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

WSOU INVESTMENTS, LLC d/b/a BRAZOS LICENSING AND DEVELOPMENT,	§	
Plaintiff,	§	
v.	§	**CIVIL ACTION NO. 6:20-cv-00891**
HUAWEI TECHNOLOGIES CO., LTD. AND HUAWEI TECHNOLOGIES USA INC.,	§	**JURY TRIAL DEMANDED**
Defendants.	§	

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development ("Brazos" or "Plaintiff"), by and through its attorneys, files this Complaint for Patent Infringement against Defendants Huawei Technologies Co. Ltd. and Huawei Technologies USA Inc. (collectively "Huawei" or "Defendants") and alleges:

NATURE OF THE ACTION

1. This is a civil action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. §§ 1, et seq., including §§ 271, 281, 284, and 285.

THE PARTIES

2. Brazos is a limited liability corporation organized and existing under the laws of Delaware, with its principal place of business at 606 Austin Avenue, Suite 6, Waco, Texas 76701.

3. On information and belief, Defendant Huawei Technologies Co., Ltd. is a Chinese corporation that does business in Texas, directly or through intermediaries, with a principal place of business at Bantian, Longgang District, Shenzhen 518129, People's Republic of China.

4. Upon information and belief, Defendant Huawei Technologies USA Inc. is a corporation organized and existing under the laws of Texas that maintains an established place of business at 2391 NE Interstate 410 Loop, San Antonio, Texas 78217. Huawei Technologies USA, Inc. is authorized to do business in Texas and may be served via its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

5. Defendants operate under and identify with the trade name "Huawei." Each of the Defendants may be referred to individually as a "Huawei Defendant" and, collectively, Defendants may be referred to below as "Huawei" or as the "Huawei Defendants."

JURISDICTION AND VENUE

6. This is an action for patent infringement which arises under the Patent Laws of the United States, in particular, 35 U.S.C. §§271, 281, 284, and 285.

7. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has specific and general personal jurisdiction over each Huawei Defendant pursuant to due process and/or the Texas Long Arm Statute, because each Huawei Defendant has committed acts giving rise to this action within Texas and within this judicial district. The Court's exercise of jurisdiction over each Huawei Defendant would not offend

traditional notions of fair play and substantial justice because Huawei has established minimum contacts with the forum. For example, on information and belief, Huawei Defendants have committed acts of infringement in this judicial district, by among other things, selling and offering for sale products that infringe the asserted patent, directly or through intermediaries, as alleged herein.

9. Venue in the Western District of Texas is proper pursuant to 28 U.S.C. §§1391 and 1400(b) because Defendants have committed acts of infringement in this judicial district and have regular and established places of business in this judicial district and in Texas. As non-limiting examples, on information and belief, Defendants have sold or offered to sell the Accused Products in this judicial district and have employees or agents that operate Huawei equipment in this judicial district, including at 189 CR 265, Georgetown, TX 78626, 1150 S. Bell Blvd., Cedar Park, TX 78613, 1399 S A W Grimes Blvd., Round Rock, TX 78664, 12335 IH 35, Jarrell, TX 76537, 1050 Rabbit Hill Rd., Unit #E, Georgetown, TX 78626, 1602 A W Grimes Blvd., Round Rock, TX 78664, 4120 IH 35 N, Georgetown, TX 78626, 900 CR 272, Leander, TX 78641, 1950 Crystal Falls Pkwy., Leander, TX 78641, 1101 N. Industrial Blvd., Round Rock, TX 78681, 506 McNeil Rd., Round Rock, TX 78681, 3210 Chisholm Trail Rd., Round Rock, TX 78681, 112 Roundville Ln., Round Rock, TX 78664, 202 Central Dr. W, Georgetown, TX 78628, 3595 E. Hwy. 29, Georgetown, TX 78626, 1402 W Welch St., Taylor, TX 76574, 3801 Oak Ridge Dr., Round Rock, TX 78681, 1957 Red Bud Ln. #B, Round Rock, TX 78664, 6603 S Lakewood Dr., Georgetown, TX 78633, 500 W Front, Hutto, TX 78634.

COUNT ONE - INFRINGEMENT OF U.S. PATENT NO. 7,406,260

10. Brazos re-alleges and incorporates by reference the preceding paragraphs of this Complaint.

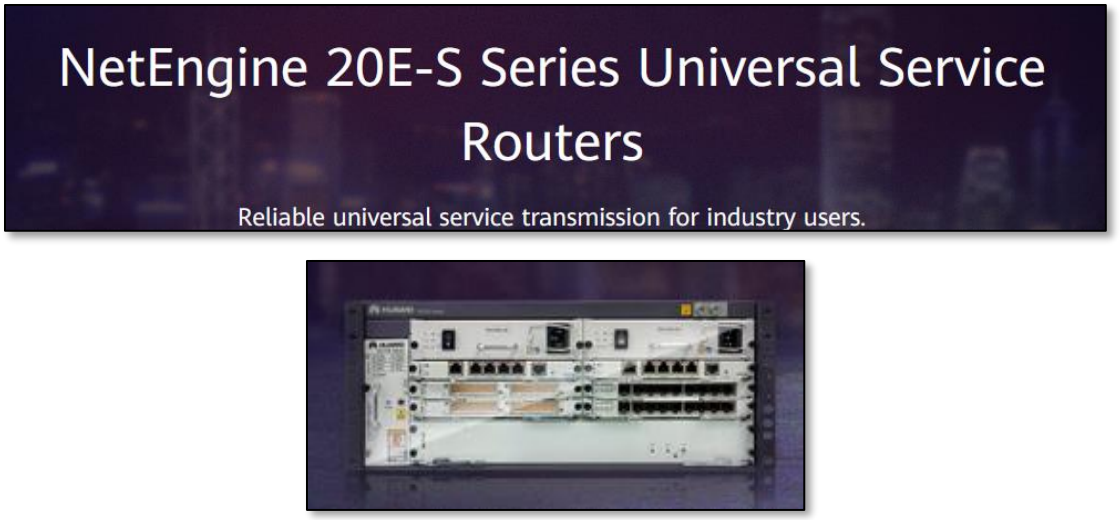
11. On July 29, 2008, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,406,260 ("the '260 Patent"), entitled "Method and system for network wide fault isolation in an optical network." A true and correct copy of the '260 Patent is attached as Exhibit A to this Complaint.

12. Brazos is the owner of all rights, title, and interest in and to the '260 Patent, including the right to assert all causes of action arising under the '260 Patent and the right to any remedies for the infringement of the '260 Patent.

13. Huawei makes, uses, sells, offers for sale, imports, and/or distributes in the United States, including within this judicial district, products such as, but not limited to, Huawei routers with fault management functionality (collectively, the "Accused Products").

14. The Accused Products include Huawei NetEngine 40E series routers.

15. Huawei's NE20E-S routers use the latest VRP8 platform, which is also used by the NE5000E core router. The VRP uses the Resilient Distributed Framework (RDF) with a separated management plane, service plane, data plane, and monitoring module.



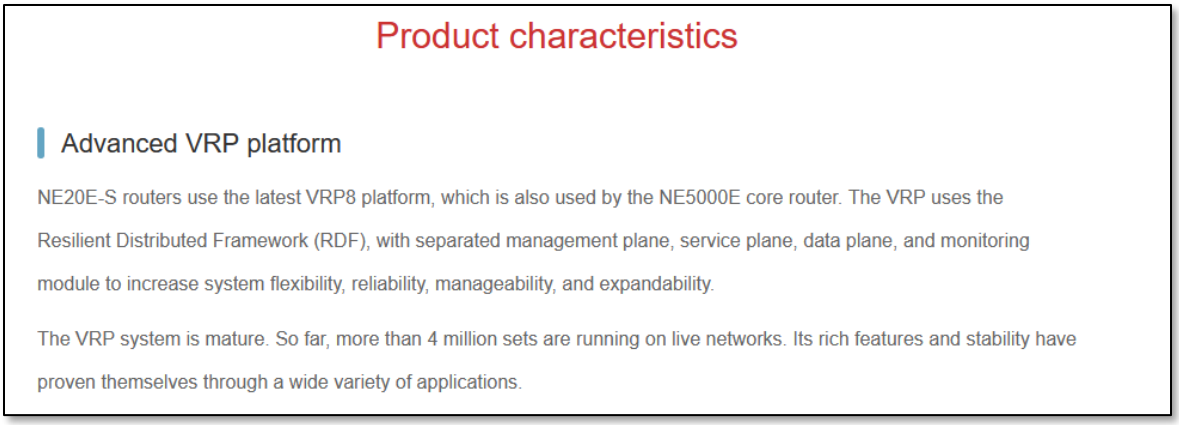
Source: https://e.huawei.com/in/products/enterprise-networking/routers/ne/ne20e-s

NetEngine 20E-S Series

The NetEngine 20E-S series is suitable for enterprise networks of various types and scales. Powered by Huawei's proprietary Network Processing (NP) chips , and packed with innovative technologies — such as Internet Protocol (IP) hard pipe, IP Flow Performance Measurement (FPM), and Bidirectional Forwarding Detection (BFD) — NetEngine 20E-S routers provide high performance transmission, high-quality private line services, and accurate fault detection and location. With 99.999% reliability achieved through comprehensive hardware and software reliability technologies, a Software-Defined Networking (SDN) architecture enables balanced traffic distribution, improving network bandwidth utilization. And with an operating temperate spanning –40°C to 65°C, the NetEngine 20E-S series is designed to withstand even the harshest environments.

Source: https://e.huawei.com/in/products/enterprise-networking/routers/ne/ne20e-s

16. In the Accused Products, the VRP8 platform in the accused instrumentality helps in locating and isolating the fault.



Product characteristics

Advanced VRP platform

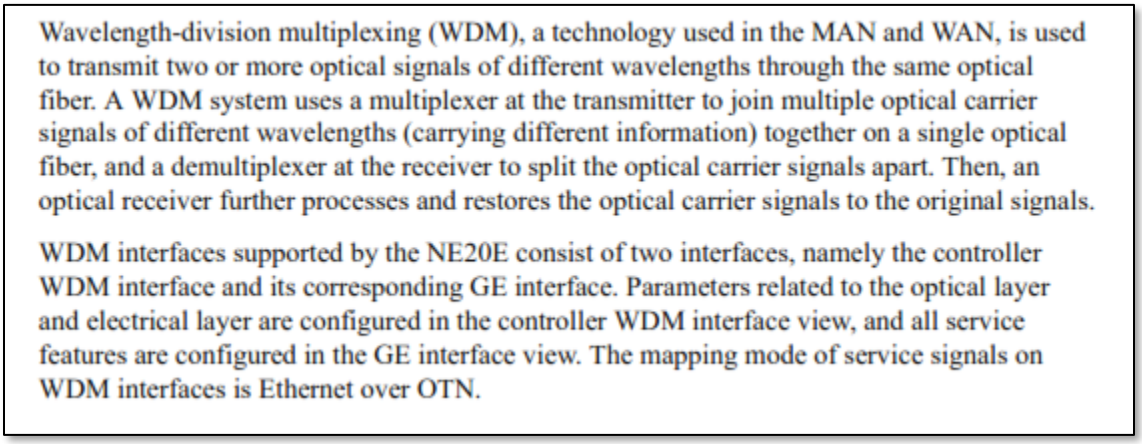
NE20E-S routers use the latest VRP8 platform, which is also used by the NE5000E core router. The VRP uses the Resilient Distributed Framework (RDF), with separated management plane, service plane, data plane, and monitoring module to increase system flexibility, reliability, manageability, and expandability.

The VRP system is mature. So far, more than 4 million sets are running on live networks. Its rich features and stability have proven themselves through a wide variety of applications.

Source: https://e.huawei.com/in/related-page/products/enterprise-network/routers/ne/ne20e-s/brochure/router_ne20e-s

17. The Accused Products support Wavelength-Division Multiplexing (WDM) interfaces. WDM is used to transmit two or more optical signals of different wavelengths through the same optical fiber.

18. The Accused Products have management functions with five major functions – performance management, configuration management, security management, fault management, and charging management. Fault management provides alarms and helps users to isolate and rectify faults.



Wavelength-division multiplexing (WDM), a technology used in the MAN and WAN, is used to transmit two or more optical signals of different wavelengths through the same optical fiber. A WDM system uses a multiplexer at the transmitter to join multiple optical carrier signals of different wavelengths (carrying different information) together on a single optical fiber, and a demultiplexer at the receiver to split the optical carrier signals apart. Then, an optical receiver further processes and restores the optical carrier signals to the original signals.

WDM interfaces supported by the NE20E consist of two interfaces, namely the controller WDM interface and its corresponding GE interface. Parameters related to the optical layer and electrical layer are configured in the controller WDM interface view, and all service features are configured in the GE interface view. The mapping mode of service signals on WDM interfaces is Ethernet over OTN.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

> The fault management function is one of five functions (performance management, configuration management, security management, fault management, and charging management) that make up a telecommunications management network. The primary purposes of this function are to monitor the operating anomalies and problems of devices and networks in real time and to monitor, report, and store data on faults and device running conditions. Fault management also provides alarms, helping users isolate or rectify faults so that affected services can be restored.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

19. The Accused Products have an alarm function that reports alarms whenever a fault is detected in the supported communication network (optical network). The Accused Products also locate and analyze the faults rapidly based on the reported alarms.

20. The VRP8 fault management model in the Accused Products helps in identifying the critical root alarm which is generated based on the fault in the network.

> Alarms are reported if a fault is detected. Classifying, associating, and processing received alarms help keep you informed of the running status of devices and helps you locate and analyze faults rapidly.
>
> Table 1-8 lists the alarm functions supported by the HUAWEI.
>
> **Table 1-8** Alarm functions

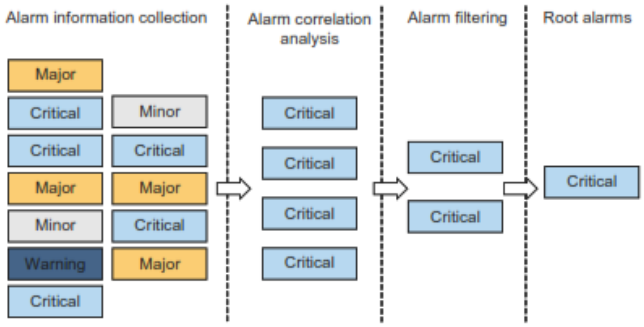
Function	Description
Alarm masking	Maintenance engineers can configure alarm masking on terminals so that terminals detect only alarms that are not masked. This function helps users ignore the alarms that do not need to be displayed.
Alarm suppression	Alarm suppression can be classified as jitter suppression or correlation suppression. ● Jitter suppression: uses alarm continuity analysis to allow the device not to report the alarm if a fault lasts only a short period of time and to display a stable alarm generated if a fault flaps. ● Correlation suppression: uses alarm correlation rules to reduce the number of reported alarms, reducing the network load and facilitating fault locating.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

Fault Management

As shown in **Figure 1-7**, the VRP8 implements fault management based on service objects. The VRP8 creates a service object relationship model to analyze the correlation between alarms, filter out invalid alarms, and report root alarms, speeding up fault identification.

Figure 1-7 VRP8 fault management model



Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

21. The Accused Product includes an internal reliability guarantee mechanism that displays the alarm and helps in locating the fault.

Use of the active alarm table and internal reliability guarantee mechanism allows alarms to be displayed immediately so that faults can be rapidly and correctly located and analyzed.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

22. In the Accused Products, in case of any fault or link down condition, all the circuit cross connects (CCC) are interrupted. This information is reported and used for the analysis of the fault isolation. Accordingly, based upon the information and belief, the accused instrumentality constructs a list of all affected OCh paths in the optical network.

Alarm Correlation Analysis

An event may cause multiple alarms. These alarms are correlated. Alarm correlation analysis facilitates fault locating by differentiating root alarms from correlative alarms.

Alarm correlation analyzes the relationships between alarms based on the predefined alarm correlations. Use the linkDown alarm as an example. If a linkDown alarm is generated on an interface and the link down event results in the interruption of circuit cross connect (CCC) services on the interface, an hwCCCVcDown alarm is generated. According to the predefined alarm correlations, the linkDown alarm is a root alarm, and the hwCCCVcDown alarm is a correlative alarm.

After the system generates an alarm, it analyzes the alarm's correlation with other existing alarms. After the analysis is complete, the alarm carries a tag identifying whether it is a root alarm, a correlative alarm or independent alarm. If the alarm needs to be sent to a Simple Network Management Protocol (SNMP) agent and forwarded to the network management system (NMS), the system determines whether NMS-based correlative alarm suppression is configured.

- If NMS-based correlative alarm suppression is configured, the system filters out correlative alarms and reports only root alarms and independent alarms to the NMS.
- If NMS-based correlative alarm suppression is not configured, the system reports root alarms, correlative alarms and independent alarms to the NMS.

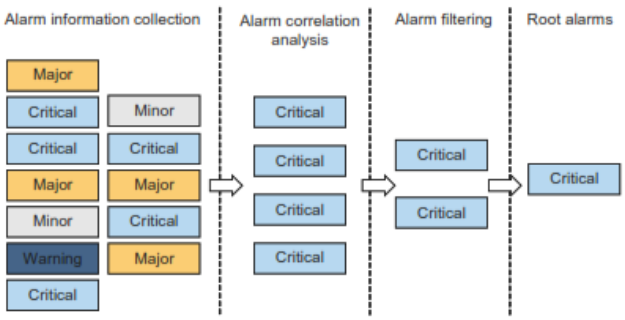
Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

23. In the Accused Products, whenever any fault occurs in the networking link (OCh path), alarms is triggered. In order to analyze and locate the fault, multiple alarms are masked in both the transmit and the receive directions.

Fault Management

As shown in **Figure 1-7**, the VRP8 implements fault management based on service objects. The VRP8 creates a service object relationship model to analyze the correlation between alarms, filter out invalid alarms, and report root alarms, speeding up fault identification.

Figure 1-7 VRP8 fault management model



Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

Alarms are reported if a fault is detected. Classifying, associating, and processing received alarms help keep you informed of the running status of devices and helps you locate and analyze faults rapidly.

Table 1-8 lists the alarm functions supported by the HUAWEI.

Table 1-8 Alarm functions

Function	Description
Alarm masking	Maintenance engineers can configure alarm masking on terminals so that terminals detect only alarms that are not masked. This function helps users ignore the alarms that do not need to be displayed.
Alarm suppression	Alarm suppression can be classified as jitter suppression or correlation suppression. ● Jitter suppression: uses alarm continuity analysis to allow the device not to report the alarm if a fault lasts only a short period of time and to display a stable alarm generated if a fault flaps. ● Correlation suppression: uses alarm correlation rules to reduce the number of reported alarms, reducing the network load and facilitating fault locating.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

24. The Accused Product gathers a list of all the alarms present at any port. A user can configure to receive updates about specific alarm or configure the threshold time after which any alarm should be reported. Reported alarms are of various categories based on the type of fault and the impacted service in the networking element (e.g, OCh alarm, port level alarm, or card level alarm).

Alarm Suppression

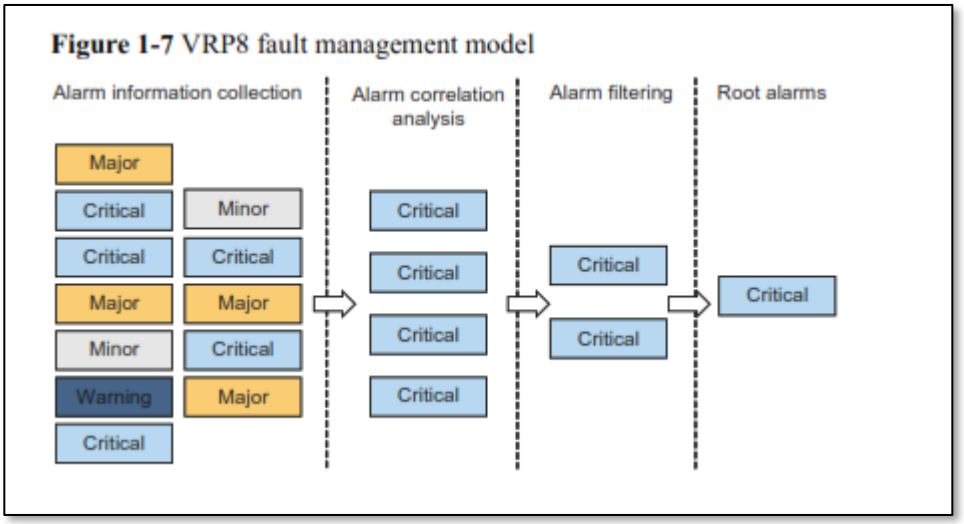
If different types of faults trigger more than one alarm, CFM alarm suppression allows the alarm with the highest level to be sent to the NMS. If alarms persist after the alarm with the highest level is cleared, the alarm with the second highest level is sent to the NMS. The process repeats until all alarms are cleared.

The principles of CFM alarm suppression are as follows:

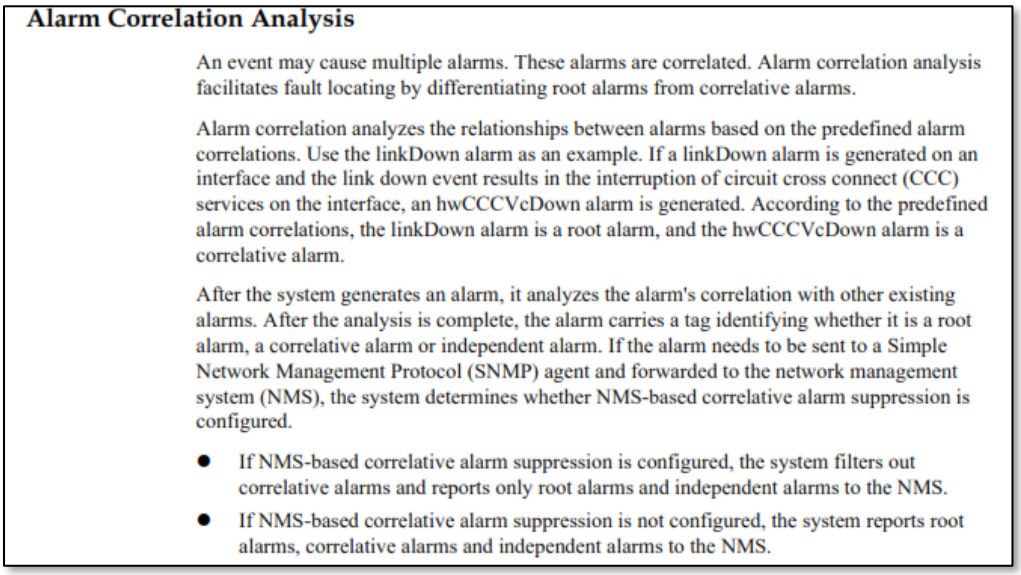
- Alarms with high levels require immediate troubleshooting.
- A single fault may trigger alarms with different levels. After the alarm with the highest level is cleared, alarms with lower levels may also be cleared.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

25. The Accused Products engage in an alarm correlation analysis to determine the correlated alarms and reduce the number of reported alarms. The Accused Products also perform Alarm filtering to report the alarms specified by a user. Once the analysis of the correlated alarms is completed by the Accused Products, information is added to each alarm in order to easily identify the root alarm, correlated alarm, and an independent alarm.



Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003



Alarm Correlation Analysis

An event may cause multiple alarms. These alarms are correlated. Alarm correlation analysis facilitates fault locating by differentiating root alarms from correlative alarms.

Alarm correlation analyzes the relationships between alarms based on the predefined alarm correlations. Use the linkDown alarm as an example. If a linkDown alarm is generated on an interface and the link down event results in the interruption of circuit cross connect (CCC) services on the interface, an hwCCCVcDown alarm is generated. According to the predefined alarm correlations, the linkDown alarm is a root alarm, and the hwCCCVcDown alarm is a correlative alarm.

After the system generates an alarm, it analyzes the alarm's correlation with other existing alarms. After the analysis is complete, the alarm carries a tag identifying whether it is a root alarm, a correlative alarm or independent alarm. If the alarm needs to be sent to a Simple Network Management Protocol (SNMP) agent and forwarded to the network management system (NMS), the system determines whether NMS-based correlative alarm suppression is configured.

- If NMS-based correlative alarm suppression is configured, the system filters out correlative alarms and reports only root alarms and independent alarms to the NMS.
- If NMS-based correlative alarm suppression is not configured, the system reports root alarms, correlative alarms and independent alarms to the NMS.

Source: https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

26. In view of preceding paragraphs, each and every element of at least claim 1 of the ’260 Patent is found in the Accused Products.

27. Huawei has and continues to directly infringe at least one claim of the ’260 Patent, literally or under the doctrine of equivalents, by making, using, selling, offering for sale, importing, and/or distributing the Accused Products in the United States, including within this judicial district, without the authority of Brazos.

28. Huawei has received notice and actual or constructive knowledge of the ’260 Patent since at least the date of service of this Complaint.

29. Since at least the date of service of this Complaint, through its actions, Huawei has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to infringe the ’260 Patent throughout the United States, including within this judicial district, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Examples of such advertising, promoting, and/or instructing include the documents at:

- https://e.huawei.com/in/products/enterprise-networking/routers/ne/ne20e-s
- https://e.huawei.com/in/related-page/products/enterprise-network/routers/ne/ne20e-s/brochure/router_ne20e-s
- https://support.huawei.com/enterprise/en/doc/EDOC1100016465?section=j003

30. Since at least the date of service of this Complaint, through its actions, Huawei has contributed to the infringement of the ’260 Patent by having others sell, offer for sale, or use the Accused Products throughout the United States, including within this judicial district, with knowledge that the Accused Products infringe the ’260 Patent. The Accused Products are especially made or adapted for infringing the ’260 Patent and have no substantial non-infringing

use. For example, in view of the preceding paragraphs, the Accused Products contain functionality which is material to at least one claim of the '260 Patent.

JURY DEMAND

Brazos hereby demands a jury on all issues so triable.

REQUEST FOR RELIEF

WHEREFORE, Brazos respectfully requests that the Court:

(A) Enter judgment that Huawei infringes one or more claims of the '260 Patent literally and/or under the doctrine of equivalents;

(B) Enter judgment that Huawei has induced infringement and continues to induce infringement of one or more claims of the '260 Patent;

(C) Enter judgment that Huawei has contributed to and continues to contribute to the infringement of one or more claims of the '260 Patent;

(D) Award Brazos damages, to be paid by Huawei in an amount adequate to compensate Brazos for such damages, together with pre-judgment and post-judgment interest for the infringement by Huawei of the '260 Patent through the date such judgment is entered in accordance with 35 U.S.C. §284, and increase such award by up to three times the amount found or assessed in accordance with 35 U.S.C. §284;

(E) Declare this case exceptional pursuant to 35 U.S.C. §285; and

(F) Award Brazos its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court.

Dated: September 29, 2020

Respectfully submitted,

/s/ James L. Etheridge

James L. Etheridge
Texas State Bar No. 24059147
Ryan S. Loveless
Texas State Bar No. 24036997
Travis L. Richins
Texas State Bar No. 24061296
Brett A. Mangrum
Texas State Bar No. 24065671
Jeffrey Huang
ETHERIDGE LAW GROUP, PLLC
2600 E. Southlake Blvd., Suite 120 / 324
Southlake, Texas 76092
Telephone: (817) 470-7249
Facsimile: (817) 887-5950
Jim@EtheridgeLaw.com
Ryan@EtheridgeLaw.com
Travis@EtheridgeLaw.com
Brett@EtheridgeLaw.com
JeffH@EtheridgeLaw.com

COUNSEL FOR PLAINTIFF