

RUSS, AUGUST & KABAT

1 RUSS AUGUST & KABAT
2 Marc A. Fenster, State Bar No. 181067
3 Email: mfenster@raklaw.com
4 Irene Y. Lee, State Bar No. 213625
5 Email: ilee@raklaw.com
6 Andrew D. Weiss, State Bar No. 232974
7 Email: aweiss@raklaw.com
8 12424 Wilshire Boulevard, 12th Floor
9 Los Angeles, California 90025
10 Telephone: 310.826.7474
11 Facsimile: 310.826.6991

12 Attorneys for Plaintiff
13 Linksmart Wireless Technology, LLC

14 UNITED STATES DISTRICT COURT
15 CENTRAL DISTRICT OF CALIFORNIA
16 SOUTHERN DIVISION

17 LINKSMART WIRELESS
18 TECHNOLOGY, LLC,

19 Plaintiff,

20 vs.

- 21 1. T-MOBILE USA, INC.;
- 22 2. LODGENET INTERACTIVE
- 23 CORP.;
- 24 3. IBAHN GENERAL HOLDINGS
- 25 CORP.;
- 26 4. ETHOSTREAM, LLC;
- 27 5. RAMADA WORLDWIDE, INC.;
- 28 6. MARRIOTT INTERNATIONAL,
- INC.;
7. SIX CONTINENTS HOTELS, INC.;
8. INTERCONTINENTAL HOTELS
- GROUP RESOURCES, INC.;
9. CHOICE HOTELS
- INTERNATIONAL, INC.; AND
10. BEST WESTERN
- INTERNATIONAL, INC.,

Defendants.

Case No. SACV12-00522 JST (ANx)

COMPLAINT

JURY TRIAL DEMANDED

COMPLAINT

COPY
FILED

2012 APR -5 PM 2:39
CLERK OF DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
SANTA ANA

BY FAX

COMPLAINT

This is an action for patent infringement, in which Linksmart Wireless Technology, LLC makes the following allegations against T-Mobile USA, Inc., LodgeNet Interactive Corp., iBAHN General Holdings Corp., EthoStream, LLC, Ramada Worldwide, Inc., Marriott International, Inc., Six Continents Hotels, Inc., InterContinental Hotels Groups Resources, Inc., Choice Hotels International, Inc. and Best Western International, Inc.

PARTIES

1. Plaintiff Linksmart Wireless Technology, LLC ("Linksmart Wireless") is a California limited liability company with its principal place of business at 301 N. Lake Ave., Suite 1001, Pasadena, California 91101..

2. On information and belief, defendant T-Mobile USA, Inc. ("T-Mobile") is a Delaware corporation with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006.

3. On information and belief, defendant LodgeNet Interactive Corporation ("LodgeNet") is a Delaware corporation with its principal place of business at 3900 West Innovation Street, Sioux Falls, South Dakota 57107.

4. On information and belief, defendant iBAHN General Holdings Corp. ("iBAHN") is a Delaware corporation with its principal place of business at 10757 South River Front Parkway, Suite 300, Salt Lake City, Utah 84095.

5. On information and belief, defendant EthoStream, LLC ("EthoStream") is a Minnesota limited liability company with its principal place of business at 10200 Innovation Drive, Suite 300, Milwaukee, Wisconsin 53226.

6. On information and belief, defendant Ramada Worldwide, Inc. ("Ramada") is a Delaware corporation with its principal place of business at 1 Sylvan Way, Parsippany, New Jersey 07054.

7. On information and belief, defendant Marriott International, Inc. ("Marriott") is a Delaware corporation with its principal place of business at 10400

1 Fernwood Road, Bethesda, Maryland 20817.

2 8. On information and belief, defendant Six Continents Hotels, Inc.
3 ("SCH") is a Delaware corporation with its principal place of business at Three
4 Ravinia Drive, Suite 100, Atlanta, Georgia 30346-2149.

5 9. On information and belief, defendant InterContinental Hotels Group
6 Resources, Inc. ("IHGR") is a Georgia corporation with its principal place of
7 business at Three Ravinia Drive, Suite 100, Atlanta, Georgia 30346-2149.

8 10. On information and belief, defendant Choice Hotels International Inc.
9 ("Choice Hotels") is a Delaware corporation with its principal place of business at
10 10750 Columbia Pike, Silver Spring, Maryland 20901.

11 11. On information and belief, defendant Best Western International, Inc.
12 ("Best Western") is a Florida corporation with its principal place of business at
13 6201 North 24th Parkway, Phoenix, Arizona 85016.

14 12. T-Mobile, LodgeNet, iBAHN, EthoStream, Ramada, Marriott, SCH,
15 IHGR, Choice Hotels and Best Western are collectively referred to herein as
16 "Defendants."

17 JURISDICTION AND VENUE

18 13. This action arises under the patent laws of the United States, Title 35
19 of the United States Code. This Court has subject matter jurisdiction pursuant to
20 28 U.S.C. §§ 1331 and 1338(a).

21 14. Venue is proper in this district under 28 U.S.C. §§ 1391 (b) and (c)
22 and 1400(b). On information and belief, each Defendant has a regular and
23 established place of business in this district, has transacted business in this district,
24 and/or has committed and/or induced acts of patent infringement in this district.

25 15. On information and belief, each Defendant is subject to this Court's
26 specific and general personal jurisdiction pursuant to due process and/or the
27 California Long Arm Statute, due at least to its substantial business in this forum,
28 including: (i) at least a portion of the infringing activities alleged herein; and (ii)

1 regularly doing or soliciting business, engaging in other persistent courses of
 2 conduct, and/or deriving substantial revenue from goods and services provided to
 3 individuals in California and in this district.

4 16. This case was originally pending in the Eastern District of Texas,
 5 styled as *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc.*, Case Nos.
 6 2:08-cv-00264, 2:08-cv-00304, 2:08-cv-00385 and 2:09-cv-00026 (consolidated).
 7 By way of compromise to address Defendants' intention to file a motion to transfer
 8 the case to California, parties dismissed the pending action in the Eastern District
 9 of Texas without prejudice. The compromise reached by the parties is reflected in
 10 the stipulation attached hereto as Exhibit B.

11 17. Pursuant to the stipulation between the parties and 35 U.S.C. § 299(c),
 12 Defendants have agreed to waive the joinder limitations of 35 U.S.C. § 299(a)-(b)
 13 as a defense to joinder in this action.

14 COUNT I

15 INFRINGEMENT OF U.S. PATENT NO. 6,779,118

16 (Against All Defendants)

17 18. Linksmart Wireless is the owner by assignment of United States
 18 Patent No. 6,779,118 ("the '118 Patent") entitled "User Specific Automatic Data
 19 Redirection System." The '118 Patent issued on August 17, 2004 from United
 20 States Patent Application No. 09/295,966 ("the '966 Application"). An Ex Parte
 21 Reexamination Certificate for the '118 Patent issued on March 27, 2012. A true
 22 and correct copy of the '118 Patent, including the Ex Parte Reexamination
 23 Certificate, is attached hereto as Exhibit A.

24 19. Koichiro Ikudome and Moon Tai Yeung are listed as the inventors on
 25 the '118 Patent.

26 20. Defendant T-Mobile has been and now is directly infringing, and
 27 indirectly infringing by way of inducing infringement and/or contributing to the
 28 infringement of the '118 Patent in the State of California, in this judicial district,

1 and elsewhere in the United States by, among other things, making, using,
2 importing, offering to sell, or selling wireless Internet access systems which utilize
3 captive portal techniques to block and/or redirect HTTP requests. These wireless
4 Internet access systems are covered by one or more claims of the '118 Patent, and
5 T-Mobile is making, using, importing, offering to sell, or selling them to the injury
6 of Linksmart Wireless. Defendant T-Mobile is thus liable for infringement of the
7 '118 Patent pursuant to 35 U.S.C. § 271.

8 21. Defendant LodgeNet has been and now is directly infringing, and
9 indirectly infringing by way of inducing infringement and/or contributing to the
10 infringement of the '118 Patent in the State of California, in this judicial district,
11 and elsewhere in the United States by, among other things, making, using,
12 importing, offering to sell, or selling wireless Internet access systems which utilize
13 captive portal techniques to block and/or redirect HTTP requests. These wireless
14 Internet access systems are covered by one or more claims of the '118 Patent, and
15 LodgeNet is making, using, importing, offering to sell, or selling them to the injury
16 of Linksmart Wireless. Defendant LodgeNet is thus liable for infringement of the
17 '118 Patent pursuant to 35 U.S.C. § 271.

18 22. Defendant iBAHN has been and now is directly infringing, and
19 indirectly infringing by way of inducing infringement and/or contributing to the
20 infringement of the '118 Patent in the State of California, in this judicial district,
21 and elsewhere in the United States by, among other things, making, using,
22 importing, offering to sell, or selling wireless Internet access systems which utilize
23 captive portal techniques to block and/or redirect HTTP requests. These wireless
24 Internet access systems are covered by one or more claims of the '118 Patent, and
25 iBAHN is making, using, importing, offering to sell, or selling them to the injury
26 of Linksmart Wireless. Defendant iBAHN is thus liable for infringement of the
27 '118 Patent pursuant to 35 U.S.C. § 271.

1 23. Defendant EthoStream has been and now is directly infringing, and
2 indirectly infringing by way of inducing infringement and/or contributing to the
3 infringement of the '118 Patent in the State of California, in this judicial district,
4 and elsewhere in the United States by, among other things, making, using,
5 importing, offering to sell, or selling wireless Internet access systems which utilize
6 captive portal techniques to block and/or redirect HTTP requests. These wireless
7 Internet access systems are covered by one or more claims of the '118 Patent, and
8 EthoStream is making, using, importing, offering to sell, or selling them to the
9 injury of Linksmart Wireless. Defendant EthoStream is thus liable for
10 infringement of the '118 Patent pursuant to 35 U.S.C. § 271.

11 24. Defendant Ramada has been and now is directly infringing, and
12 indirectly infringing by way of inducing infringement and/or contributing to the
13 infringement of the '118 Patent in the State of California, in this judicial district,
14 and elsewhere in the United States by, among other things, using, importing,
15 offering to sell, selling, or inducing others to use wireless Internet access systems
16 which utilize captive portal techniques to block and/or redirect HTTP requests.
17 These wireless Internet access systems are covered by one or more claims of the
18 '118 Patent, and Ramada is using, importing, offering to sell, selling, or inducing
19 others to use them to the injury of Linksmart Wireless. Defendant Ramada is thus
20 liable for infringement of the '118 Patent pursuant to 35 U.S.C. § 271.

21 25. Defendant Marriott has been and now is directly infringing, and
22 indirectly infringing by way of inducing infringement and/or contributing to the
23 infringement of the '118 Patent in the State of California, in this judicial district,
24 and elsewhere in the United States by, among other things, using, importing,
25 offering to sell, selling, or inducing others to use wireless Internet access systems
26 which utilize captive portal techniques to block and/or redirect HTTP requests.
27 These wireless Internet access systems are covered by one or more claims of the
28 '118 Patent, and Marriott is using, importing, offering to sell, selling, or inducing

1 others to use them to the injury of Linksmart Wireless. Defendant Marriott is thus
2 liable for infringement of the '118 Patent pursuant to 35 U.S.C. § 271.

3 26. Defendant SCH has been and now is directly infringing, and indirectly
4 infringing by way of inducing infringement and/or contributing to the infringement
5 of the '118 Patent in the State of California, in this judicial district, and elsewhere
6 in the United States by, among other things, using, importing, offering to sell,
7 selling, or inducing others to use wireless Internet access systems which utilize
8 captive portal techniques to block and/or redirect HTTP requests. These wireless
9 Internet access systems are covered by one or more claims of the '118 Patent, and
10 SCH is using, importing, offering to sell, selling, or inducing others to use them to
11 the injury of Linksmart Wireless. Defendant SCH is thus liable for infringement of
12 the '118 Patent pursuant to 35 U.S.C. § 271.

13 27. Defendant IHGR has been and now is directly infringing, and
14 indirectly infringing by way of inducing infringement and/or contributing to the
15 infringement of the '118 Patent in the State of California, in this judicial district,
16 and elsewhere in the United States by, among other things, using, importing,
17 offering to sell, selling, or inducing others to use wireless Internet access systems
18 which utilize captive portal techniques to block and/or redirect HTTP requests.
19 These wireless Internet access systems are covered by one or more claims of the
20 '118 Patent, and IHGR is using, importing, offering to sell, selling, or inducing
21 others to use them to the injury of Linksmart Wireless. Defendant IHGR is thus
22 liable for infringement of the '118 Patent pursuant to 35 U.S.C. § 271.

23 28. Defendant Choice Hotels has been and now is directly infringing, and
24 indirectly infringing by way of inducing infringement and/or contributing to the
25 infringement of the '118 Patent in the State of California, in this judicial district,
26 and elsewhere in the United States by, among other things, using, importing,
27 offering to sell, selling, or inducing others to use wireless Internet access systems
28 which utilize captive portal techniques to block and/or redirect HTTP requests.

1 These wireless Internet access systems are covered by one or more claims of the
2 '118 Patent, and Choice Hotels is using, importing, offering to sell, selling, or
3 inducing others to use them to the injury of Linksmart Wireless. Defendant Choice
4 Hotels is thus liable for infringement of the '118 Patent pursuant to 35 U.S.C. §
5 271.

6 29. Defendant Best Western has been and now is directly infringing, and
7 indirectly infringing by way of inducing infringement and/or contributing to the
8 infringement of the '118 Patent in the State of California, in this judicial district,
9 and elsewhere in the United States by, among other things, using, importing,
10 offering to sell, selling, or inducing others to use wireless Internet access systems
11 which utilize captive portal techniques to block and/or redirect HTTP requests.
12 These wireless Internet access systems are covered by one or more claims of the
13 '118 Patent, and Best Western is using, importing, offering to sell, selling, or
14 inducing others to use them to the injury of Linksmart Wireless. Defendant Best
15 Western is thus liable for infringement of the '118 Patent pursuant to 35 U.S.C. §
16 271.

17 30. Defendants have actively induced and are actively inducing
18 infringement of the '118 Patent and are liable for contributory infringement of the
19 '118 Patent.

20 31. As a result of Defendants' infringement of the '118 Patent, Linksmart
21 Wireless has suffered monetary damages in an amount not yet determined, and will
22 continue to suffer damages in the future unless Defendants' infringing activities are
23 enjoined by this Court.

24 32. Unless a permanent injunction is issued enjoining these Defendants
25 and their agents, servants, employees, attorneys, representatives, affiliates, and all
26 others acting on their behalf from infringing the '118 Patent, Linksmart Wireless
27 will be greatly and irreparably harmed.

28 **PRAYER FOR RELIEF**

1 WHEREFORE, Linksmart Wireless respectfully requests that this Court
2 enter:

3 1. A judgment in favor of Linksmart Wireless that each of the
4 Defendants has infringed, directly and/or indirectly, by way of inducing and/or
5 contributing to the infringement of the '118 Patent, and that such infringement was
6 willful;

7 2. A permanent injunction enjoining Defendants and their officers,
8 directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries,
9 parents, and all others acting in concert or privity with any of them from
10 infringing, inducing the infringement of, or contributing to the infringement of the
11 '118 Patent;

12 3. A judgment and order requiring Defendants to pay Linksmart
13 Wireless its damages, costs, expenses, and prejudgment and post-judgment interest
14 for Defendants' infringement of the '118 Patent as provided under 35 U.S.C. §
15 284;

16 4. An award to Linksmart Wireless for enhanced damages resulting from
17 the knowing, deliberate, and willful nature of Defendants' prohibited conduct with
18 notice being made at least as early as the date of the filing of the case against each
19 Defendant in the Eastern District of Texas, as provided under 35 U.S.C. § 284;

20 5. A judgment and order finding that this is an exceptional case within
21 the meaning of 35 U.S.C. § 285 and awarding to Linksmart Wireless its reasonable
22 attorneys' fees; and

23 6. Any and all other relief to which Linksmart Wireless may show itself
24 to be entitled.

DEMAND FOR JURY TRIAL

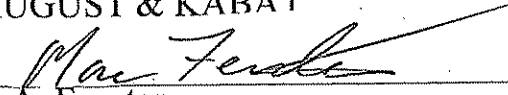
Linksmart Wireless, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: April 5, 2012

Respectfully submitted,

RUSS AUGUST & KABAT

By:


Marc A. Fenster

Marc A. Fenster, Cal. Bar No. 181067

Email: mfenster@raklaw.com

Irene Y. Lee, Cal. Bar No. 213625

Email: ilee@raklaw.com

Andrew D. Weiss, Cal. Bar No. 232974

Email: aweiss@raklaw.com

12424 Wilshire Boulevard, 12th Floor

Los Angeles, California 90025

Telephone: 310.826.7474

Facsimile: 310.826.6991

Attorneys for Plaintiff

Linksmart Wireless Technology, LLC

EXHIBIT A



US006779118B1

(12) **United States Patent**
Ikudome et al.

(10) Patent No.: **US 6,779,118 B1**
(45) Date of Patent: **Aug. 17, 2004**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US);
Moon Tai Yeung, Alhambra, CA (US)

(73) Assignee: **Auriq Systems, Inc.**, Pasadena, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

EP	0 854 621	7/1998
EP	0854621 A *	7/1998
WO	96/05549	2/1996
WO	9605549 *	2/1996
WO	98/03927	1/1998
WO	9826548 *	6/1998
WO	98/26548	6/1998
WO	99/57660	11/1999
WO	00/16529	3/2000

* cited by examiner

(21) Appl. No.: **09/295,966**

(22) Filed: **Apr. 21, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) Int. Cl.⁷ **G06F 12/14**

(52) U.S. Cl. **713/201**

(58) Field of Search 713/200, 201,
713/202, 165, 168, 193; 709/229; 380/200,
201, 230; 340/825.31, 825.34; 705/57,
58

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,696,898 A 12/1997 Baker et al. 395/187.01
6,157,829 A * 12/2000 Grube et al. 455/414.1
6,233,686 B1 5/2001 Dutta

FOREIGN PATENT DOCUMENTS

CA 2226814 3/2003

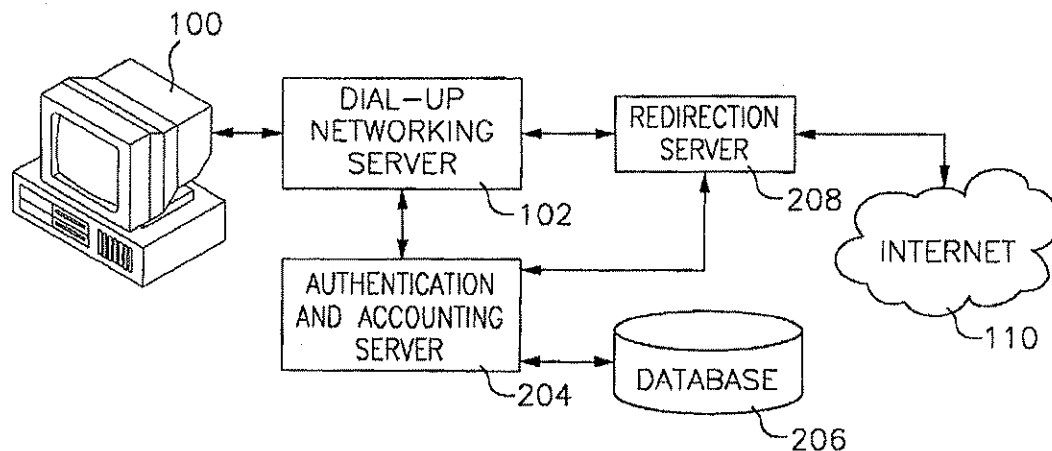
Primary Examiner—Pierre Elisca

(74) Attorney, Agent, or Firm—Christie, Parker & Hale, LLP

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.

27 Claims, 1 Drawing Sheet



U.S. Patent

Aug. 17, 2004

US 6,779,118 B1

FIG. 1

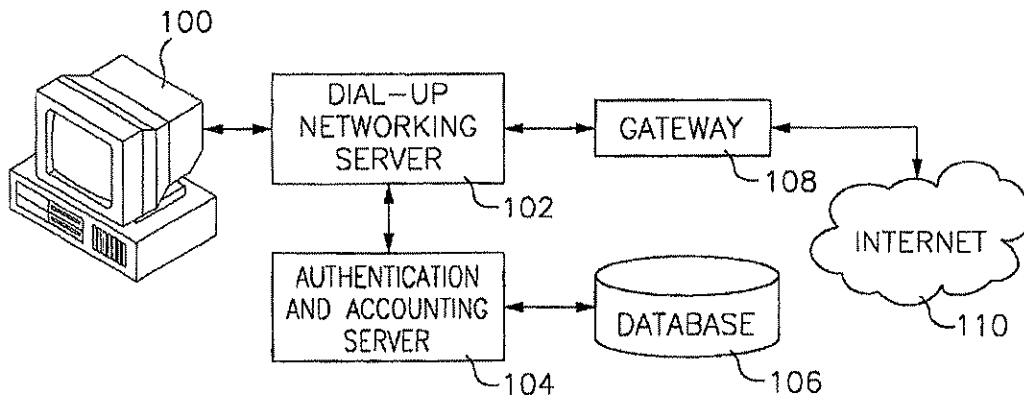
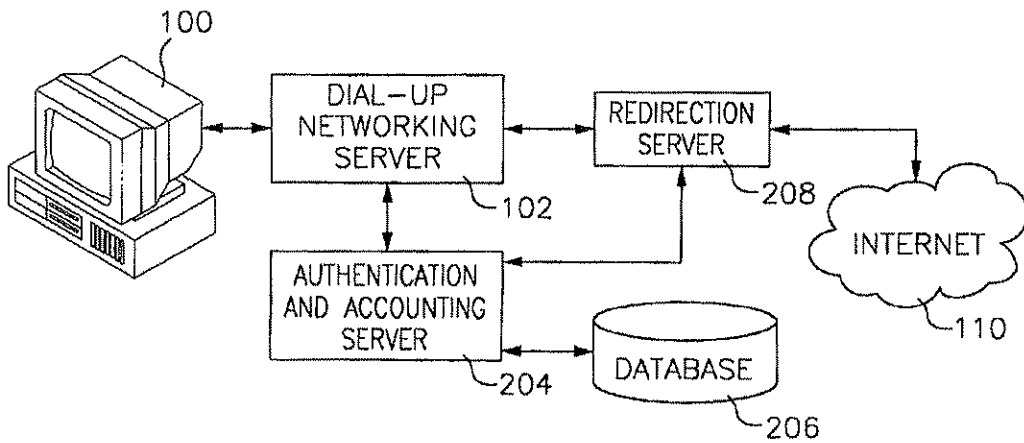


FIG. 2



US 6,779,118 B1

1

USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

RELATED APPLICATION

This application claims priority of U.S. Provisional Application No. 60/084,014 filed May 4, 1998, the disclosure of which is incorporated fully herein by reference.

FIELD OF THE INVENTION

This invention relates to the field of Internet communications, more particularly, to a database system for use in dynamically redirecting and filtering Internet traffic.

BACKGROUND OF THE INVENTION

In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a physical connection between their computer 100 and a dial-up networking server 102, the user provides to the dial-up networking server their user ID and password. The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104. A detailed description of the IP communications protocol is discussed in *Internetworking with TCP/IP*, 3rd ed., Douglas Comer, Prentice Hall, 1995, which is fully incorporated herein by reference. The authentication and accounting server, upon verification of the user ID and password using a database 106 would send an authorization message to the dial-up networking server 102 to allow the user to use the temporary IP address assigned to that user by the dial-up networking server and then logs the connection and assigned IP address. For the duration of that session, whenever the user would make a request to the Internet 110 via a gateway 108, the end user would be identified by the temporarily assigned IP address.

The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page—hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. Alternately, redirection can also be accomplished by coding the page such that it instructs the browser to run a program, like a Java applet or the like, which then redirects the browser. One disadvantage with current redirection technology is that control of the redirection is at the remote end, or WWW server end—and not the local, or user end. That is to say that the redirection is performed by the remote server, not the user's local gateway.

2

Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, they can filter outgoing packets sent from users to a specific destination as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. For example, the packet filter can determine if the packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. Service identification is achieved by identifying the terminating port number contained within each IP packet header. Port numbers are standard within the industry to allow for interoperability between equipment. Packet filtering devices allow network administrators to filter packets based on the source and/or destination information, as well as on the type of service being transmitted within each IP packet. Unlike redirection technology, packet filtering technology allows control at the local end of the network connection, typically by the network administrator. However, packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device.

Packet filter devices are often used with proxy server systems, which provide access control to the Internet and are most often used to control access to the world wide web. In a typical configuration, a firewall or other packet filtering device filters all WWW requests to the Internet from a local network, except for packets from the proxy server. That is to say that a packet filter or firewall blocks all traffic originating from within the local network which is destined for connection to a remote server on port 80 (the standard WWW port number). However, the packet filter or firewall permits such traffic to and from the proxy server. Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. When the proxy server receives a packet, the destination is checked against a database for approval. If the destination is allowed, the proxy server simply forwards packets between the local user and the remote server outside the firewall. However, proxy servers are limited to either blocking or allowing specific system terminals access to remote databases.

A recent system is disclosed in U.S. Pat. No. 5,696,898. This patent discloses a system, similar to a proxy server, that allows network administrators to restrict specific IP addresses inside a firewall from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW/Internet). According to the disclosure, the system has a relational database which allows network administrators to restrict specific terminals, or groups of terminals, from accessing certain locations. Similarly limited as a proxy server, this invention can only block or allow terminals' access to remote sites. This system is also static in that rules programmed into the database need to be reprogramming in order to change which locations specific terminals may access.

SUMMARY OF THE INVENTION

The present invention allows for creating and implementing dynamically changing rules, to allow the redirection, blocking, or allowing, of specific data traffic for specific users, as a function of database entries and the user's activity. In certain embodiments according to the present invention, when the user connects to the local network, as in the prior art system, the user's ID and password are sent to

US 6,779,118 B1

3

the authentication accounting server. The user ID and password are checked against information in an authentication database. The database also contains personalized filtering and redirection information for the particular user ID. During the connection process, the dial-up network server provides the authentication accounting server with the IP address that is going to be temporarily assigned to the user. The authentication accounting server then sends both the user's temporary IP address and all of the particular user's filter and redirection information to a redirection server. The IP address temporarily assigned to the end user is then sent back to the end user for use in connecting to the network.

Once connected to the network, all data packets sent to, or received by, the user include the user's temporary IP address in the IP packet header. The redirection server uses the filter and redirection information supplied by the authentication accounting server, for that particular IP address, to either allow packets to pass through the redirection server unmolested, block the request all together, or modify the request according to the redirection information.

When the user terminates the connection with the network, the dial-up network server informs the authentication accounting server, which in turn, sends a message to the redirection server telling it to remove any remaining filtering and redirection information for the terminated user's temporary IP address. This then allows the dial-up network to reassign that IP address to another user. In such a case, the authentication accounting server retrieves the new user's filter and redirection information from the database and passes it, with the same IP address which is now being used by a different user, to the redirection server. This new user's filter may be different from the first user's filter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a typical Internet Service Provider environment.

FIG. 2 is a block diagram of an embodiment of an Internet Service Provider environment with integrated redirection system.

DETAILED DESCRIPTION OF THE INVENTION

In the following embodiments of the invention, common reference numerals are used to represent the same components. If the features of an embodiment are incorporated into a single system, these components can be shared and perform all the functions of the described embodiments.

FIG. 2 shows a typical Internet Service Provider (ISP) environment with integrated user specific automatic data redirection system. In a typical use of the system, a user employs a personal computer (PC) 100, which connects to the network. The system employs: a dial-up network server 102, an authentication accounting server 204, a database 206 and a redirection server 208.

The PC 100 first connects to the dial-up network server 102. The connection is typically created using a computer modem, however a local area network (LAN) or other communications link can be employed. The dial-up network server 102 is used to establish a communications link with the user's PC 100 using a standard communications protocol. In the preferred embodiment Point to Point Protocol (PPP) is used to establish the physical link between the PC 100 and the dial-up network server 102, and to dynamically assign the PC 100 an IP address from a list of available addresses. However, other embodiments may employ dif-

4

ferent communications protocols, and the IP address may also be permanently assigned to the PC 100. Dial-up network servers 102, PPP and dynamic IP address assignment are well known in the art.

An authentication accounting server with Auto-Navi component (hereinafter, authentication accounting server) 204 is used to authenticate user ID and permit, or deny, access to the network. The authentication accounting server 204 queries the database 206 to determine if the user ID is authorized to access the network. If the authentication accounting server 204 determines the user ID is authorized, the authentication accounting server 204 signals the dial-up network server 102 to assign the PC 100 an IP address, and the Auto-Navi component of the authentication accounting server 204 sends the redirection server 208 (1) the filter and redirection information stored in database 206 for that user ID and (2) the temporarily assigned IP address for the session. One example of an authentication accounting server is discussed in U.S. Pat. No. 5,845,070, which is fully incorporated here by reference. Other types of authentication accounting servers are known in the art. However, these authentication accounting servers lack an Auto-Navi component.

The system described herein operates based on user ID's supplied to it by a computer. Thus the system does not "know" who the human being "user" is at the keyboard of the computer that supplies a user ID. However, for the purposes of this detailed description, "user" will often be used as a short hand expression for "the person supplying inputs to a computer that is supplying the system with a particular user ID."

The database 206 is a relational database which stores the system data. FIG. 3 shows one embodiment of the database structure. The database, in the preferred embodiment, includes the following fields: a user account number, the services allowed or denied each user (for example: e-mail, Telnet, FTP, WWW), and the locations each user is allowed to access.

Rule sets are employed by the system and are unique for each user ID, or a group of user ID's. The rule sets specify elements or conditions about the user's session. Rule sets may contain data about a type of service which may or may not be accessed, a location which may or may not be accessed, how long to keep the rule set active, under what conditions the rule set should be removed, when and how to modify the rule set during a session, and the like. Rule sets may also have a preconfigured maximum lifetime to ensure their removal from the system.

The redirection server 208 is logically located between the user's computer 100 and the network, and controls the user's access to the network. The redirection server 208 performs all the central tasks of the system. The redirection server 208 receives information regarding newly established sessions from the authentication accounting server 204. The Auto-Navi component of the authentication accounting server 204 queries the database for the rule set to apply to each new session, and forwards the rule set and the currently assigned IP address to the redirection server 208. The redirection server 208 receives the IP address and rule set, and is programed to implement the rule set for the IP address, as well as other attendant logical decisions such as: checking data packets and blocking or allowing the packets as a function of the rule sets, performing the physical redirection of data packets based on the rule sets, and dynamically changing the rule sets based on conditions. When the redirection server 208 receives information

US 6,779,118 B1

5

regarding a terminated session from the authentication accounting server 204, the redirection server 208 removes any outstanding rule sets and information associated with the session. The redirection server 208 also checks for and removes expired rule sets from time to time.

In an alternate embodiment, the redirection server 208 reports all or some selection of session information to the database 206. This information may then be used for reporting, or additional rule set generation.

System Features Overview

In the present embodiment, each specific user may be limited to, or allowed, specific IP services, such as WWW, FTP and Telnet. This allows a user, for example, WWW access, but not FTP access or Telnet access. A user's access can be dynamically changed by editing the user's database record and commanding the Auto-Navi component of the authentication accounting server 204 to transmit the user's new rule set and current IP address to the redirection server 208.

A user's access can be "locked" to only allow access to one location, or a set of locations, without affecting other users' access. Each time a locked user attempts to access another location, the redirection server 208 redirects the user to a default location. In such a case, the redirection server 208 acts either as proxy for the destination address, or in the case of WWW traffic the redirection server 208 replies to the user's request with a page containing a redirection command.

A user may also be periodically redirected to a location, based on a period of time or some other condition. For example, the user will first be redirected to a location regardless of what location the user attempts to reach, then permitted to access other locations, but every ten minutes the user is automatically redirected to the first location. The redirection server 208 accomplishes such a rule set by setting an initial temporary rule set to redirect all traffic; after the user accesses the redirected location, the redirection server then either replaces the temporary rule set with the user's standard rule set or removes the rule set altogether from the redirection server 208. After a certain or variable time period, such as ten minutes, the redirection server 208 reinstates the rule set again.

The following steps describe details of a typical user session:

A user connects to the dial-up network server 102 through computer 100.

The user inputs user ID and password to the dial-up network server 102 using computer 100 which forwards the information to the authentication accounting server 204

The authentication accounting server 204 queries database 206 and performs validation check of user ID and password.

Upon a successful user authentication, the dial-up network server 102 completes the negotiation and assigns an IP address to the user. Typically, the authentication accounting server 204 logs the connection in the database 206.

The Auto-Navi component of the authentication accounting server 204 then sends both the user's rule set (contained in database 206) and the user's IP address (assigned by the dial-up network server 102) in real time to the redirection server 208 so that it can filter the user's IP packets.

6

The redirection server 208 programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user's data as a function of the rule set.

The following is an example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-2) was such as to only allow that user to access the web site www.us.com, and permit Telnet services, and redirect all web access from any server at xyz.com to www.us.com, then the logic would be as follows:

The database 206 would contain the following record for user UserID-2:

ID	UserID-2	
Password:	secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	www.us.com	0
http	*.xyz.com=>www.us.com	0

the user initiates a session, and sends the correct user ID and password (UserID-2 and secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns UserID-2 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
  ( ((request type=HTTP) AND (destination address=
    www.us.com) ) OR (request type=Telnet)
  ) THEN ok.
IF source IP-address=10.0.0.1 AND
  ( (request type=HTTP) AND (destination address=
    *.xyz.com)
  ) THEN (redirect=www.us.com)
```

The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-2) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine within the xyz.com domain) the traffic is redirected by the redirection server 208 to www.us.com. Similarly, if the user attempts to connect to any service other than HTTP at www.us.com or Telnet anywhere, the packet will simply be blocked by the redirection server 208.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

The following is another example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-3) was to force the user to visit the web site www.widgetsell.com, first, then to have unfettered access to other web sites, then the logic would be as follows:

US 6,779,118 B1

7

The database 206 would contain the following record for user UserID-3;

ID	UserID-3	
Password:	top-secret	
#####		
### Rule Sets ###		
#####		
#service	rule	expire
http	"=>www.widgetsell.com	1x

the user initiates a session, and sends the correct user ID and password (UserID-3 and top-secret) to the dial-up network server 102. As both the user ID and password are correct, the authentication accounting server 204 authorizes the dial-up network server 102 to establish a session. The dial-up network server 102 assigns user ID 3 an IP address (for example, 10.0.0.1) to the user and passes the IP address to the authentication accounting server 204.

The Auto-Navi component of the authentication accounting server 204 sends both the user's rule set and the user's IP address (10.0.0.1) to the redirection server 208.

The redirection server 208 programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server 208 to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
(request type=HTTP) THEN (redirect=
www.widgetsell.com)
THEN SET NEW RULE
IF source IP-address=10.0.0.1 AND
(request type=HTTP) THEN ok.
```

The redirection server 208 monitors all the IP packets, checking each against the rule set. In this situation, if IP address 10.0.0.1 (the address assigned to user ID UserID-3) attempts to send a packet containing HTTP data (i.e., attempts to connect to port 80 on any machine) the traffic is redirected by the redirection server 208 to www.widgetsell.com. Once this is done, the redirection server 208 will remove the rule set and the user is free to use the web unmolested.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

In an alternate embodiment a user may be periodically redirected to a location, based on the number of other factors, such as the number of locations accessed, the time spent at a location, the types of locations accessed, and other such factors.

A user's account can also be disabled after the user has exceeded a length of time. The authentication accounting server 204 keeps track of user's time online. Prepaid use subscriptions can thus be easily managed by the authentication accounting Server 204.

In yet another embodiment, signals from the Internet 110 side of redirection server 208 can be used to modify rule sets being used by the redirection server. Preferably, encryption and/or authentication are used to verify that the server or other computer on the Internet 110 side of redirection server 208 is authorized to modify the rule set or rule sets that are being attempted to be modified. An example of this embodiment is where it is desired that a user be redirected to a particular web site until the fill out a questionnaire or satisfy some other requirement on such a web site. In this example,

8

the redirection server redirects a user to a particular web site that includes a questionnaire. After this web site receives acceptable data in all required fields, the web site then sends an authorization to the redirection server that deletes the redirection to the questionnaire web site from the rule set for the user who successfully completed the questionnaire. Of course, the type of modification an outside server can make to a rule set on the redirection server is not limited to deleting a redirection rule, but can include any other type of modification to the rule set that is supported by the redirection server as discussed above.

It will be clear to one skilled in the art that the invention may be implemented to control (block, allow and redirect) any type of service, such as Telnet, FTP, WWW and the like. The invention is easily programmed to accommodate new services or networks and is not limited to those services and networks (e.g., the Internet) now known in the art.

It will also be clear that the invention may be implemented on a non-IP based networks which implement other addressing schemes, such as IPX, MAC addresses and the like. While the operational environment detailed in the preferred embodiment is that of an ISP connecting users to the Internet, it will be clear to one skilled in the art that the invention may be implemented in any application where control over users' access to a network or network resources is needed, such as a local area network, wide area network and the like. Accordingly, neither the environment nor the communications protocols are limited to those discussed.

What is claimed is:

1. A system comprising:

- a database with entries correlating each of a plurality of user IDs with an individualized rule set;
- a dial-up network server that receives user IDs from users' computers;
- a redirection server connected to the dial-up network server and a public network, and
- an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

2. The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

3. The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

4. The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

5. The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

6. The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

US 6,779,118 B1

9

7. The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

8. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server, the method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

9. The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

10. The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

11. The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

12. The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

13. The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations as a function of the individualized rule set.

14. The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

15. A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access.

16. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

10

18. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user access.

19. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user access.

22. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

23. The system of claim 15, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

24. The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

25. In a system comprising a redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; the method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

26. The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user access.

27. The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user access.

* * * * *



US006779118C1

(12) **EX PARTE REEXAMINATION CERTIFICATE** (8926th)
United States Patent
Ikudome et al.

(10) **Number:** **US 6,779,118 C1**
 (45) **Certificate Issued:** **Mar. 27, 2012**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US);
Moon Tai Yeung, Alhambra, CA (US)

(73) Assignee: **Linksmart Wireless Technology, LLC**,
 Pasadena, CA (US)

Reexamination Request:

No. 90/009,301, Dec. 17, 2008

Reexamination Certificate for:

Patent No.: **6,779,118**
 Issued: **Aug. 17, 2004**
 Appl. No.: **09/295,966**
 Filed: **Apr. 21, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/00 (2006.01)

(52) **U.S. Cl.** 726/7; 726/14

(58) **Field of Classification Search** 726/8
 See application file for complete search history.

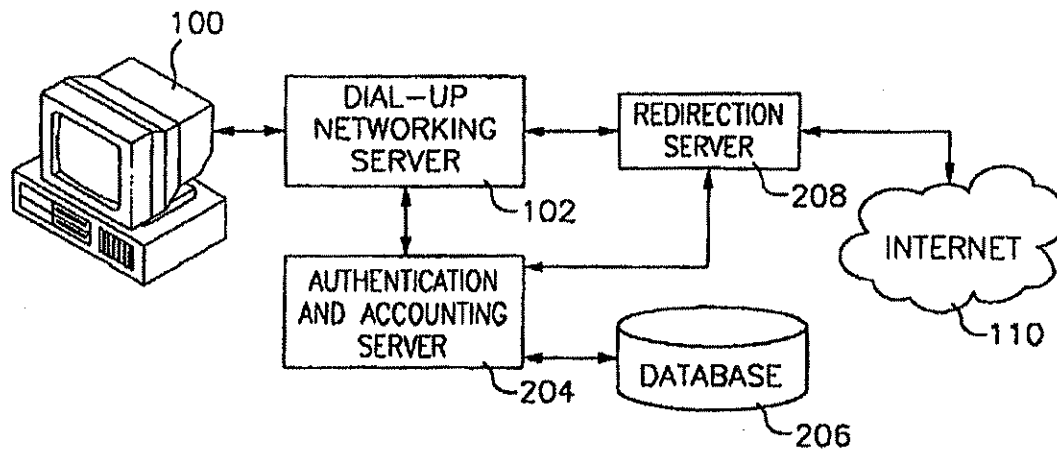
References Cited

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/009,301, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner—Samuel Rimell

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.



US 6,779,118 C1

1
EX PARTE
REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS
INDICATED BELOW.

Matter enclosed in heavy brackets [] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims 2-7 and 9-14 is confirmed.

Claims 1, 8, 15 and 25 are cancelled.

Claims 16-23 and 26-27 are determined to be patentable as amended.

Claim 24, dependent on an amended claim, is determined to be patentable.

New claims 28-90 are added and determined to be patentable.

16. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

2

18. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*
wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;
wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and
wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user [access] accesses.

19. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*
wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;
wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. [The system of claim 15,] *A system comprising: a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;*

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

US 6,779,118 C1

3

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user [access] accesses.

22. [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user [access] accesses.

23. [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

26. The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user [access] accesses.

27. The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and [the] a location or locations the user [access] accesses.

28. The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

29. The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

4

30. The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

31. The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

32. The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

33. The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

34. The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

35. The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

36. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

37. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

38. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

US 6,779,118 C1

5

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

39. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

40. The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

41. The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

42. The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

43. The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

44. A system comprising:

a database with entries correlating each of a plurality of user IDs with an individualized rule set;

a dial-up network server that receives user IDs from users' computers;

a redirection server connected between the dial-up network server and a public network, and

an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

45. The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

6

46. The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

47. The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

48. The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

49. The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

50. The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

51. The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

52. The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

53. The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

54. The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

55. The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

56. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection servers, a method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

57. The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

58. The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

59. The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

60. The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

61. The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

US 6,779,118 C1

7

62. The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

63. The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

64. The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

65. The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

66. The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

67. The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

68. A system comprising:

a redirection server connected between a user computer and a public network, the redirection server programmed with a users' rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.

69. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

70. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

71. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

72. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

73. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

74. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

75. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

8

76. The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

77. The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

78. The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

79. The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

80. The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

81. The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

82. The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

83. In a system comprising a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; a method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and

wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

84. The method of claim 83, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

85. The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.

86. The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

87. The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule

US 6,779,118 C1

9

set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

88. The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

89. The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new desti-

10

nation address based on a request type and an attempted destination address.

90. The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.

* * * * *

EXHIBIT B

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LINKSMART WIRELESS TECHNOLOGY,
LLC,

Plaintiff,

v.

T-MOBILE USA, INC., et al.

Defendants.

AND RELATED COUNTERCLAIMS.

Case No. 2:08-cv-00264-DF-CE
Case No. 2:08-cv-00304-DF-CE
Case No. 2:08-cv-00385-DF-CE
Case No. 2:09-cv-00026-DF-CE

CONSOLIDATED

**STIPULATION REGARDING DISMISSAL AND REILING IN THE CENTRAL
DISTRICT OF CALIFORNIA, SOUTHERN DIVISION**

Plaintiff Linksmart Wireless Technology, LLC ("Linksmart") and Defendants Cisco Systems, Inc., T-Mobile USA Inc., LodgeNet Interactive Corp., Marriott International, Inc., InterContinental Hotels Resource Group, Inc., Six Continents Hotels, Inc., iBahn General Holdings Corp., Ethostream, LLC, Ramada World Wide, Best Western International Inc., and Choice Hotels International (collectively, "Defendants"), by and through counsel, hereby stipulate to the following:

1. This stipulation is entered into by way of compromise to address Defendants' intention to file a motion to transfer the case to California.
2. The parties jointly stipulate to dismiss without prejudice the instant action pursuant to Fed. R. Civ. P. 41(a)(2).
3. Linksmart will re-file its action against Defendants in the United States District Court for the Central District of California, Southern Division, and do so by April 6, 2012. The re-filed pleading shall not contain any grounds or causes of action, against any Defendant, that are new or additional to those of the pleading against that Defendant now pending in this Court. Linksmart reserves the right to argue, in the action to be filed in the

Central District of California, Southern Division, that it may assert new and/or amended claims from the reexamined '118 patent. Defendants reserve the right to oppose any such argument. For the sake of clarity, this paragraph is not intended to resolve any such dispute.

4. The parties' agreement to dismiss the instant action without prejudice shall not count as a dismissal pursuant to the second sentence of Fed. R. Civ. P. 41(a)(1)(B) and may in no circumstances be construed as an adjudication on the merits in the action to be filed in accordance with paragraph 3.

5. The Defendants agree to answer the complaint, and will not move pursuant to Fed. R. Civ. P. 12, in the action to be filed in accordance with paragraph 3.

6. Pursuant to 35 U.S.C. § 299(c), Defendants hereby waive the joinder limitations of 35 U.S.C. § 299(a)-(b) as a defense to joinder in the action filed in accordance with paragraph 3. Defendants retain all rights apart from 35 U.S.C. § 299 to seek severance, to seek separate trials, or to argue improper joinder on any basis existing in the cases now pending in this Court.

7. Defendants authorize their respective counsel of record in the instant case to accept service of the action to be filed in accordance with paragraph 3 and counsel have so agreed to accept service on behalf of their client(s). Linksmart may effect service upon the Defendants by delivering an OCR'ed copy of the summons and the complaint via electronic mail to their respective counsel of record in the instant case. Within 5 business days of being provided with the form, counsel for each of the Defendants agrees to sign and return to Linksmart a copy of the signed Notice of Lawsuit and Request for Waiver of Service of Summons (form CV-39).

8. With respect to damages, the parties agree to treat the action to be filed in accordance with paragraph 3 as if it had been filed on the date of the original complaint filed against each respective Defendant in this action. The intent of the parties is that this Stipulation regarding dismissal shall not, in the action to be filed in accordance with paragraph 3, give rise to any statute of limitations defense not already available to

Defendants in the instant action. Defendants retain all other damages defenses, including the defenses that each Defendant had as of the date of the filing of the original complaint against each respective Defendant. Defendants also retain all defenses due to intervening rights arising from any concluded, pending or future reexamination of the '118 patent.

9. The parties agree that the written discovery limitations agreed to in the instant action (D.I. 212) shall be used in the action to be filed in accordance with paragraph 3.

10. The parties agree that all discovery, including deposition testimony, document production and interrogatory responses, served in the instant action may be reused in an action filed in accordance with paragraph 3, subject to any evidentiary or other objections.

11. The total hours of depositions taken in the instant action will be taken into account when determining the number of deposition hours permitted in the action to be filed in accordance with paragraph 3. For the sake of clarity, this paragraph does not resolve any disputes regarding additional deposition time, including additional deposition time with inventors of the '118 patent.

12. Any issue not expressly addressed in this Stipulation shall be addressed by the Parties in the action to be filed in accordance with paragraph 3.

13. Any complaint filed by Linksmart against any of the currently named defendants (a) after April 6, 2012, or (b) which contains allegations that are new or additional to those contained in the original filing in the instant actions against such defendant(s), is specifically exempt from, and shall not be subject to, the terms of this Stipulation with respect to that defendant(s).

14. Each Defendant, and any entities under the Defendant's control, agrees (a) not to file a declaratory judgment action against Linksmart regarding the '118 patent or the reexamined '118 patent prior to April 7, 2012; and (b) after April 7, 2012, not to file a declaratory judgment action against Linksmart regarding issues asserted against that Defendant in the action filed in accordance with paragraph 3 except if filed as counterclaims

in that same action. This paragraph does not apply to entities outside of Defendants' control, including vendors, customers, franchisees and member hotels.

Dated: April 3, 2012

Respectfully submitted,

By: /s/ Andrew D. Weiss
Marc A. Fenster, CA SB #181067
E-mail: mfenster@raklaw.com
Andrew D. Weiss, CA SB #232974
E-mail: aweiss@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Andrew W. Spangler, TX SB #24041960
Email: spangler@spanglerlawpc.com
SPANGLER LAW PC
208 N. Green Street, Suite 300
Longview, TX 75601
Telephone: 903/753-9300
Facsimile: 903/553-0403

**Attorneys for Plaintiff
LINKSMART WIRELESS
TECHNOLOGY, LLC**

By: /s/ Noah A. Levine
Noah Levine
David B. Bassett
WilmerHale
399 Park Avenue
New York, NY 10022
212-230-8800
212-230-8888 (fax)
noah.levine@wilmerhale.com
david.bassett@wilmerhale.com

William F. Lee
Jonathan Andron
WilmerHale
60 State Street
Boston MA 02109

617-526-6000
617-526-5000 (fax)
william.lee@wilmerhale.com
jonathan.andron@wilmerhale.com

Michael Ernest Richardson
Beck Redden & Secrest - Houston
1221 McKinney
Suite 4500
Houston, TX 77010-2010
713-951-6284
713-951-3720 (fax)
mrichardson@brsfirm.com

**Attorneys for Cisco Systems, Inc. and
T-Mobile USA Inc.**

/s/ Kirk Ruthenberg
Kirk R Ruthenberg
SNR Denton
1301 K Street, NW
Suite 600E
Washington , DC 20005
202/408-6410
Fax: 202/408-6399
Email: kirk.ruthenberg@snrdenton.com

Attorneys for T-Mobile USA, Inc.

By: /s/ Mark E. Ungerman
Jennifer Parker Ainsworth
State Bar No. 00784720
WILSON, ROBERTSON
& CORNELIUS, P.C.
909 ESE Loop 323, Suite 400
P.O. Box 7339 [75711]
Tyler, Texas 75701
Tel.. 903-509-5000
Fax 903-509-5092

Mark E. Ungerman
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Tel. 202-887-1500

Fax 202-887-0763
Email: mungerman@mofo.com

Attorneys for LodgeNet Interactive Corp.

By: /s/ John M. Guaragna
John M. Guaragna, Esq.
State Bar No. 24043308
DLA Piper LLP
401 Congress Avenue, Suite 2500
Austin, TX 78701-3799
Tel. 512-457-7000
Fax 512-457-7001

**Attorneys for Defendants Marriott
International, Inc.,
InterContinental Hotels Group Resources,
Inc., and Six Continents Hotels, Inc.**

By: /s/ Michael Broaddus
David J. Burman
LEAD ATTORNEY
DBurman@perkinscoie.com
Michael D. Broaddus
MBroaddus@perkinscoie.com
PERKINS COIE LLP
1201 Third Ave., 48th Floor
Seattle, WA 98101
Tel. 206-359-8000
Fax 206-359-9000

Michael E. Jones
mikejones@potterminton.com
Allen Gardner
allengardner@potterminton.com
POTTER MINTON
110 N. College 500 Plaza Tower
Tyler, Texas 75702
Tel. 903-597-8311
Fax 903-593-0846 (facsimile)

**Attorneys for iBahn General Holdings
Corp.**

/s/ James D. Peterson
James D. Peterson
jpeterson@gklaw.com
Godfrey & Kahn, S.C.
One East Main Street, Suite 500
Madison, Wisconsin 53703
Tel. 608.257.3911
Fax. 608.257.0609

Christine J. Moser
Baker Hostetler
3200 National City Center
1900 East North St
Cleveland, Ohio 44114-3485
Tel. 216-621-0200
Fax 216-696-0740
cmoser@bakerlaw.com

**Attorneys for Ethostream, LLC and
Ramada World Wide**

/s/ David E. Rogers
David E. Rogers
drogers@swlaw.com
Sid Leach
sleach@swlaw.com
Snell & Wilmer, LLP
400 E Van Buren St #1900
Phoenix, AZ 85004-2202
Tel. 602.382.6225
Fax. 602.382.6070

Christopher M. Joe
Chris.Joe@bjciplaw.com
Brian A. Carpenter
Brian.Carpenter@bjciplaw.com
Buether Joe & Carpenter, LLC
1700 Pacific, Suite 2390
Dallas, TX 75201
Tel. 214-466-1272
Fax 214-635-1828

**Attorneys for Best Western International
Inc.**

/s/ Michael C. Smith
Michael Charles Smith
Siebman Reynolds Burg Phillips & Smith, LLP
713 South Washington
Marshall, TX 75670
Tel. 903-938-8900
Fax 972-767-4620 (fax)
michaelsmith@siebman.com

Kevin P. Anderson
Greg Lyons
Wiley Rein LLP
1776 K Street NW
Tel. 202-719-7000
Fax 202-719-7049
kanderson@wileyrein.com
glyons@wiley.rein.com

**Attorney for Choice Hotels International,
Inc.**

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Josephine Tucker and the assigned discovery Magistrate Judge is Arthur Nakazato.

The case number on all documents filed with the Court should read as follows:

SACV12- 522 JST (ANx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

☐ **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

☒ **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

☐ **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

RUSS AUGUST & KABAT
 Marc A. Fenster, CA-SBN:181067
 Email: mfenster@raklaw.com
 12424 Wilshire Boulevard, 12th Floor
 Los Angeles, CA 90025
 Telephone: 310/826-7474/Facsimile: 310/826-6991

UNITED STATES DISTRICT COURT
 CENTRAL DISTRICT OF CALIFORNIA

LINKSMART WIRELESS TECHNOLOGY, LLC

CASE NUMBER

SACV12-00522 JST (ANx)

PLAINTIFF(S)

v.

T-MOBILE USA, INC.; LODENET INTERACTIVE
 CORP.; IBAHN GENERAL HOLDINGS CORP.;
 ETHOSTREAM, LLC; [Continued on Attached]

DEFENDANT(S).

SUMMONS

TO: DEFENDANT(S):

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☒ complaint ☐ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Marc A. Fenster, whose address is Russ August & Kabat, 12424 Wilshire Blvd., 12th Fl., Los Angeles, CA 90025. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Clerk, U.S. District Court

Dated: 4/5/2012

By: Denise Vo
 Deputy Clerk



(Seal of the Court)

1191

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

ATTACHMENT TO SUMMONS

CONTINUED LIST OF DEFENDANTS:

RAMADA WORLDWIDE, INC.;
MARRIOTT INTERNATIONAL, INC.;
SIX CONTINENTS HOTELS, INC.;
INTERCONTINENTAL HOTELS GROUP RESOURCES, INC.
CHOICE HOTELS INTERNATIONAL, INC.; AND
BEST WESTERN INTERNATIONAL, INC.

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself <input type="checkbox"/>) LINKSMART WIRELESS TECHNOLOGY, LLC	DEFENDANTS T-MOBILE USA, INC.; LODGENET INTERACTIVE CORP.; IBARN GENERAL HOLDINGS CORP.; ETHOSTREAM, LLC; [Continued on Attached]						
Attorneys for Plaintiff LINKSMART WIRELESS TECHNOLOGY, LLC	Attorneys for Defendant						
(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.) Marc A. Fenster, CA-SBN:181067, Email: mfenster@raklaw.com RUSS AUGUST & KABAT 12424 Wilshire Blvd., 12th Fl. Los Angeles, CA 90025; 310/826-7474							
II. BASIS OF JURISDICTION (Place an X in one box only.) <input type="checkbox"/> 1 U.S. Government Plaintiff <input checked="" type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) <input type="checkbox"/> 2 U.S. Government Defendant <input type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)	III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.) <table style="width:100%; border: none;"> <tr> <td style="width:40%; border: none;"> Citizen of This State Citizen of Another State Citizen or Subject of a Foreign Country </td> <td style="width:20%; border: none; text-align: center;"> PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 3 </td> <td style="width:40%; border: none;"> Incorporated or Principal Place of Business in this State Incorporated and Principal Place of Business in Another State Foreign Nation </td> </tr> <tr> <td style="border: none;"></td> <td style="border: none; text-align: center;"> PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 6 </td> <td style="border: none;"></td> </tr> </table>	Citizen of This State Citizen of Another State Citizen or Subject of a Foreign Country	PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 3	Incorporated or Principal Place of Business in this State Incorporated and Principal Place of Business in Another State Foreign Nation		PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 6	
Citizen of This State Citizen of Another State Citizen or Subject of a Foreign Country	PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 3	Incorporated or Principal Place of Business in this State Incorporated and Principal Place of Business in Another State Foreign Nation					
	PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 6						
IV. ORIGIN (Place an X in one box only.) <input checked="" type="checkbox"/> 1 Original Proceeding <input type="checkbox"/> 2 Removed from State Court <input type="checkbox"/> 3 Remanded from Appellate Court <input type="checkbox"/> 4 Reinstated or Reopened <input type="checkbox"/> 5 Transferred from another district (specify): <input type="checkbox"/> 6 Multi-District Litigation <input type="checkbox"/> 7 Appeal to District Judge from Magistrate Judge							
V. REQUESTED IN COMPLAINT: JURY DEMAND: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No (Check 'Yes' only if demanded in complaint.) CLASS ACTION under F.R.C.P. 23: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No MONEY DEMANDED IN COMPLAINT: \$ over 75,000							
VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.) 28 U.S.C. Sections 1331, 1338(a)							
VII. NATURE OF SUIT (Place an X in one box only.) <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width:16.6%; vertical-align: top;"> OTHER STATUTES <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 490 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes </td> <td style="width:16.6%; vertical-align: top;"> CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property </td> <td style="width:16.6%; vertical-align: top;"> TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury-Med Malpractice <input type="checkbox"/> 365 Personal Injury-Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 402 Naturalization Application <input type="checkbox"/> 403 Habeas Corpus-Alien Detainee <input type="checkbox"/> 405 Other Immigration Actions </td> <td style="width:16.6%; vertical-align: top;"> TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage-Product Liability BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights </td> <td style="width:16.6%; vertical-align: top;"> PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 Habeas Corpus <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other </td> <td style="width:16.6%; vertical-align: top;"> LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input checked="" type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609 </td> </tr> </table>		OTHER STATUTES <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 490 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes	CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury-Med Malpractice <input type="checkbox"/> 365 Personal Injury-Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 402 Naturalization Application <input type="checkbox"/> 403 Habeas Corpus-Alien Detainee <input type="checkbox"/> 405 Other Immigration Actions	TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage-Product Liability BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 Habeas Corpus <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other	LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input checked="" type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
OTHER STATUTES <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 490 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes	CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury-Med Malpractice <input type="checkbox"/> 365 Personal Injury-Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 402 Naturalization Application <input type="checkbox"/> 403 Habeas Corpus-Alien Detainee <input type="checkbox"/> 405 Other Immigration Actions	TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage-Product Liability BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 Habeas Corpus <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other	LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input checked="" type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609		

FOR OFFICE USE ONLY: Case Number: **SACV12-00522 JST (ANx)**
 AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET**

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☒ No ☐ Yes
If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☒ No ☐ Yes
If yes, list case number(s): _____

Civil cases are deemed related if a previously filed case and the present case:

- (Check all boxes that apply) ☐ A. Arise from the same or closely related transactions, happenings, or events; or
☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
☐ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

- (a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.
☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	

- (b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.
☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	(T-Mobile) WA; (LodgeNet) SD; (iBAHN) UT; (EthoStream) WI; (Ramada) NJ; (Marriott) MD; (SCH) GA; (IHGR) GA; (Choice Hotels) MD; (Best Western) AZ

- (c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.
Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Orange	

* Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties

Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER): Man Fent Date April 5, 2012

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))

ATTACHMENT TO CIVIL COVER SHEET

CONTINUED LIST OF DEFENDANTS:

RAMADA WORLDWIDE, INC.;
MARRIOTT INTERNATIONAL, INC.;
SIX CONTINENTS HOTELS, INC.;
INTERCONTINENTAL HOTELS GROUP RESOURCES, INC.
CHOICE HOTELS INTERNATIONAL, INC.; AND
BEST WESTERN INTERNATIONAL, INC.