performs the entirety of all translation needed by the TRILL network to route the packet from the egress RBridge to the exit termination device (i.e., the packet's final destination) when it "performs an L2 lookup of the Server DA located in the encapsulated Ethernet packet header."



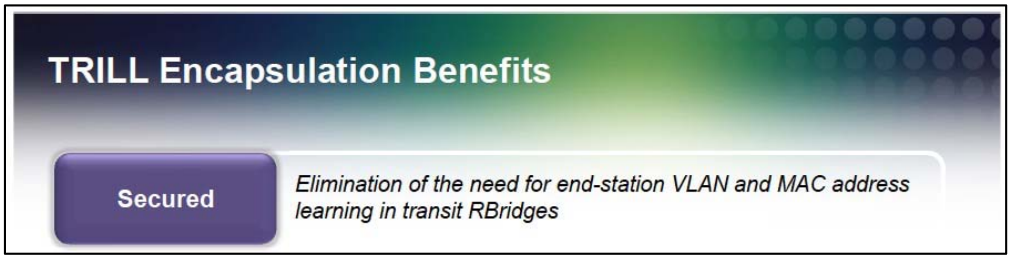
RBridge D receives the TRILL formatted packet and determines that the egress RBridge for the packet is itself. Since the RBridge is located at the TRILL egress boundary, RBridge D must decapsulate the PC data packet by removing the TRILL header and performs an L2 lookup of the Server DA located in the encapsulated Ethernet packet header. The Server DA lookup returns the egress port for the Server and the Ethernet packet is sent.

Advanced Features, *ExtremeXOS 15.5 User Guide*, Extreme Networks Technical Documentation (June 2014), at 25.



The TRILL protocol treats each port in a VLAN as a distinctly separate interface (except when the ports are aggregated as an aggregation group). Thus, there could be multiple RBridges connected via point-to-point links to a single RBridge on VLAN 1. Each port to which another RBridge is connected is considered an adjacency on a non-shared link. This is an important distinction between TRILL and other routing protocols that use the IP interface to differentiate interfaces. An IP interface may have multiple ports that are members of a VLAN, and thus an IP interface. Since TRILL does not use IP addresses, the TRILL topology is port based and the VLAN tag is merely used to provide backwards compatibility so that standard 802.1Q bridges can co-exist with RBridges.

Advanced Features, *ExtremeXOS 15.5 User Guide*, Extreme Networks Technical Documentation (June 2014), at 14 (highlighting added).


TRILL Encapsulation Benefits

Elimination of the need for end-station VLAN and MAC address learning in transit RBridges

Pete Williams, *How to Scale the Data Centre with TRILL (and Other Technology)*, EXTREME NETWORKS PRESENTATION (2013), at 10.

146. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Extreme Networks ’286 Accused Products, Extreme Networks 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).

147. On information and belief, Extreme Networks also indirectly infringes the ’286 patent by actively inducing infringement under 35 U.S.C. § 271(b).

148. On information and belief, Extreme Networks 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, Extreme Networks knew of the ’286 patent and knew of its infringement, including by way of this lawsuit.

149. On information and belief, Extreme Networks intended to induce patent infringement by third-party customers and users of the Extreme Networks ’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. Extreme Networks specifically intended and was aware that the normal and customary use of the accused products would infringe the ’286 patent. Extreme Networks 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, Extreme Networks provides the Extreme Networks ’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 Extreme Networks further provides documentation and training materials that cause

customers of the Extreme Networks ’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 Extreme Networks ’286 Accused Products, Extreme Networks specifically intended to induce infringement of the ’286 patent, including at least claim 6. On information and belief, Extreme Networks engaged in such inducement to promote the sales of the Extreme Networks ’286 Accused Products and to actively induce its customers to infringe the ’286 patent. Accordingly, Extreme Networks 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.

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

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

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

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

153. 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.

154. 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.

155. 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.

156. 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.

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

158. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BlackDiamond-X series switches, including but not limited to the Extreme Networks X8 Series switches (collectively, “the Extreme Networks BD-X Switches”).

159. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X670 series switches, including but not limited to the Extreme Networks Summit X670-48x, the Summit X670V-48x, and the Summit X670V-48t switches (collectively, “the Extreme Networks Summit X670 Switches”).

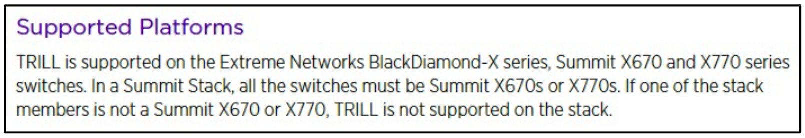
160. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks Summit X770 series switches, including but not limited to the Extreme Networks Summit X770-32q switch (collectively, “the Extreme Networks Summit X770 Switches”).

161. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks EXOS operating system.

162. Extreme Networks makes, uses, sells, offers to sell, and/or imports the Extreme Networks BD-X Switches, the Extreme Networks Summit X670 Switches, the Extreme Networks Summit X770 Switches, and the Extreme Networks EXOS operating system (collectively, "the Extreme Networks '259 Accused Products").

163. Extreme Networks makes, uses, sells, and/or offers to sell networks comprised of the Extreme Networks '259 Accused Products ("an Extreme Networks '259 Accused Product Network").

164. On information and belief, an Extreme Networks '259 Accused Product Network implements at least the TRILL protocol.

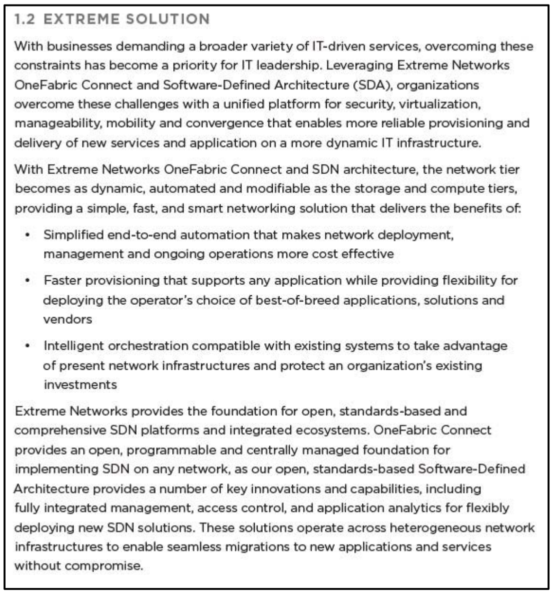


Supported Platforms

TRILL is supported on the Extreme Networks BlackDiamond-X series, Summit X670 and X770 series switches. In a Summit Stack, all the switches must be Summit X670s or X770s. If one of the stack members is not a Summit X670 or X770, TRILL is not supported on the stack.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 13.

165. On information and belief, the Extreme Networks '259 Accused Products perform a method of transporting packets across a network.



1.2 EXTREME SOLUTION

With businesses demanding a broader variety of IT-driven services, overcoming these constraints has become a priority for IT leadership. Leveraging Extreme Networks OneFabric Connect and Software-Defined Architecture (SDA), organizations overcome these challenges with a unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure.

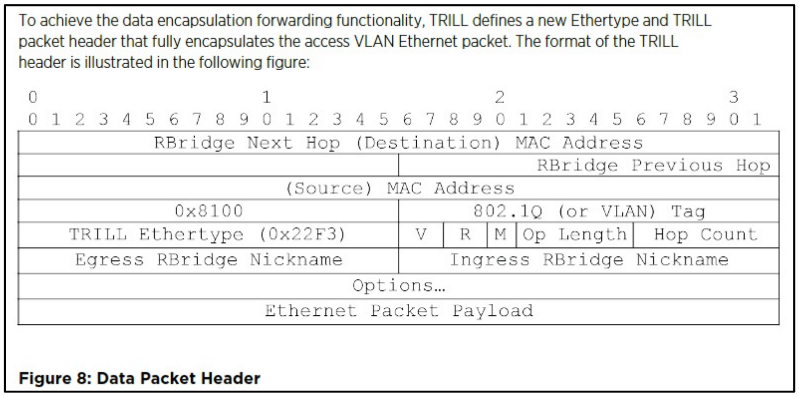
With Extreme Networks OneFabric Connect and SDN architecture, the network tier becomes as dynamic, automated and modifiable as the storage and compute tiers, providing a simple, fast, and smart networking solution that delivers the benefits of:

- Simplified end-to-end automation that makes network deployment, management and ongoing operations more cost effective
- Faster provisioning that supports any application while providing flexibility for deploying the operator's choice of best-of-breed applications, solutions and vendors
- Intelligent orchestration compatible with existing systems to take advantage of present network infrastructures and protect an organization's existing investments

Extreme Networks provides the foundation for open, standards-based and comprehensive SDN platforms and integrated ecosystems. OneFabric Connect provides an open, programmable and centrally managed foundation for implementing SDN on any network, as our open, standards-based Software-Defined Architecture provides a number of key innovations and capabilities, including fully integrated management, access control, and application analytics for flexibly deploying new SDN solutions. These solutions operate across heterogeneous network infrastructures to enable seamless migrations to new applications and services without compromise.

Data Center Solutions Guide, A Solution White Paper, EXTREME NETWORKS TECHNICAL DOCUMENTATION (2014), at 5.

166. On information and belief, the Extreme Networks ’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 TRILL network are encapsulated within a TRILL header, which includes, for example, an Egress RBridge Nickname field that contains the RBridge Nickname of the exit end switch.



To achieve the data encapsulation forwarding functionality, TRILL defines a new Ethertype and TRILL packet header that fully encapsulates the access VLAN Ethernet packet. The format of the TRILL header is illustrated in the following figure:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|          RBridge Next Hop (Destination) MAC Address           |
+-------------------------------+-------------------------------+
|                               |          RBridge Previous Hop |
+-------------------------------+-------------------------------+
|                     (Source) MAC Address                      |
+-------------------------------+-------------------------------+
|            0x8100             |      802.1Q (or VLAN) Tag     |
+-------------------------------+---+---+---+---------+---------+
|      TRILL Ethertype (0x22F3) | V | R | M |Op Length|Hop Count|
+-------------------------------+---+---+---+---------+---------+
|     Egress RBridge Nickname   |    Ingress RBridge Nickname   |
+-------------------------------+-------------------------------+
|                           Options…                            |
+---------------------------------------------------------------+
|                    Ethernet Packet Payload                    |
+---------------------------------------------------------------+
```

Figure 8: Data Packet Header

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 23.

167. On information and belief, the Extreme Networks ’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 TRILL network, the Extreme Networks ’259 Accused Products are grouped into ingress RBridges, intermediate RBridges, and egress RBridges based on whether they are entry switches, core switches, or exit switches.

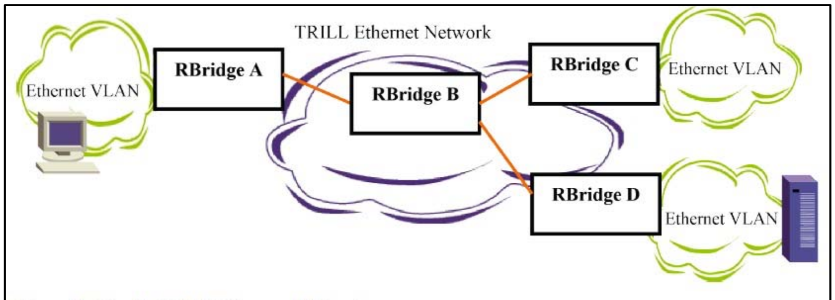
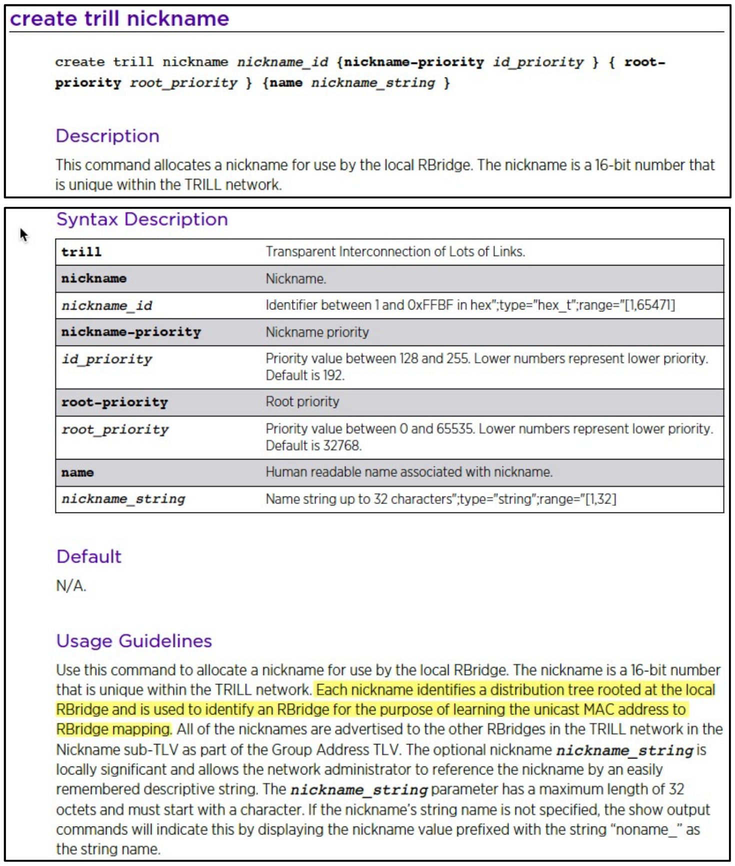


Figure 9: Simple TRILL Reference Network

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 24.

168. On information and belief, the Extreme Networks ’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 RBridge is assigned a unique RBridge Nickname, which includes a nickname priority value and a root priority value that are used in determining the topology of distribution trees within a TRILL 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.



create trill nickname

```
create trill nickname nickname_id {nickname-priority id_priority } { root-
priority root_priority } {name nickname_string }
```

Description

This command allocates a nickname for use by the local RBridge. The nickname is a 16-bit number that is unique within the TRILL network.

Syntax Description

trill	Transparent Interconnection of Lots of Links.
nickname	Nickname.
nickname_id	Identifier between 1 and 0xFFBF in hex";type="hex_t";range="[1,65471]
nickname-priority	Nickname priority
id_priority	Priority value between 128 and 255. Lower numbers represent lower priority. Default is 192.
root-priority	Root priority
root_priority	Priority value between 0 and 65535. Lower numbers represent lower priority. Default is 32768.
name	Human readable name associated with nickname.
nickname_string	Name string up to 32 characters";type="string";range="[1,32]

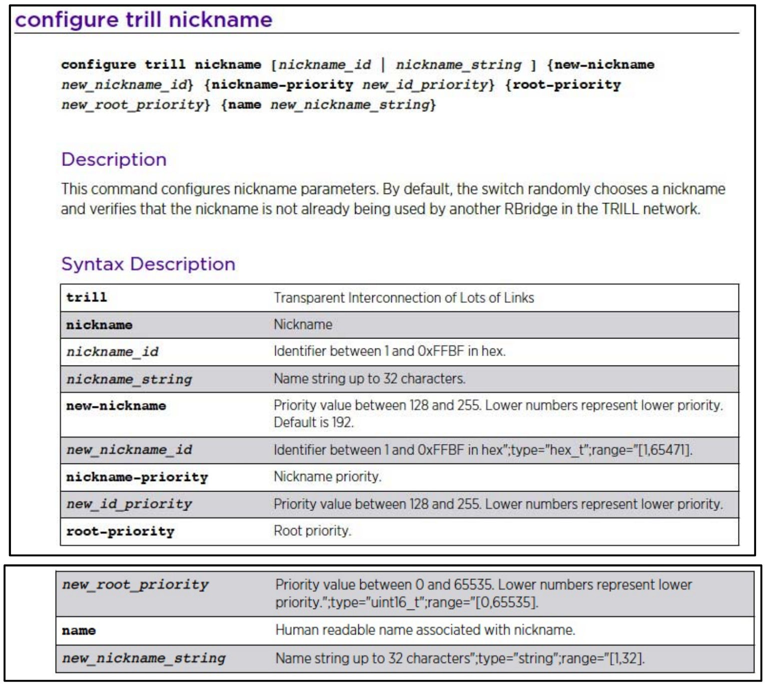
Default

N/A.

Usage Guidelines

Use this command to allocate a nickname for use by the local RBridge. The nickname is a 16-bit number that is unique within the TRILL network. Each nickname identifies a distribution tree rooted at the local RBridge and is used to identify an RBridge for the purpose of learning the unicast MAC address to RBridge mapping. All of the nicknames are advertised to the other RBridges in the TRILL network in the Nickname sub-TLV as part of the Group Address TLV. The optional nickname ***nickname_string*** is locally significant and allows the network administrator to reference the nickname by an easily remembered descriptive string. The ***nickname_string*** parameter has a maximum length of 32 octets and must start with a character. If the nickname's string name is not specified, the show output commands will indicate this by displaying the nickname value prefixed with the string “noname_” as the string name.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 265-66.



configure trill nickname

```
configure trill nickname [nickname_id | nickname_string ] {new-nickname
new_nickname_id} {nickname-priority new_id_priority} {root-priority
new_root_priority} {name new_nickname_string}
```

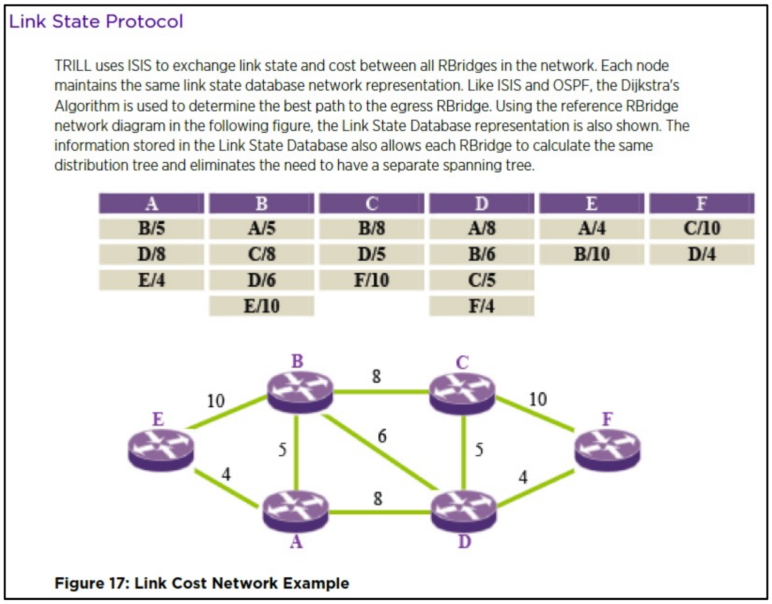
Description

This command configures nickname parameters. By default, the switch randomly chooses a nickname and verifies that the nickname is not already being used by another RBridge in the TRILL network.

Syntax Description

trill	Transparent Interconnection of Lots of Links
nickname	Nickname
nickname_id	Identifier between 1 and 0xFFBF in hex.
nickname_string	Name string up to 32 characters.
new-nickname	Priority value between 128 and 255. Lower numbers represent lower priority. Default is 192.
new_nickname_id	Identifier between 1 and 0xFFBF in hex";type="hex_t";range="[1,65471].
nickname-priority	Nickname priority.
new_id_priority	Priority value between 128 and 255. Lower numbers represent lower priority.
root-priority	Root priority.
new_root_priority	Priority value between 0 and 65535. Lower numbers represent lower priority.";type="uint16_t";range="[0,65535].
name	Human readable name associated with nickname.
new_nickname_string	Name string up to 32 characters";type="string";range="[1,32].

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 237-38.



Link State Protocol

TRILL uses ISIS to exchange link state and cost between all RBridges in the network. Each node maintains the same link state database network representation. Like ISIS and OSPF, the Dijkstra's Algorithm is used to determine the best path to the egress RBridge. Using the reference RBridge network diagram in the following figure, the Link State Database representation is also shown. The information stored in the Link State Database also allows each RBridge to calculate the same distribution tree and eliminates the need to have a separate spanning tree.

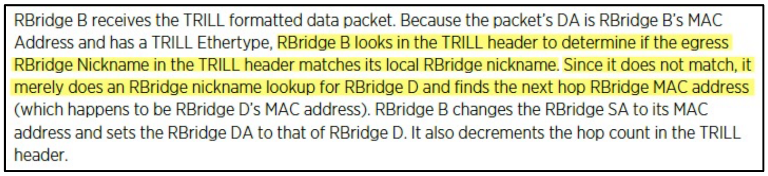
A	B	C	D	E	F
B/5	A/5	B/8	A/8	A/4	C/10
D/8	C/8	D/5	B/6	B/10	D/4
E/4	D/6	F/10	C/5		
	E/10		F/4		

Figure 17: Link Cost Network Example

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 31.

169. On information and belief, the Extreme Networks ’259 Accused Products compare the destination transport identification of a packet with the transport identification of a

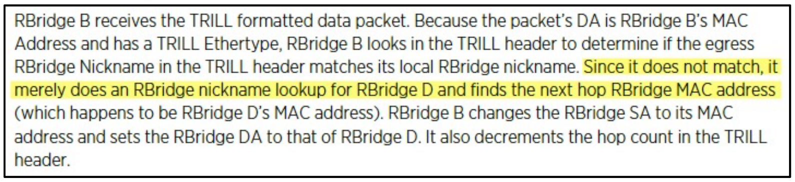
routing switch. For example, data packets entering a TRILL network are encapsulated within a TRILL Header, which includes an Egress RBridge Nickname field that contains the RBridge Nickname of the egress RBridge. Switches running TRILL, such as the Extreme Networks ’259 Accused Products, compare the value in the Egress RBridge Nickname field to values in the switches’ memory.



RBridge B receives the TRILL formatted data packet. Because the packet's DA is RBridge B's MAC Address and has a TRILL Ethertype, RBridge B looks in the TRILL header to determine if the egress RBridge Nickname in the TRILL header matches its local RBridge nickname. Since it does not match, it merely does an RBridge nickname lookup for RBridge D and finds the next hop RBridge MAC address (which happens to be RBridge D's MAC address). RBridge B changes the RBridge SA to its MAC address and sets the RBridge DA to that of RBridge D. It also decrements the hop count in the TRILL header.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 25 (highlighting added).

170. On information and belief, the Extreme Networks ’259 Accused Products forward data packets through a network based on the comparison of destination transport identification. For example, switches running TRILL, such as the Extreme Networks ’259 Accused Products, forward encapsulated data packets using the Egress RBridge Nickname.



RBridge B receives the TRILL formatted data packet. Because the packet's DA is RBridge B's MAC Address and has a TRILL Ethertype, RBridge B looks in the TRILL header to determine if the egress RBridge Nickname in the TRILL header matches its local RBridge nickname. Since it does not match, it merely does an RBridge nickname lookup for RBridge D and finds the next hop RBridge MAC address (which happens to be RBridge D's MAC address). RBridge B changes the RBridge SA to its MAC address and sets the RBridge DA to that of RBridge D. It also decrements the hop count in the TRILL header.

Advanced Features, *ExtremeXOS 15.5 User Guide*, EXTREME NETWORKS TECHNICAL DOCUMENTATION (June 2014), at 25 (highlighting added).

171. By making, using, testing, offering for sale, and/or selling communication network products and services, including but not limited to the Extreme Networks ’259 Accused Products, Extreme Networks 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).

172. On information and belief, Extreme Networks also indirectly infringes the ’259 patent by actively inducing infringement under 35 U.S.C. § 271(b).

173. On information and belief, Extreme Networks 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, Extreme Networks knew of the ’259 patent and knew of its infringement, including by way of this lawsuit.

174. On information and belief, Extreme Networks intended to induce patent infringement by third-party customers and users of the Extreme Networks ’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. Extreme Networks specifically intended and was aware that the normal and customary use of the accused products would infringe the ’259 patent. Extreme Networks 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, Extreme Networks provides the Extreme Networks ’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 Extreme Networks further provides documentation and training materials that cause customers of the Extreme Networks ’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 Extreme Networks ’259 Accused Products, Extreme Networks specifically intended to induce infringement of the ’259 patent, including at least claim 9. On information and belief, Extreme Networks engaged in such inducement to promote the sales of the Extreme Networks ’259 Accused Products and to actively induce its customers to infringe the ’259 patent. Accordingly, Extreme Networks 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.

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

176. As a result of Extreme Networks' infringement of the '259 patent, Dunti has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Extreme Networks' infringement, but in no event less than a reasonable royalty for the use made of the invention by Extreme Networks 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 Extreme Networks has infringed, either literally and/or under the doctrine of equivalents, the '462 patent, the '701 patent, the '235 patent, the '286 patent, and/or the '259 patent;

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

C. A judgment and order requiring Extreme Networks 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 20, 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