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

LIONRA TECHNOLOGIES LIMITED, *Plaintiff,* v. CISCO SYSTEMS, INC., *Defendant.*	Case No. 2:22-cv-305 **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Lionra Technologies Limited ("Lionra") files this complaint against Cisco Systems, Inc. ("Cisco" or "Defendant"), alleging infringement of U.S. Patent Nos. 7,916,630, 8,566,612, 7,921,323, 7,302,708, and 7,685,436 ("Patents-in-Suit"). The Accused Products are computer networking and security products made, used, offered for sale, sold, imported by Defendant in the United States and supplied by Defendant to its customers and integrated into electronic devices sold in the United States.

Plaintiff Lionra and the Patents-in-Suit

1. Plaintiff Lionra is a technology licensing company organized under the laws of Ireland, with its headquarters at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland.

2. Lionra is the owner of U.S. Patent No. 7,916,630, entitled "Monitoring Condition of Network with Distributed Components," which issued March 29, 2011 (the "'630 patent"). A copy of the '630 patent is attached to this complaint as Exhibit 1.

3. Lionra is the owner of U.S. Patent No. 8,566,612, entitled “System and Method for a Secure I/O Interface,” which issued October 2, 2013 (the “’612 patent”). A copy of the ’612 patent is attached to this complaint as Exhibit 2.

4. Lionra is the owner of U.S. Patent No. 7,921,323, entitled “Reconfigurable Communications Infrastructure for ASIC Networks,” which issued November 16, 2006 (the “’323 patent”). A copy of the ’323 patent is attached to this complaint as Exhibit 3.

5. Lionra is the owner of U.S. Patent No. 7,302,708, entitled “Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism,” which issued November 27, 2007 (the “’708 patent”). A copy of the ’708 patent is attached to this complaint as Exhibit 4.

6. Lionra is the owner of U.S. Patent No. 7,685,436, entitled “System and Method for a Secure I/O Interface,” which issued March 23, 2010 (the “’436 patent”). A copy of the ’436 patent is attached to this complaint as Exhibit 5.

Defendant and the Accused Products

7. On information and belief, Defendant Cisco is a California corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco can be served through its registered agent, Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, TX 78701.

8. The Accused Products include firewall products such as the Cisco Firepower 4100 and the Cisco Secure Web Application Firewall, aggregation router products such as the Cisco ASR 901, wireless access points such as the Cisco Catalyst 9100, network switch products such as the Cisco Catalyst 9500.

Jurisdiction and Venue

9. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Cisco in this action because, among other reasons, Cisco has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with the forum state of Texas. Cisco maintains several places of business within the State, including at 2250 East President George Bush Turnpike, Richardson, TX 75082. Cisco 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, making, using, importing, offering for sale, and/or selling products and/or services that infringe the patents-in-suit. Thus, Cisco purposefully availed itself of the benefits of doing business in the State of Texas and the exercise of jurisdiction over Cisco would not offend traditional notions of fair play and substantial justice. Cisco is registered to do business in the State of Texas, and has appointed Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, TX 78701 as its agent for service of process.

11. Venue is proper in this district under 28 U.S.C. §1400(b) and 28 U.S.C. §§ 1391(c). Defendants have regular and established places of business in this district as set forth above.

Count 1 – Claim for infringement of the ’630 patent.

12. Lionra incorporates by reference each of the allegations in paragraphs 1–11 above and further alleges as follows:

13. On March 29, 2011, the United States Patent and Trademark Office issued U.S. Patent No. 7,916,630, entitled “Monitoring Condition of Network with Distributed Components.” Ex. 1.

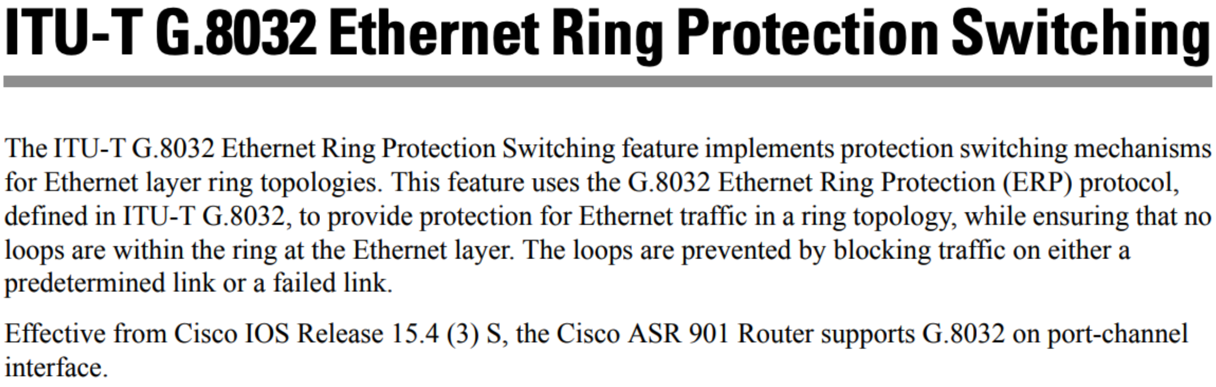
14. Lionra is the owner of the ’630 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

15. Each claim of the ’630 patent is valid, enforceable, and patent-eligible.

16. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’630 patent, and Lionra is entitled to damages for Defendant’s past infringement.

17. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’630 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’630 patent and by inducing others to infringe the claims of the ’630 patent without a license or permission from Lionra. These products include without limitation the Cisco ASR 901 Router, which infringes at least claim 1 of the ’630 patent.

18. On information and belief, the ASR 901 performs a method for monitoring a system condition of a network with distributed components organized in a logical ring structure:



ITU-T G.8032 Ethernet Ring Protection Switching

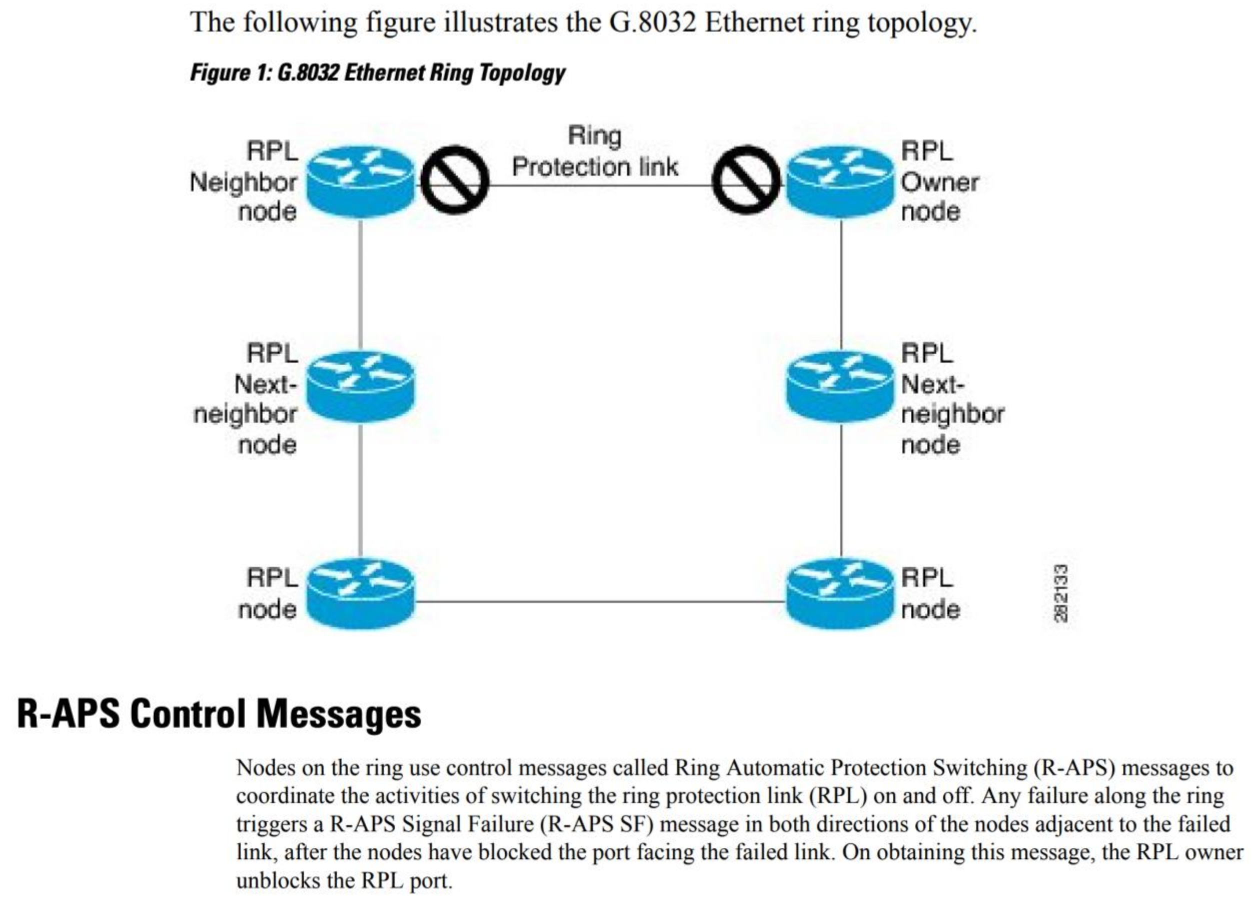
The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

Effective from Cisco IOS Release 15.4 (3) S, the Cisco ASR 901 Router supports G.8032 on port-channel interface.

(https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0111111.pdf at 1.)

19. On information and belief, in the ASR 901 each component in the system monitors only a single respective neighboring component among said distributed components that is a predecessor

or successor of said each component in the logical ring structure to determine a current condition of the respective neighboring component:



The following figure illustrates the G.8032 Ethernet ring topology.

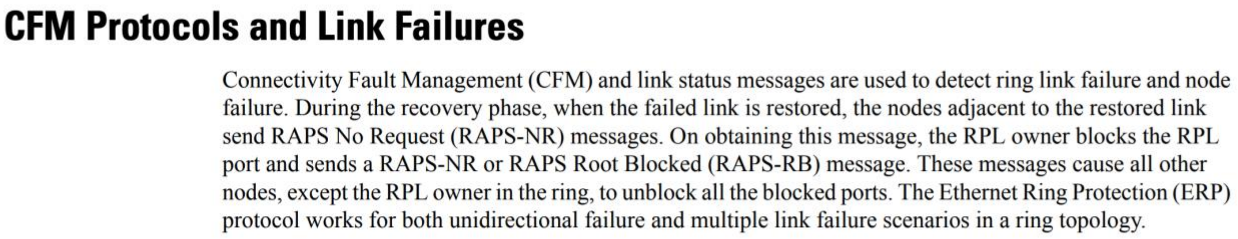
Figure 1: G.8032 Ethernet Ring Topology

R-APS Control Messages

Nodes on the ring use control messages called Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the ring protection link (RPL) on and off. Any failure along the ring triggers a R-APS Signal Failure (R-APS SF) message in both directions of the nodes adjacent to the failed link, after the nodes have blocked the port facing the failed link. On obtaining this message, the RPL owner unblocks the RPL port.

(https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s/b_scg_for_asr901s_chapter_0101011.pdf at 3, 5.)

20. On information and belief, in the ASR 901 each component in the system informs all other components of the system about the current condition of the respective neighboring component when the current condition corresponds to at least one predefined condition:



CFM Protocols and Link Failures

Connectivity Fault Management (CFM) and link status messages are used to detect ring link failure and node failure. During the recovery phase, when the failed link is restored, the nodes adjacent to the restored link send RAPS No Request (RAPS-NR) messages. On obtaining this message, the RPL owner blocks the RPL port and sends a RAPS-NR or RAPS Root Blocked (RAPS-RB) message. These messages cause all other nodes, except the RPL owner in the ring, to unblock all the blocked ports. The Ethernet Ring Protection (ERP) protocol works for both unidirectional failure and multiple link failure scenarios in a ring topology.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**