

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

FILED
U. S. DISTRICT COURT
Eastern District of Texas
FEB 5 2003
DAVID MALAND, CLERK
By
Deputy

CISCO SYSTEMS, INC. AND
CISCO TECHNOLOGY, INC.

Plaintiffs,

v.

HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI AMERICA, INC. AND
FUTUREWEI TECHNOLOGIES, INC.,

Defendants.

CIVIL ACTION NO. 2:03-CV-027 TJW

JURY REQUESTED

CISCO'S MOTION FOR PRELIMINARY INJUNCTION

Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (collectively "Cisco") move for a preliminary injunction to enjoin defendant Huawei Technologies Co., Ltd. ("Huawei Technologies") and its wholly owned U.S. subsidiaries FutureWei Technologies, Inc. ("FutureWei") and Huawei America, Inc. ("Huawei America") (collectively "Huawei") from continuing their wholesale infringement of Cisco's copyrights and misappropriation of Cisco's trade secrets. In an effort to develop and market a "clone" of Cisco's popular network routers, Defendants engaged in a pattern of blatant and systematic copying of Cisco's router technology, including the copyrighted operating system which controls Cisco routers, the innovative user interface by which customers manage Cisco's routers, and the extensive user documentation Cisco has developed to educate customers on the use of its operating system and interface. Defendants have engaged in what amounts to theft of Cisco's intellectual property by misappropriating and copying Cisco's source code, duplicating Cisco's user interface, and plagiarizing extensively from Cisco's user manuals.

Cisco thus seeks a preliminary injunction to enjoin Defendants from selling or distributing in the United States their infringing routers, the operating system for those routers and the infringing copies of Defendants' user manuals. Cisco further seeks a preliminary injunction requiring Defendants to return to Cisco all copies of Cisco's source code which Defendants illegally misappropriated and possess.

I. INTRODUCTION

Cisco has long been a world leader in the development of network routers (computer-like devices that connect one network to another and allow worldwide communication through the Internet). Cisco has developed router technology that is widely viewed as the best in the world. At the heart of its router technology is a computer program for a complex operating system known as the Internetwork Operating System ("IOS") which controls the functions of Cisco's routers. The IOS software implements a distinctive user interface commonly referred to as the Cisco "CLI" or "Command Line Interface," which allows customers to communicate with and operate the Cisco routers. Both IOS and the Cisco CLI are the products of years of investment and creative endeavor by Cisco engineers and represent some of the most valuable technology owned by the company. Cisco also has spent years in developing comprehensive user documentation (such as user manuals) that educate customers on the use of IOS and the Cisco CLI.

Huawei Technologies is a multi-billion dollar company headquartered in mainland China that manufactures and sells telecommunications and network equipment throughout the world. It formed two U.S. subsidiaries to assist in the marketing and sale of its products in the United States: FutureWei located in Plano, Texas and Huawei America located in San Jose, California. Together, the Defendants have offered for sale in the United States a network router, which is marketed under the trade name "Quidway," which they promote as providing the same functionality and performance as Cisco's routers. As Cisco has discovered through months of investigation, however, the Quidway router, its operating system, and the accompanying user documentation are the product of theft of Cisco's intellectual property. The

evidence assembled by Cisco and submitted in support of this Motion establishes a widespread pattern of copyright infringement and trade secret misappropriation.

First, Huawei unlawfully gained access to the source code of Cisco's IOS program, which Cisco maintains as a trade secret, and copied extensively from it in developing the operating system for the Quidway routers. Second, Defendants duplicated Cisco's CLI user interface by copying hundreds of commands from the Cisco CLI, the unique organization of those commands created by Cisco, and even the descriptions or definitions of those commands composed by Cisco. As a result of this extensive copying, Huawei can now approach thousands of Cisco customers worldwide who have been trained on the use of the Cisco CLI and entice them to purchase the infringing Quidway routers by asserting that they will not have to learn a new user interface. Third, having based their own operating system on the stolen IOS source code and having duplicated the copyrighted Cisco CLI interface, Defendants proceeded to copy, in some instances word for word, the format and text of Cisco's user manuals in order to create user documentation that is virtually identical to Cisco's user documentation. Finally, Defendants' pattern of theft and misappropriation includes patent infringement as well. In order to try to achieve Cisco functionality, Huawei has adopted in its Quidway routers patented Cisco processes in violation of no less than five Cisco patents.

The evidence Cisco submits in support of its Motion for a Preliminary Injunction demonstrates clear-cut violations of copyright and trade secret law by Defendants that will result in irreparable harm to Cisco if the injunction is not granted.

- Cisco has strong evidence of Defendants' theft and misappropriation of Cisco's IOS source code. The operating system Huawei embeds in its Quidway routers for sale in the United States and elsewhere is known as the Versatile Routing Platform ("VRP"). After it obtained a Quidway router sold by Huawei in the United States, Cisco analyzed the VRP code and found telltale signs that it was developed using Cisco's source code. For example, the VRP code contains hundreds of lines of textual statements known as "text strings" that are identical – both in their sequence and phrasing – to the text strings originally placed in Cisco's IOS source

code when the IOS program was developed. The presence of these text strings in the VRP code cannot be explained by coincidence or a lawful endeavor. The only logical explanation for their presence in VRP is that the Huawei programmers who wrote the VRP code had Cisco's source code available to them, they copied the source code, and as a consequence the Cisco text strings ended up, like finger prints, in the VRP program. This conclusion also is buttressed by the presence in the VRP code of unique file names and a software "bug" found in the IOS source code. The only plausible explanation for the presence of these file names and bug in VRP is that they were adopted through Huawei's copying of the IOS source code.

- Cisco's CLI is a user interface consisting of hundreds of "commands" (*i.e.*, instructions to the router) organized in an elaborate, carefully designed hierarchy. The user of a Cisco router uses these commands to send instructions to or obtain status information from the router. There are multiple ways to design a user interface for a network router if one engages in independent development, but Huawei has chosen to simply copy the Cisco interface, adopting many of the same commands and organizing them in essentially the same arrangement. The result is that the VRP interface bears a striking similarity to the Cisco interface, enabling Huawei to capitalize on the investments made by thousands of Cisco customers in training their employees on the use of Cisco's CLI.

- Huawei's copying of Cisco's user manuals has been blatant and pervasive. Not only is the format and organization of Cisco's user manuals replicated in the Huawei user manuals, but Huawei lifted whole portions of text out of the Cisco manuals and simply pasted them into the Huawei manuals.

As a result of Defendants' theft of Cisco's intellectual property, Defendants are now attempting to market and sell in the United States Quidway routers that are being promoted as virtual clones of Cisco's routers. To foster the message that Quidway routers are interchangeable with Cisco routers, Defendants have even adopted Cisco's router numbering system and router nomenclature.

Cisco is entitled to an immediate preliminary injunction to enjoin Defendants' unlawful conduct pending final resolution of this case. Unless Defendants are preliminarily enjoined, they will continue to engage in infringing activities and reap the benefits of their infringement and misappropriation. Cisco thus seeks a preliminary injunction enjoining Defendants from selling, offering to sell or distributing in the United States its infringing line of Quidway routers, the VRP operating system for these routers, and the associated user documentation. Cisco further seeks a preliminary injunction requiring Defendants to return to Cisco all versions of the Cisco source code that Defendants, or anyone acting on their behalf, have in their possession or control. Lastly, Cisco asks the Court to impound all Quidway routers, all copies of the VRP operating system, all copies of the VRP user documentation, and all Huawei routers and switches that use the VRP operating system that Defendants have in their possession or control in the United States.

II. STATEMENT OF FACTS AND EVIDENCE

A. Cisco's Router Technology is Protected Under Copyright and Trade Secret Law

Cisco has achieved its widely recognized position of leadership in router technology through a combination of hard work, creative innovation and hundreds of millions of dollars in research and development expenditures. Routers connect one computer network to another and allow information, which is broken down into "packets" of data, to be transmitted between networks locally, regionally and internationally. Routers form the structural backbone of the Internet. *See* Exhibit 1, Declaration of Brian Jacklin ("Jacklin Decl."), ¶¶ 7-8.

One of the key components of its routers is Cisco's IOS operating system, the complex computer program that manages the functions and operations of the routers. IOS is the product of over 15 years of development and programming by hundreds of Cisco engineers. *See* Exhibit 2, Declaration of Charles Giancarlo ("Giancarlo Decl."), ¶ 7. Since the introduction of IOS in the mid-1980s, Cisco continuously has upgraded and improved IOS through multiple releases. It now is a computer program with approximately fifteen million lines of source code.

See Exhibit 3, Declaration of Michel Langlois ("Langlois Decl."), ¶ 3. The IOS software is not only the operating system for Cisco's routers, it also serves as the operating system for many of Cisco's other network products, such as switches and gateways. See *id.*, ¶¶ 3, 5.

Like any computer, a network router must have a "user interface" that allows the user to communicate with the router. In the case of routers, the user typically is the information technology ("IT") manager, the person who manages an organization's network. The user interface gives the IT manager a means of communicating with the router to initially configure it to operate in the network and then manage its operation. The IOS software implements Cisco's proprietary CLI user interface. The CLI is a "command line interface," a type of interface that utilizes textual commands to communicate with the router. Each command corresponds to a function that the router can perform. See Exhibit 1, Jacklin Decl., ¶¶ 9-15.

Cisco's CLI consists of hundreds of commands organized in a carefully designed hierarchy. The commands are structured in this hierarchy so that the input of one command will lead the user to additional commands at a level farther down in the hierarchy. The hierarchy, therefore, consists of multiple levels of commands and subcommands through which the user navigates as he or she is configuring the router to the network or managing its operation. See Exhibit 1, Jacklin Decl., ¶¶ 15-18. Cisco has incurred substantial expense in creating its user interface, which is unique among router vendors throughout the world. Cisco engineers had to compose the commands, the descriptions for the commands to enable the users to understand their function, and textual messages that provide feedback to users. In addition, Cisco engineers had to decide how to arrange and group the commands in the most efficient organization. See Exhibit 3, Langlois Decl., ¶¶ 13-14. There is a wide range of expression available to developers of user interfaces for network routers and other devices and Cisco's CLI interface reflects its own creative choices in designing an interface. See *id.*, ¶¶ 8-28.

To assist its customers in the use of Cisco's IOS and CLI, Cisco has prepared extensive user manuals. See Exhibit 4, Declaration of Brian Adams ("Adams Decl."), ¶¶ 5-23. The manuals, which are maintained on Cisco's website for download by customers, are divided

into two components: Command References and Configuration Guides. *See id.*, ¶¶ 6, 23. The Command Reference describes Cisco's CLI and its individual commands.

Cisco's IOS, CLI and user manuals are protected by both registered copyrights and trade secrets. In this case, Cisco is suing for infringement of its registered copyrights in seven IOS programs: Versions 11.0, 11.1, 11.2, 11.3, 12.0, 12.1, and 12.2. *See Exhibit 5, Declaration of Todd Briggs ("Briggs Decl."), Exhibits L-R.* These registered copyrights protect both the source and object code of the IOS, the Cisco's CLI user interface implemented by IOS, and the corresponding user documentation. In addition, Cisco maintains its IOS source code as a highly guarded trade secret and has gone to great lengths to protect the source code from unauthorized disclosure or dissemination outside the company. *See Exhibit 3, Langlois Decl., ¶ 4.*

B. Defendants Have Recently Begun to Sell and Market Infringing Quidway Routers in the United States

Huawei Technologies is a multi-billion dollar Chinese company that conducts business throughout the world in the manufacture and sale of telecommunications and network equipment. It has established two wholly owned subsidiaries in the United States: FutureWei Technologies which is located in Plano, Texas, and Huawei America which is located in both Plano and San Jose, California. Huawei maintains sales offices in both locations. In addition, Huawei recently opened a research and development facility in Plano, Texas, and is actively recruiting employees for that facility. *See Exhibit 5, Briggs Decl., ¶¶ 4-6.*

Huawei offers for sale a line of network routers under the name Quidway. Huawei has promoted its Quidway routers as operating in a manner very similar to Cisco routers, that is, providing comparable functionality, and even indicating that those trained in the use of Cisco routers do not need further training to operate Huawei products. *See Exhibit 6, Declaration of Scott McElroy ("McElroy Decl."), ¶ 3.* Huawei has even adopted Cisco's product numbering system. *See Exhibit 2, Giancarlo Decl., ¶ 10.* For example, Huawei offers Quidway Series 2600 and 3600 routers to mimic the numbering system for Cisco's Series 2600/3600

routers. See Exhibit 5, Briggs Decl., ¶ 19. The operating system for the Quidway routers is called "Versatile Routing Platform" or "VRP." Just like IOS, VRP implements a user interface that is based on a hierarchy of "commands" to communicate with the router.

Cisco was able to obtain for inspection a Quidway router sold to a customer located in California. See Exhibit 6, McElroy Decl., ¶ 9; Exhibit 5, Briggs Decl., ¶¶ 15-16. The router, a Quidway Series 3600 router, contained the VRP operating system, Version 1.5.6, installed on the router when sold to the customer (Cityware). The router sold to Cityware also came with a CD-ROM of the Quidway user manual, Version 1.5. See Exhibit 1, Jacklin Decl., ¶ 20. Cisco analyzed this router, the installed version of VRP and the user manual. See Exhibit 1, Jacklin Decl., ¶ 20; Exhibit 7, Declaration of Tim Gage ("Gage Decl."), ¶ 12; Exhibit 8, Declaration of David Klausner ("Klausner Decl."), ¶¶ 25, 33, 36. That inspection revealed a massive misappropriation and infringement of Cisco's IOS source code, the Cisco CLI interface and Cisco's user manuals.

C. Defendants Copied Cisco's Source Code

As explained in the declaration of David Klausner, Cisco's computer code expert, source code copying can be uncovered through the examination of "text strings" found in the object code of a computer program. Text strings are a sequence of characters in human readable form (e.g., English phrases) that software programmers compose as they write source code. See Exhibit 8, Klausner Decl., ¶¶ 10-20. A text string provides instructions or feedback to the program user when the program is being operated. The following is an example of one of the many text strings originally written into the IOS source code by Cisco's programmers:

"EIGRP:%s multicast flow blocking cleared"

Depending on the size of a program, there can be thousands of text strings in the source code of a large program. Once all of the source code of a program is written, it will contain distinctive text strings that appear in a prescribed sequence from beginning to end, just as a novel will have distinctive sentences that appear in a certain order. See Exhibit 8, Klausner Decl., ¶ 15. When source code is compiled into object code for execution on a computer, the text

CISCO'S MOTION FOR PRELIMINARY INJUNCTION 8

strings remain in their human readable form. The text strings thus form a record in the object code of the source code from which the object code was compiled. Text strings can be used by computer experts to investigate source code copying when only object code is available for inspection. *See* Exhibit 8, Klausner Decl., ¶¶ 13-14.

The VRP object code contains hundreds of lines of text strings that are identical to text strings written by Cisco programmers in the IOS source code. *See* Exhibit 7, Gage Decl., ¶¶ 16-17; Exhibit 8, Klausner Decl., ¶¶ 27-28. When the Cisco programmers wrote the source code, they composed unique text strings which were imbedded in the source code in a prescribed order. These unique text strings now appear in Huawei's VRP code in the same sequence. *See* Exhibit 7, Gage Decl., ¶¶ 16-17, 23-30; Exhibit 8, Klausner Decl., ¶¶ 27-28. Both Cisco employee Tim Gage and expert David Klausner have documented this finding. In paragraph 16 of his declaration, Mr. Gage lists a sample of some of the text strings found in Version 1.5.6 of VRP and compares them to text strings found in the object code of one of the key modules of Cisco IOS. Not only are the text strings *identical*, but they appear in the *same sequence*. Mr. Klausner came to the same conclusion in his examination. *See* Exhibit 8, Klausner Decl., ¶¶ 27-28. Mr. Klausner's declaration contains a table comparing the text strings from the two computer programs which demonstrate the presence of hundreds and hundreds of Cisco text strings in Huawei's VRP code. *See* Exhibit 8, Klausner Decl., Exhibit B.

Furthermore, Mr. Gage compared the Huawei text strings to the text strings as they were originally written into Cisco's IOS source code. The results of this comparison, which are submitted under seal because of the secret nature of Cisco's source code, confirm the inescapable conclusion that Huawei had access to Cisco's source code and copied it. *See* Exhibit 7, Gage Decl., ¶¶ 19-30 (filed under seal).

There is no explanation for the presence of so many of Cisco's unique text strings in the same sequence in Huawei's code other than that Huawei obtained access to Cisco's source code and copied it. Cisco never disclosed any of its source code to Defendants, nor did it ever authorize anyone else to disclose the source code to Defendants. Cisco has zealously guarded

the secrecy of its source code and would never have condoned the disclosure of it to a competitor like Huawei. According to the Gage and Klausner Declarations, it is inconceivable that Huawei programmers could independently compose hundreds of text strings that are *identical* in phrasing to Cisco's unique text strings and arrange them in *precisely the same order* as they were arranged by Cisco's programmers. See Exhibit 7, Gage Decl., ¶¶ 18, 24, 26, 28, 30; Exhibit 8, Klausner Decl., ¶¶ 30-31. After observing text strings from Cisco's source code in the VRP object code, Mr. Gage concluded that this could only have happened through source code copying. See Exhibit 7, Gage Decl., ¶¶ 17, 22, 46. Mr. Klausner concluded that the odds that these text strings would find their way into the VRP code through coincidence or independent work are nil. See Exhibit 8, Klausner Decl., ¶ 31.

There is other strong evidence indicating Huawei's copying of Cisco's source code. For example, the VRP object code contains unique Cisco file names used in one of the key modules in Cisco's IOS source code known as EIGRP. See Exhibit 7, Gage Decl., ¶¶ 31-36. EIGRP is a proprietary protocol developed by Cisco to improve the efficiency of the process for routing packets from one network to another. See Exhibit 7, Gage Decl., ¶¶ 39-40. The VRP object code contains text strings referring to the file names IGRP2.C, IPIGRP2.C and DUAL.C. IGRP2.C, IPIGRP2.C and DUAL.C are Cisco's internal, non-public naming conventions for EIGRP files that would be known only to individuals intimately familiar with Cisco's source code. See *id.* Furthermore, the VRP program embodies a very unique software "bug" that is found in the Cisco EIGRP source code. See *id.*, ¶ 38. This bug is attributable to an obscure flaw in the way the Cisco IOS source code was written. This same bug is found in Huawei's VRP program. See *id.*, ¶ 44. If Huawei had independently developed its VRP program, there would be no reason for Huawei to have included this bug in its own software. The presence of the bug is another telltale sign that Huawei gained unauthorized access to Cisco's source code and copied it in the development of VRP. See *id.*, ¶ 45.

D. Defendants Copied Cisco's Proprietary CLI

Huawei's VRP program implements a command line interface that utilizes, like IOS, a hierarchy of commands to communicate with the router. Not only did Huawei elect to mimic Cisco's selection of a command line interface but it has copied the structure and details of Cisco's CLI in order to create a clone of the Cisco interface.

Huawei's access to Cisco's CLI is beyond dispute. Because Cisco's CLI can be visually observed during the operation of a Cisco router and is extensively displayed in Cisco's user documentation, Huawei had no difficulty in using the Cisco CLI as a model. Huawei engaged in massive copying of Cisco's CLI, copying hundreds of the commands themselves, the definitions Cisco gives to those commands, and the organization of the commands. Huawei's copying is graphically demonstrated in Exhibit B to the Jacklin Declaration. *See* Exhibit 1, Jacklin Decl., Exhibit B. Exhibit B lists Huawei's VRP commands as they are organized in Huawei's user manual, together with the definition or description of the commands. It compares these commands and their descriptions to the corresponding Cisco commands. Verbatim copying is indicated by yellow highlighting; substantial copying, where minor changes were made, is indicated by blue highlighting. As Mr. Jacklin testifies in his declaration, the conclusion is inescapable that Huawei made no effort to independently develop a user interface. *See* Exhibit 1, Jacklin Decl., ¶ 28.

Given that the VRP interface is a virtual clone of Cisco's CLI, Huawei can now promote its routers to Cisco's customers by telling them that they will not have to learn a new interface. As one Huawei distributor declared, he was "impressed by the ability of a Cisco-trained engineer to take a Huawei product out of the box and use it." *See* Exhibit 5, Briggs Decl., ¶ 18, Exhibit S. By choosing copyright infringement over independent development, Huawei has avoided the time-consuming, expensive and intellectually challenging process of developing its own interface as well as avoiding the expensive process of training potential users in a new interface.

E. Defendants Copied Cisco's User Manuals

The Huawei user manual distributed with Huawei's Quidway router is for the most part a slavish copy of the Cisco user manual. Huawei refers to its manual as the "Command Reference," the same term used by Cisco. Furthermore, Huawei has copied the format and organization of Cisco's Command Reference, organizing the text in almost precisely the same manner in which the text in Cisco's manual is organized. Most notably, Huawei has lifted whole portions of text out of the Cisco manual and inserted it in the Huawei manual as its own. See Exhibit 4, Adams Decl., ¶¶ 24-34; Exhibit 5, Briggs Decl., ¶¶ 11-13, Exhibit K.

The extent of Huawei's copying is graphically reflected in Exhibit K to the Briggs Declaration. This exhibit presents a side-by-side comparison of 64 examples of pages taken from the Huawei manual, Version 1.5, and the corresponding pages of the Cisco Command Reference. See Exhibit 5, Briggs Decl., Exhibit K. Text that Huawei copied verbatim is highlighted in yellow. Minor changes Huawei made to mask the plagiarism, such as changes in capitalization or minor wording changes, are shown in blue. Page after page of yellow highlighting in Exhibit K reveals the pervasive nature of Huawei's copying. Throughout the Huawei user manual there are mistakes that reveal an intent to copy. See Exhibit 4, Adams Decl., ¶¶ 30-33; Exhibit 8, Klausner Decl., ¶¶ 34-36. For example, Huawei adopted a command called "range area" which is simply Cisco's command "area range" in reverse order. See Exhibit 4, Adams Decl., ¶ 33. Huawei's "range area" command has the same description as Cisco's "area range" command. Yet when Huawei copied the command description from the Cisco documentation, its plagiarizer forgot to change the order of the command words so that the Huawei description refers to the "area range command" in describing Huawei's "range area" command. *Id.*

In the fall of 2002, after Huawei sensed that Cisco was prepared to take legal action, Huawei posted a new version of its user manual on its website that removes portions of the copied text relating to Cisco's proprietary protocols. See Exhibit 5, Briggs Decl., ¶ 14. Not only does this version continue to contain plagiarized materials, but by deleting material on

Cisco's proprietary protocols from the manuals, while leaving the implementing capabilities in the software itself, Defendants have attempted to conceal some of the most egregious instances of copying. This version constitutes an implicit acknowledgement of Defendants' wrongful conduct.

III. ARGUMENT

A. Cisco Satisfies Each of the Standards for a Preliminary Injunction

In order to obtain a preliminary injunction to prevent Huawei from continuing on its course of blatant copying, Cisco must demonstrate (1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable injury if the injunction is not issued, (3) that the threatened injury to Cisco outweighs any damage the injunction might cause to the Defendants, and (4) that the injunction will not disserve the public interest. *See DSC Communications Corp. v. DGI Technologies, Inc.*, 81 F.3d 597, 600 (5th Cir. 1996). Cisco has satisfied each of these elements.

B. Cisco is Likely to Succeed on Its Copyright Infringement Claims

To prevail on its claims of copyright infringement, Cisco must prove (1) ownership of a valid copyright and (2) copying of the protected work by the alleged infringer. *See Engineering Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1340 (5th Cir. 1994) ("*Engineering Dynamics I*"), *reh'g denied*, 46 F.3d 408 (5th Cir. 1995) ("*Engineering Dynamics II*"). "A plaintiff establishes ownership by demonstrating that the material is copyrightable and that he complied with the statutory requirements in securing the copyright." *Central Point Software, Inc. v. Nugent*, 903 F. Supp. 1057, 1059 (E.D. Tex. 1995).

Cisco has valid certificates of copyright registration for its IOS computer programs. *See Exhibit 5, Briggs Decl., Exhibits L-R.* Registration of a copyright is *prima facie* evidence of the validity of the copyright and the originality of the work. *See Edmark Industries Sdn. Bhd v. South Asia Int'l (H.K.) Ltd.*, 89 F. Supp.2d 840, 844 (E.D. Tex. 2000). Cisco's registrations cover the computer code in the programs, both its object and source code; the CLI user interface implemented by the code, including the screen displays which manifest the CLI;

and the user documentation associated with programs. According to guidelines published by the U.S. Copyright Office, a single registration for a computer program is sufficient to protect not only the code itself, but the screen displays generated by the code (*i.e.*, the user interface) and the user documentation. See U.S. Copyright Office, Circular 61, at 2-3. Indeed, the Copyright Office expressly encourages owners of computer programs to use a single registration to protect code and screen displays.¹

To prove copying of its protected works, Cisco must establish that Defendants had access to the copyrighted works and that the accused works are “substantially similar” to the copyrighted works. See *Engineering Dynamics I*, 26 F.3d at 1341. While substantial similarity must be measured by comparing the products as a whole, “the more exact a duplication of constituent pieces of a work the less overall similarity that may be required.” *Engineering Dynamics II*, 43 F.3d at 410 (citing *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 548 (1985) (finding that 300 words copied from plaintiff’s 450-page book constituted infringement)).

The evidence in this case is overwhelming that Huawei has infringed Cisco’s copyrights by making unauthorized copies of (1) Cisco’s source code, (2) Cisco’s CLI, and (3) Cisco’s user documentation.

1. **Source Code Copying**

The copyright laws protect Cisco’s IOS source code from copying. See *Engineering Dynamics I*, 26 F.3d at 1341; see also *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1249 (3rd Cir. 1983) (“Thus a computer program, whether in object code or source code,... is protected from unauthorized copying”). Cisco’s inspection of the Huawei VRP operating system reveals conclusive evidence that Huawei had access to Cisco’s source code and copied it in connection with the development of VRP. In addressing the incriminating

¹ “The Copyright Office has consistently believed that a single registration is sufficient to protect the copyright in a computer program and related screen displays, including video games, without a separate registration for the screen displays or a specific reference to them on the application for the computer program.” U.S. Copyright Office Circular 61, p. 3.

presence of hundreds of unique Cisco text strings in the VRP object code, Mr. Klausner concludes that this evidence rules out independent development by Huawei:

It is highly improbable, if not impossible, that a Huawei programmer independently created identical source code text strings to those found in Cisco's source code. Many of the text strings which are identical are so unique in their phrasing that it is inconceivable that they could coincidentally have been created by two sets of programmers working independently.

Exhibit 8, Klausner Decl., ¶ 30.

Mr. Gage, who had the opportunity to compare the text strings found in VRP with the text strings originally written into the IOS source code, concluded that his comparison presents "overwhelming evidence of source code copying. . . ." See Exhibit 7, Gage Decl., ¶28. His conclusion is buttressed by the presence in Huawei's VRP object code of unique Cisco source code file names that have never been publicly disclosed. The only logical explanation for the presence of these file names in Huawei's object code is that Huawei copied these source code files from Cisco's. See Exhibit 7, Gage Decl., ¶ 36. Similarly, the presence of a unique Cisco software bug in the Huawei code is even more evidence that Huawei copied Cisco's source code. See Exhibit 7, Gage Decl., ¶¶ 45-46. The bug in question is so rare and complex in its nature that it is inconceivable that Huawei programmers, working independently and without reference to Cisco's source code, could erroneously create the same bug in the VRP code. See *Engineering Dynamics, Inc. v. Structural Software, Inc.*, 785 F. Supp. 576, 583 (E.D. La. 1991) (stating that "one of the most significant evidences of copying is the copying of errors"); see also *United Telephone Company of Missouri v. Johnson Publishing Co., Inc.*, 671 F. Supp. 1514, 1521 (W.D. Mo. 1987) (same); *Financial Information, Inc. v. Moody's Investors Servs., Inc.*, 599 F. Supp. 994, 996 n.3 (S.D.N.Y. 1983) (same). The presence of so many similarities that cannot be explained by coincidence or independent development is compelling evidence that Huawei engaged in literal copying of Cisco's IOS code. See *Tradescape.com v. Shivaram*, 77 F. Supp.2d 408, 417-18 (S.D.N.Y. 1999) (finding that multiple similarities between two computer programs

which had no innocent explanation was evidence of literal copying and supported grant of preliminary injunction).

Even though Cisco does not yet know the precise means by which Huawei obtained access to Cisco's source code, the glaring similarities involving the text strings, file names and the software bug are so striking that they lead inescapably to the conclusion that Huawei had access to Cisco's source code. The "striking similarity" doctrine adopted by the Fifth Circuit holds that if two works are so strikingly similar as to preclude the possibility of independent creation, copying may be proved without a showing of access. *See Peel & Co., Inc. v. The Rug Market*, 238 F.3d 391, 395 (5th Cir. 2001); *see also Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543, 551 (N.D. Tex. 1997). The striking similarity between the VRP object code and the Cisco code for comparable functions precludes any possibility that this portion of VRP was independently developed.

Based on the overwhelming evidence that Huawei copied Cisco's source code in the development of VRP, Cisco is entitled to a preliminary injunction enjoining Defendants from using, distributing, selling, reproducing or continuing to profit from the infringing VRP program. *See Control Data Systems, Inc. v. Infoware, Inc.*, 903 F. Supp. 1316, 1326-27 (D. Minn. 1995) (granting preliminary injunction which enjoined defendant from licensing, selling, distributing, or otherwise marketing computer program copied from plaintiff's source code).

Cisco further is entitled to a preliminary injunction enjoining Defendants from selling, offering to sell, distributing or otherwise using Quidway routers or other Huawei routers that utilize VRP as the operating system. The evidence establishes conclusively that Huawei sells its Quidway and other VRP-controlled routers with the VRP program pre-installed on the router. *See Exhibit 1, Jacklin Decl.*, ¶ 20. The routers therefore are infringing articles as well.

2. Copying of the Cisco CLI

It is well-established that copyright law protects the user interface of a computer program. "Most courts confronted with the issue have determined that copyright protection extends not only to the literal elements of a program, *i.e.*, its source code and object code, but

also to its ‘non-literal’ elements, such as the program architecture, ‘structure, sequence and organization’, operational modules, and *computer-user interface*.” *Engineering Dynamics I*, 26 F.3d at 1341 (emphasis added); *see also Kepner-Tregoe, Inc. v. Leadership Software, Inc.*, 12 F.3d 527, 536 n.20, (5th Cir. 1994) (Fifth Circuit decision embracing “the general, non-controversial proposition that non-literal aspects of copyrighted works – like structure, sequence, and organization – *may* be protected under copyright law: a proposition that has been approved by Supreme Court precedent.”)

In *Engineering Dynamics I*, the Fifth Circuit examined a claim of infringement of “input-output formats” that comprised the user interface of a computer program designed to solve structural engineering problems. *Engineering Dynamics I*, 26 F.3d at 1338. The input-output formats were used to input information regarding building stresses and to view the resulting calculations. *Id.* at 1338-39. Defendant copied many of plaintiff’s input-output formats in order to sell a competing program to plaintiff’s customers without having to re-train them in the use of a new user interface. *Id.* at 1339. The Fifth Circuit rejected the defendant’s argument that the input-output formats were not copyrightable because they were utilitarian, unoriginal or mere ideas. *Id.* at 1342-47.²

Cisco’s CLI interface is a substantially more expressive work than the input-output formats that the Fifth Circuit reviewed in the *Engineering Dynamics* case. *See* Exhibit 3, Langlois Decl., ¶¶ 8-28 (describing the extensive creative effort in designing Cisco’s CLI). In designing its CLI, Cisco engineers faced many decisions and had many choices about the expressive elements of the interface. Not only did they have to decide whether to pursue a command line interface or some other alternative, they had to compose hundreds of different commands and command descriptions. The resulting work is a highly expressive work that is entitled to strong copyright protection under Fifth Circuit precedent.

² The Fifth Circuit remanded the case to the trial court for further proceedings on whether the input-output formats were dictated by industry standards. *Engineering Dynamics I*, 26 F.3d at 1346-47. There was no subsequent trial court ruling on this issue.

Based on the comparison presented of the VRP user interface with Cisco's CLI, there can be no question that Huawei has engaged in calculated, extensive copying of Cisco's interface in an attempt to create an interface for its own Quidway routers that replicates Cisco's CLI. The copying extends to all components of Cisco's CLI: the commands themselves, the descriptions Cisco gives to the commands, and the hierarchical structure of the commands. Huawei's copying of Cisco's CLI is neither *de minimus* nor inadvertent. The extent of the copying belies any claim that Huawei engaged in independent development.

3. User Manual Copying

Cisco's user manuals are protected under the copyright laws. *See Engineering Dynamics I*, 26 F.3d at 1339 (describing plaintiff's copyrights in its user manuals). As demonstrated in Exhibit K to the Briggs Declaration, the evidence is incontrovertible that Huawei has engaged in the copying of Cisco's Command Reference user manual. *See Exhibit 5, Briggs Decl., Exhibit K.* Huawei not only replicated the organization and layout of Cisco's manuals but lifted whole portions of text directly from the Cisco manuals and inserted them into Huawei's manuals. Even where Huawei attempted to make minor changes to mask its copying, it only succeeded in creating more incriminating evidence of its intent. *See Exhibit 8, Klausner Decl., ¶ 36.* For example, Huawei changed Cisco command "IPX maximum-paths" to "IPX max-paths." *See Exhibit 4, Adams Decl., ¶ 32.* Yet, Huawei's copying of the Cisco command reference was so slavish that Huawei copied Cisco's description of its command, with the reference to "IPX maximum-paths," without regard to the fact that it had made a cosmetic change to the command name. Thus, Huawei's command reference purports to describe the "IPX max-paths" command but mistakenly refers to it as the "IPX maximum-paths" command. *Id.*

The minor changes Huawei made to the Cisco text, in a sea of otherwise verbatim copying, is evidence of an incriminating intent. "[T]he existence of only minor differences may itself suggest copying, indicating that the infringer attempted to avoid liability by contributing only trivial variations." *Concrete Machinery Co., Inc. v. Classic Lawn Ornaments, Inc.*, 843 F. CISCO'S MOTION FOR PRELIMINARY INJUNCTION

2d 600, 608 (1st Cir. 1988); see also *Flomerics Ltd. v. Fluid Dynamics Int'l, Inc.*, 880 F. Supp. 60, 62 (D. Mass. 1995) (preliminary injunction entered to enjoin infringement of computer user manual where the copying was “so blatant it repeats verbatim phrases, and even an algebraic error, found in the Flotherm manual”). As the Fifth Circuit has previously stated, “Infringement is not confined to exact reproduction but includes colorable alterations made to disguise the piracy.” *Tennessee Fabricating Co. v. Moultrie Mfg. Co.*, 421 F.2d 279, 284 (5th Cir. 1970).

Moreover, Huawei’s slavish copying of Cisco’s copyrighted user manuals exposes an underlying disregard for intellectual property rights that pervades Defendants’ conduct. Defendants’ violations of Cisco’s rights extend to all aspects of Cisco’s router technology. That Defendants are now engaging in efforts to cover up their infringements, by removing their user manuals from their website, only adds to the mountain of evidence of a pattern of misconduct.

C. Cisco is Likely to Prevail on Its Trade Secret Misappropriation Claim

Cisco’s IOS source code, which has been the subject of reasonable steps to protect it from public disclosure or dissemination to unauthorized parties, is entitled to trade secret protection. See *Transdes Corp. v. Guy F. Atkinson Company*, 996 F.2d 655, 663 (4th Cir. 1993) (“source code can and does qualify as a trade secret”); see also *Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772, 784 (5th Cir. 1999) (identifying elements of trade secret misappropriation under Texas law as (a) existence of a trade secret, (b) acquisition of a trade secret through improper means, and (c) use of a trade secret without authorization). As discussed above, the presence of an extensive number of Cisco’s text strings, non-public file names and a software bug in the Huawei VRP software cannot be logically or credibly explained by independent development or coincidence. The programmers who produced the VRP program, or at least key portions of it, had to have available to them Cisco’s related source code. Cisco has never made that source code publicly available. Nor has Cisco ever provided that source code to Huawei or anyone acting on Huawei’s behalf. Cisco has zealously guarded its source code as a trade secret and has taken reasonable steps to protect its secrecy.

While Cisco does not yet know the particular means by which Huawei obtained access to Cisco's source code, Cisco does know that its possession by Huawei was unauthorized. Technology and software companies universally recognize computer source code as highly confidential. When Huawei copied Cisco's source code, it had to know that it was violating Cisco's legal rights. Even now, Defendants are exhibiting by their conduct an admission of guilt. As established in the declaration of Scott McElroy, Huawei representatives are now attempting to retrieve Quidway routers and VRP programs distributed in the United States, asserting that they will be replaced and "deported" out of the United States. See Exhibit 6, McElroy Decl., ¶¶ 10-11. Not only do these actions threaten a destruction of relevant evidence, which is addressed in Cisco's separate Motion to Preserve Evidence, but they speak volumes about Defendants' awareness of their wrongdoing.

D. Cisco Faces Irreparable Injury if the Injunction is Not Issued

If a preliminary injunction is not issued, Cisco faces a serious threat of irreparable injury. Huawei is now offering for sale and selling in the United States and throughout the world network routers that were built on the basis of a massive misappropriation of Cisco's intellectual property. Utilizing the fruits of this misappropriation, Defendants are now approaching Cisco's customers with a "same as Cisco" marketing program so that they can enjoy the fruits of Cisco's technology development program without paying for it. See Exhibit 2, Giancarlo Decl., ¶ 15.

By copying Cisco's technology, Defendants can "free ride" on Cisco's technological development and customer training. See Exhibit 2, Giancarlo Decl., ¶¶ 12-15. By copying from Cisco, Huawei avoided the expense and technological challenge of developing its own operating system, user interface and user documentation. Allowing Defendants to compete against Cisco based on technology stolen from Cisco will cause Cisco irreparable injury. As the District Court held in *DSC Communications Corp. v. DGI Technologies, Inc.*, 898 F. Supp. 1183, 1195 (N.D. Tex. 1995), the copying of operating system software establishes irreparable injury because the infringer gains an unfair advantage by avoiding the expense of independent development. "These operating system software programs are an important part of DSC's

business. If DGI continues to use this software, it will be gaining an unjust advantage, the advantage of using the time and expertise DSC expended developing the copyrighted material.”

Id.

Moreover, there is compelling evidence that Cisco’s highly valuable source code is now in the possession of Defendants who can undermine the value of that source code by continuing to use it or disclose it to others. By copying the source code, Cisco’s CLI and Cisco’s user manuals, Defendants have deprived Cisco of the exclusivity and control to which Cisco is entitled under the copyright laws. Courts regularly recognize such loss of exclusivity as irreparable injury warranting the issue of injunctive relief. As the court noted in *DSC Communications*, the owner of a copyrighted software program suffers irreparable injury from infringement through the loss of its ability to control the use and dissemination of its work.

DSC loses physical control of its software and its software copyright rights when an unlicensed user has a copy of that software. If the Court were to allow DGI to continue to possess these unauthorized copies, there is nothing to prevent DGI from disclosing the operating system software to other parties.

DSC Communications, 898 F. Supp. at 1195.

E. The Threatened Injury to Cisco Far Outweighs Any Injury to Huawei from Issuance of the Injunction

The threatened injury to Cisco clearly outweighs any harm to Defendants. First, Defendants cannot be heard to complain that a preliminary injunction correcting the pattern of infringement they have engaged in will hurt their business. They were not entitled in the first place to structure their business around the theft of Cisco’s technology. “[E]ven assuming the injunction would have a . . . devastating effect . . . a knowing infringer cannot be permitted to construct its business around its infringement.” *Autoskill Inc. v. National Education Support System, Inc.*, 994 F.2d 1476, 1498 (10th Cir. 1993); *accord Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1255 (3rd Cir. 1983).

Second, the irreparable injury Cisco faces if a preliminary injunction is not granted far outweighs any injury to Defendants if their infringement is enjoined. Cisco’s IOS

operating system and its CLI user interface are invaluable components of Cisco's business. The IOS operating system not only runs Cisco's routers, it also is the operating system for many of Cisco's other network products, such as switches and gateways. If a preliminary injunction is not issued, and Defendants are permitted to continue to distribute their routers, software and user manuals that are the fruits of illicit copying, Cisco will suffer the loss of an important technological advantage it created through many years of work and investment.

The injury Huawei will suffer if it is enjoined from distributing infringing products in the United States pales in comparison to the injury to Cisco. Huawei is a multi-billion dollar corporation with many product lines in the telecommunications area. A preliminary injunction against the distribution and sale of Quidway routers, the VRP operating system and the Quidway user manuals will not threaten the viability of Huawei. Moreover, Defendants are now attempting to "recall" and replace their Quidway routers with other products. *See* Exhibit 6, McElroy Decl., ¶¶ 10-11. Defendants apparently recognize that they have no legal right to distribute and sell the infringing Quidway routers in the United States. A preliminary injunction implementing a prohibition against the distribution and sale of Quidway routers in the United States will cause little, if any, harm to Defendants in light of the steps that they have already taken to remove the routers that have already been sold.

F. The Issuance of Preliminary Injunction Would Further the Public Interest

This is a case in which a large corporation has acted in blatant disregard of United States copyright and trade secret laws. Huawei misappropriated whatever it needed to in order to bring to market a Cisco "clone" without incurring the substantial expense of independent development or even attempting to avoid Cisco's intellectual property. One cannot imagine a more compelling case in which enforcement of United States intellectual property laws would serve the public interest. *See DSC Communications Corp. v. DGI Technologies, Inc.*, 898 F. Supp. at 1196 ("The Court finds as a matter of law that the injunction would serve the public interest by preserving the integrity of copyright laws which encourage individual effort and creativity by granting valuable enforceable rights."). Indeed, Cisco submits that it would be a

CISCO'S MOTION FOR PRELIMINARY INJUNCTION

major disservice to the public interest if a preliminary injunction were not issued, thereby allowing Huawei to continue to profit from the blatant copying that has occurred.

G. Defendants' Infringing Products Should be Impounded Pursuant to 17 U.S.C. § 503(a)

The Copyright Act authorizes a court to order the impoundment of infringing products or materials. *See* 17 U.S.C. § 503(a). In determining whether to impound allegedly infringing materials, district courts have applied the same standards that govern requests for preliminary injunctive relief. *See, e.g., Columbia Pictures Indus., Inc. v. Jasso*, 927 F. Supp. 1075, 1076 (N.D. Ill. 1996); *WPOW, Inc. v. MRLJ Enterprises*, 584 F. Supp. 132, 135 (D.D.C. 1984). Impoundment pursuant to 17 U.S.C. § 503(a) is particularly appropriate when there is a risk that Defendants "will attempt to destroy, remove or hide" allegedly infringing material. *See Columbia*, 927 F. Supp. at 1077.

In light of the compelling evidence against Defendants, and the evidence that Defendants are attempting to "deport" infringing Quidway routers and software from the United States, Cisco seeks an impoundment order pursuant to Section 503(a) of the Copyright Act. Cisco seeks an order requiring Defendants to turn over to Cisco, for impoundment in a secure facility, all Quidway routers, VRP source code and Quidway user manuals now or hereafter in the possession of Defendants in the United States, pending final resolution of this action. Defendants' blatant infringement of Cisco's rights, and their attempts to move evidence out of the country, justify the issuance of such an impoundment order. *See Yamate USA Corp. v. Sugerman*, 20 U.S.P.Q.2d 1590, 1600 (D.N.J. 1991) (granting request for impoundment order because plaintiff demonstrated entitlement to a preliminary injunction).

H. Bond

In order to obtain a preliminary injunction, Cisco recognizes it must post an appropriate bond. *See* Fed. R. Civ. P. 65(c) (stating that "[n]o . . . preliminary injunction shall issue except upon the giving of security by the applicant, in such sum as the court deems proper, for the payment of such costs and damages as may be incurred or suffered by any party who is

found to have been wrongfully enjoined or restrained”); *see also Phillips v. Chas. Schreiner Bank*, 894 F.2d 127, 131 (5th Cir. 1990). To the extent that a bond may be required for the return of Cisco’s stolen source code and any object code derived therefrom, a *de minimus* amount is appropriate because Cisco seeks only the return of stolen property. Huawei has no right to possess Cisco’s source code in the first place. As to the amount of bond appropriate for the prohibition against Defendants’ sales and distribution of infringing items in the United States, the Court should consider that Defendants already are attempting to remove infringing products. *See Exhibit 6, McElroy Decl.*, ¶¶ 10, 11. Given that Defendants only recently began to sell Quidway routers in the United States and given their efforts to retrieve sold routers, Cisco submits that a bond of \$50,000 is appropriate.

IV. CONCLUSION

Cisco’s evidence establishes conclusively that Defendants engaged in a systematic pattern of copying Cisco’s computer programs, user interface and user documentation in order to unfairly gain the benefit of Cisco’s years of work and innovation. Cisco is entitled to a preliminary injunction to enjoin Defendants from continuing their acts of infringement, and from profiting from their infringement to date, pending a trial on the merits. The preliminary injunction should:

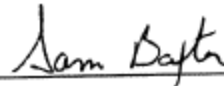
(a) enjoin Defendants, and all persons and entities in concert with them, from importing, exporting, selling, offering for sale, distributing, reproducing or using in the United States its Quidway line of routers, the VRP operating system, the VRP user documentation, or any router or switch that uses VRP;

(b) require Defendants to return to Cisco all copies of all versions of Cisco’s source code and any version of object code compiled from such source code; and

(c) require Defendants to deliver to Cisco, for impoundment, all Quidway routers, all copies of the VRP operating system, all copies of the VRP user documentation, and all Huawei routers and switches that use the VRP operating system that are in Defendants’ possession or control in the United States or subsequently come into their possession or control.

Dated: February 5, 2003

Respectfully submitted,



Sam F. Baxter
Attorney-In-Charge for Plaintiff
State Bar No. 01938000

McKool Smith, P.C.
P.O. Box O
505 East Travis Street, Suite 105
Marshall, TX 75670
Telephone: (903) 927-2111
Facsimile: (903) 927-2622

Jeffrey R. Bragalone
State Bar No. 02885775

McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone (214) 978-4000
Facsimile: (214)978-4044

OF COUNSEL:

ORRICK, HERRINGTON & SUTCLIFFE LLP
Chris R. Ottenweller (Ca. State Bar No. 73649)
G. Hopkins Guy (Ca. State Bar No. 124811)
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401