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

Competitive Access Systems, Inc., Plaintiff, - vs. - **Oracle Corporation** and **Oracle America, Inc.**, Defendants.	Civil Action No. 2:22-cv-287 **Jury Trial Demanded**

COMPLAINT FOR PATENT INFRINGEMENT

Competitive Access Systems, Inc. ("CAS") hereby brings this action for patent infringement against Oracle Corporation and Oracle America, Inc. (together "Oracle").

CAS alleges infringement of U.S. Patent No. 8,228,801, entitled "Broadband Communications Device" (the '801 patent), U.S. Patent No. 9,350,649, entitled "Multipath Communication Devices and Methods" (the '649 patent), and U.S. Patent No 10,868,908, entitled "Devices and Methods for Multipath Communications" (the '908 patent), at least by reason of Defendants' sale and servicing of the Oracle MPTCP Products and Oracle SD-WAN Products.

True and correct copies of the '801, '649, and '908 patents (together "Patents-in-Suit" or "Asserted Patents") are attached as Exhibits A, B, and C, respectively.

The Parties

1. Plaintiff Competitive Access Systems, Inc. is a Texas corporation with its principal place of business at 3019 Charles Drive, Wylie, Texas 75098. CAS is a technology and products development company. CAS is located in this judicial district and has

been for years. CAS was founded by Eric Delangis, the sole named inventor of the Asserted Patents. Mr. Delangis also lives in this judicial district.

2. Defendant Oracle Corporation is a Delaware corporation with regular and established places of business in this judicial district, located at 7460 Warren Parkway, Frisco, Texas 75034 and at 7164 Technology Drive, Frisco, Texas 75034. On information and belief, Oracle Corporation is the creator, developer, seller, and servicer of Oracle Linux and Oracle SD-WAN products.

3. Defendant Oracle America, Inc. is a Delaware corporation with a regular and established place of business in this judicial district, located at 7460 Warren Parkway, Frisco, Texas 75034 and at 7164 Technology Drive, Frisco, Texas 75034. On information and belief, Oracle America, Inc. (formerly known as Sun Microsystems and acquired in 2010 by Oracle Corporation) is an agent of Oracle Corporation, is under the control of Oracle Corporation, and has been granted authority to act on Oracle Corporation's behalf. On information and belief, Oracle America, Inc. is the creator, developer, seller, and servicer of Oracle Solaris.

Jurisdiction and Venue

4. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 101 et seq. The Court therefore has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Oracle is subject to this Court's specific and general personal jurisdiction, pursuant to constitutional due process and the Texas Long-Arm Statute, due at least to their extensive business in this District, including their infringement alleged herein. Oracle's principal place of business, its headquarters, is in Austin, Texas. Also, on infor-

mation and belief, Oracle, directly or through subsidiaries or intermediaries, ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises its products and services in the United States and in this District.

6. On information and belief, Oracle, directly and through subsidiaries or intermediaries, has purposefully and voluntarily placed one or more of its infringing products, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers or consumers in this District, including the Oracle MPTCP Products and Oracle SD-WAN Products. On information and belief, Oracle has customers in Texas and this district that have purchased and used infringing Oracle MPTCP Products and Oracle SD-WAN Products. Oracle therefore has committed acts of infringement within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Oracle would not offend traditional notions of fair play and substantial justice.

7. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b).

8. For years, Oracle has maintained a regional field office in Frisco, Texas. Oracle removed the Frisco office from its listing of Field Offices on its webpage. But it was listed as recently as June 28, 2022. *See* June 28, 2022, capture of Oracle United States Field Office webpage, available at https://web.archive.org/web/20220628184410/https://www.oracle.com/corporate/contact/field-offices.html (last accessed July 26, 2022).

Texas

World Headquarters	Frisco	San Antonio
2300 Oracle Way Austin, TX 78741 Phone: +1.737.867.1000	7460 Warren Parkway Suite 300 Frisco, TX 75034 Phone: +1.972.963.2300 Fax: +1.972.963.2301	613 NW Loop 410 Suite 1000 San Antonio, TX 78216-5507 Phone: +1.210.536.9200 Fax: +1.210.541.0598

And Oracle also continues to actively advertise for job openings at its Frisco office, including postings as recent as July 18, 2022. *See* Oracle Job Search, available at https://eeho.fa.us2.oraclecloud.com/hcmUI/CandidateExperience/en/sites/CX_1/requisitions/preview/174061/?keyword=texas&location=United+States&locationId=300000000149325&locationLevel=country (last accessed July 26, 2022); *see also* https://www.linkedin.com/jobs/search/?currentJobId=3167415611&keywords=oracle%20frisco; https://www.linkedin.com/jobs/search/?keywords=oracle%20frisco&origin=BLENDED_SEARCH_RESULT_CARD_NAVIGATION&currentJobId=3153688404; https://www.linkedin.com/jobs/search/?currentJobId=3141988447&keywords=oracle%20frisco; https://www.linkedin.com/jobs/search/?currentJobId=3139070817&keywords=oracle%20frisco. On information and belief, there are Oracle employees that continue to work in Frisco, Texas. On information and belief, Oracle continues to operate a regular and established place of business in Frisco, Texas, despite removing it from their website. Oracle also provides service to customers in Carrollton, Texas, within this judicial district, and, on information and belief, maintains a regular and established place of business from which its employees provide that service. *See* Oracle Service Locations, available at https://www.oracle.com/us/support/library/service-locations-073430.pdf (last accessed July 26, 2022).

9. Oracle also acquired Federos LLC, a leading provider of cloud-enabled, AI-optimized network assurance, analytics, and automation software, on December 23, 2021. Oracle Communications Blog, Oracle Acquires Federos: Empowering service providers with AI-optimized service and network assurance, analytics, and automated orchestration, available at https://blogs.oracle.com/oracle-communications/post/oracle-acquires-federos (last accessed July 26, 2022). Federos is being "incorporated into Oracle Communications' Service and Network Orchestration portfolio." *Id.*; *see also* https://www.linkedin.com/company/federosllc/posts/?feedView=all (post stating "Federos is now a part of Oracle and we will soon post exclusively via Oracle Communications, please follow us there"). Federos' website now forwards to Oracle's Unified Assurance webpage. *See* federos.com (last accessed July 26, 2022).

10. Federos is based in Frisco, Texas, with a principal office located at 7164 Technology Drive, Frisco, Texas 75033. After the acquisition, that office has served as a regular and established place of business of Oracle.

11. Oracle also has committed acts of infringement in this judicial district. Specifically, the offers for sale, servicing, and use of infringing Oracle MPTCP Products and Oracle SD-WAN Products. For example, DATA, Inc., which maintains an office in Plano, Texas in this judicial district, is an Oracle Linux customer. *See* https://enlyft.com/tech/products/oracle-linux; https://datainc.biz/about-us/locations/.

Who uses Oracle Linux?

Some of the companies that use Oracle Linux include:

Company	Website	Country	Revenue	Company Size
Univera, Inc.	univera.com	United States	1M-10M	10-50
DATA Inc.	datainc.biz	United States	100M-200M	500-1000
Lorven Technologies	lorventech.com	United States	10M-50M	50-200
CONFIDENTIAL RECORDS, INC.	confidentialrecordsinc.com	United States	0M-1M	1-10

On information and belief, Oracle also has sold and serviced infringing SD-WAN products to customers in this judicial district.

The Patents-in-Suit

A. The ’801 Patent

12. U.S. Patent No. 8,228,801 (the ’801 patent), entitled “Broadband Communications Device,” was duly and legally issued on July 24, 2012 by the U.S. Patent and Trademark Office. The underlying application, U.S. Patent Application No. 12/581,852, was filed on October 19, 2009. It claims priority to U.S. Patent Application No. 10/686,375, filed October 14, 2003, and U.S. Provisional Patent Application Ser. No. 60/418,521, filed October 15, 2002. A true and correct copy of the ’801 patent is attached as Exhibit A and incorporated by reference.

13. The ’801 patent is directed to patent-eligible subject matter pursuant to 35 U.S.C. § 101.

14. The ’801 patent is valid and enforceable, and presumed as such, pursuant to 35 U.S.C. § 282.

15. CAS is the assignee of all right, title, and interest in the ’801 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the ’801 patent. Accordingly, CAS possesses the exclusive right and has standing to prosecute the present action for infringement of the ’801 patent by Oracle.

B. The ’649 Patent

16. U.S. Patent No. 9,350,649 (the ’649 patent), entitled “Multipath Communication Devices and Methods,” was duly and legally issued on May 24, 2016 by the U.S. Patent and Trademark Office. The underlying application, U.S. Patent Application No. 14/512,414, was filed on October 11, 2014. It claims priority to U.S. Patent Application No. 13/531,294, filed June 22, 2012, U.S. Patent Application No. 12/581,825, filed October 19, 2009, U.S. Patent Application No. 10/686,375, filed October 14, 2003, and U.S. Provisional Patent Application Ser. No. 60/418,521, filed October 15, 2002. A true and correct copy of the ’649 patent is attached as Exhibit B and incorporated by reference.

17. The ’649 patent is directed to patent-eligible subject matter pursuant to 35 U.S.C. § 101.

18. The ’649 patent is valid and enforceable, and presumed as such, pursuant to 35 U.S.C. § 282.

19. CAS is the assignee of all right, title, and interest in the ’649 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the ’649 patent. Accordingly, CAS possesses the exclusive right and has standing to prosecute the present action for infringement of the ’649 patent by Oracle.

C. The ’908 Patent

20. U.S. Patent No. 10,868,908 (the ’908 patent), entitled “Devices and Methods for Multipath Communications,” was duly and legally issued on December 15, 2020 by the U.S. Patent and Trademark Office. The underlying application, U.S. Patent Application No. 15/161,787, was filed on May 23, 2016. It claims priority to U.S. Patent Application No. 14/512,414, filed October 11, 2014, U.S. Patent Application No. 13/531,294,

filed June 22, 2012, U.S. Patent Application No. 12/581,825, filed October 19, 2009, U.S. Patent Application No. 10/686,375, filed October 14, 2003, and U.S. Provisional Patent Application Ser. No. 60/418,521, filed October 15, 2002. A true and correct copy of the '908 patent is attached as Exhibit C and incorporated by reference.

21. The '908 patent is directed to patent-eligible subject matter pursuant to 35 U.S.C. § 101.

22. The '908 patent is valid and enforceable, and presumed as such, pursuant to 35 U.S.C. § 282.

23. CAS is the assignee of all right, title, and interest in the '908 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '908 patent. Accordingly, CAS possesses the exclusive right and has standing to prosecute the present action for infringement of the '908 patent by Oracle.

CAS's History of Innovation

24. CAS was founded by Eric Delangis to support the development of his patented router technologies. While living in rural Colorado, Mr. Delangis was unable to obtain high speed internet. Rather than settle for slow dial-up internet, Mr. Delangis attempted to find a commercial solution for pooling multiple internet connections. When he was unable to locate any solutions to his problem, Mr. Delangis invented innovative router technology to route data over several internet connections, including DSL, ISDN, dial-up, and wireless connections, and combine the received data for the intended receiving device. In particular, Mr. Delangis developed a variety of systems and protocols for transmitting and receiving data in a faster and more efficient manner by transmitting data over multiple communication channels and aggregating the transmitted data

to improve the effective bandwidth between the sender and recipient of the data. The usage of multiple communication channels further provides enhanced reliability as data can be transmitted even when some of the communication channels are suffering reduced performance or are unavailable. This improves the functionality of the computer networks themselves, particularly as compared to the solutions available at the time Mr. Delangis invented his router technology. Mr. Delangis's solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.

25. The Patents-in-Suit are the result of years of research and development in networking technology by Mr. Delangis. These innovations have enabled Oracle to provide enhanced and expanded products and services to its customers, which in turn has increased revenues for Oracle.

Allegations of Patent Infringement

26. Oracle makes, uses, sells, offers for sale, and services certain software products, including its Oracle MPTCP Products and Oracle SD-WAN Products (together the "Accused Products"). The Oracle MPTCP Products include Oracle Solaris, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6, Oracle Linux 9, and products that operate in a similar manner. The Oracle SD-WAN Products include the Oracle Talari Appliances, including the Talari E50 Appliance, Talari E100 Appliance, Talari D2000 Appliance, Talari D6000 Appliance, Talari T5000 Appliance, and devices that operate in a similar manner, Oracle SD-WAN Virtual Appliances, Oracle SD-WAN Edge, Oracle SD-WAN Aware, Oracle SD-WAN Orchestration Cloud Service, Oracle SD-WAN, and devices that operate in a similar manner. Identification of the Accused Products will be supplemented as needed in Plaintiff's infringement contentions pursuant to

the Court's scheduling order and local rules. The Accused Products directly and indirectly infringe, literally or under the doctrine of equivalents, one or more claims of each of the Patents-in-Suit.

27. CAS has, to the extent required, complied with the marking statute, 35 U.S.C. § 287.

28. As set forth below, the Accused Products incorporate, without any license or permission from CAS, technology protected by the Patents-in-Suit.

Count 1: Infringement of U.S. Patent No. 8,228,801

29. CAS incorporates by reference and realleges each and every allegation of Paragraphs 1 through 28 as if set forth herein.

30. CAS owns all substantial rights, interest, and title in and to the '801 Patent, including the sole and exclusive right to prosecute this action and enforce the '801 Patent against infringers, and to collect damages for all relevant times.

31. Without a license or permission from CAS, Oracle has infringed and will continue to infringe one or more claims of the '801 patent, directly or indirectly, by making, having made, using, offering for sale, or selling the Accused Products in violation of 35 U.S.C. § 271.

32. Oracle enables and induces its customers to infringe one or more claims of the '801 patent by providing documentation and support services to its customers which direct its customers to directly infringe one or more claims of the '801 patent. Oracle aids, instructs, supports and otherwise acts with the intent to cause an end user to use the Accused Products in a manner that infringes one or more claims of the '801 patent. Oracle has had knowledge of the '801 patent at least since the filing of this complaint.

33. Oracle's infringement is willful, at least beginning with the filing of this complaint.

34. Oracle's acts of infringement of the '801 patent have caused and will continue to cause CAS damages for which CAS is entitled compensation pursuant to 35 U.S.C. § 284, in the form of lost profits, a reasonable royalty, or some other method to be proved at trial.

35. On information and belief, Oracle has directly and indirectly infringed one or more claims of the '801 patent under 35 U.S.C. § 271(a) in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for sale, and servicing the Oracle MPTCP Products that satisfy every limitation of at least claim 1 of the '801 patent. If any limitation of claim 1 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

36. Exemplary claim charts detailing representative infringement by the Oracle MPTCP Products of claim 1 of the '801 patent are attached as Exhibit D.

37. On information and belief, Oracle has directly and indirectly infringed one or more claims of the '801 patent under 35 U.S.C. § 271(a) in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for sale, and servicing the Oracle SD-WAN Products that satisfy every limitation of at least claim 10 of the '801 patent. If any limitation of claim 10 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

38. Exemplary claim charts detailing representative infringement by the Oracle SD-WAN Products of claim 10 of the '801 patent are attached as Exhibit E.

Count 2: Infringement of U.S. Patent No. 9,350,649

39. CAS incorporates by reference and realleges each and every allegation of Paragraphs 1 through 38 as if set forth herein.

40. CAS owns all substantial rights, interest, and title in and to the '649 Patent, including the sole and exclusive right to prosecute this action and enforce the '649 Patent against infringers, and to collect damages for all relevant times.

41. Without a license or permission from CAS, Oracle has infringed and will continue to infringe one or more claims of the '649 patent, directly or indirectly, by making, having made, using, offering for sale, or selling the Accused Products in violation of 35 U.S.C. § 271.

42. Oracle enables and induces its customers to infringe one or more claims of the '649 patent by providing documentation and support services to its customers which direct its customers to directly infringe one or more claims of the '649 patent. Oracle aids, instructs, supports and otherwise acts with the intent to cause an end user to use the Accused Products in a manner that infringes one or more claims of the '649 patent. Oracle has had knowledge of the '649 patent at least since the filing of this complaint.

43. Oracle's infringement is willful, at least beginning with the filing of this complaint.

44. Oracle's acts of infringement of the '649 patent have caused and will continue to cause CAS damages for which CAS is entitled compensation pursuant to 35 U.S.C. § 284.

45. On information and belief, Oracle has directly and indirectly infringed one or more claims of the '649 patent in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for

sale, and servicing the Oracle MPTCP Products that satisfy every limitation of at least claim 7 of the ’649 patent. If any limitation of claim 7 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

46. Attached as Exhibit F are exemplary claim charts detailing representative infringement of claim 7 of the ’649 patent.

47. On information and belief, Oracle has directly and indirectly infringed one or more claims of the ’649 patent in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for sale, and servicing the Oracle SD-WAN Products that satisfy every limitation of at least claim 1 of the ’649 patent. If any limitation of claim 1 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

48. Attached as Exhibit G are exemplary claim charts detailing representative infringement of claim 1 of the ’649 patent.

Count 3: Infringement of U.S. Patent No. 10,868,908

49. CAS incorporates by reference and realleges each and every allegation of Paragraphs 1 through 48 as if set forth herein.

50. CAS owns all substantial rights, interest, and title in and to the ’908 Patent, including the sole and exclusive right to prosecute this action and enforce the ’908 Patent against infringers, and to collect damages for all relevant times.

51. Without a license or permission from CAS, Oracle has infringed and will continue to infringe one or more claims of the ’908 patent, directly or indirectly, by making, having made, using, offering for sale, or selling the Accused Products in violation of 35 U.S.C. § 271.

52. Oracle enables and induces its customers to infringe one or more claims of the ’908 patent by providing documentation and support services to its customers which direct its customers to directly infringe one or more claims of the ’908 patent. Oracle aids, instructs, supports and otherwise acts with the intent to cause an end user to use the Accused Products in a manner that infringes one or more claims of the ’908 patent. Oracle has had knowledge of the ’908 patent at least since the filing of this complaint.

53. Oracle’s infringement is willful, at least beginning with the filing of this complaint.

54. Oracle’s acts of infringement of the ’908 patent have caused and will continue to cause CAS damages for which CAS is entitled compensation pursuant to 35 U.S.C. § 284.

55. On information and belief, Oracle has directly and indirectly infringed one or more claims of the ’908 patent in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for sale, and servicing the Oracle MPTCP Products that satisfy every limitation of at least claim 1 of the ’908 patent. If any limitation of claim 1 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

56. Exemplary claim charts detailing representative infringement of claim 1 of the ’908 patent are attached as Exhibit H.

57. On information and belief, Oracle has directly and indirectly infringed one or more claims of the ’908 patent in the Eastern District of Texas, the State of Texas, and elsewhere in the United States, by at least making, using, testing, selling, offering for sale, and servicing the Oracle SD-WAN Products that satisfy every limitation of at

least claim 13 of the ’908 patent. If any limitation of claim 13 is not practiced in a literal sense, then that limitation is present under the doctrine of equivalents.

58. Exemplary claim charts detailing representative infringement of claim 13 of the ’908 patent are attached as Exhibit I.

Jury Demand

59. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, CAS respectfully requests a trial by jury of any issues so triable by right.

Prayer for Relief

Wherefore, CAS requests judgment against Oracle Corporation and Oracle America, Inc. as follows:

A. Adjudging that Oracle Corporation and Oracle America, Inc. have directly infringed the ’801 patent, in violation of 35 U.S.C. § 271(a);

B. Adjudging that Oracle Corporation and Oracle America, Inc. have directly infringed the ’649 patent, in violation of 35 U.S.C. § 271(a);

C. Adjudging that Oracle Corporation and Oracle America, Inc. have directly infringed the ’908 patent, in violation of 35 U.S.C. § 271(a);

D. Adjudging that Oracle Corporation and Oracle America, Inc. have indirectly infringed the Patents-in-Suit by inducing its customer’s direct infringement of the Patents-in-Suit and hold Oracle Corporation and Oracle America, Inc. liable for such infringement;

E. Ordering Oracle Corporation and Oracle America, Inc. to account for and pay damages adequate to compensate CAS for Oracle Corporation’s and Oracle America, Inc.’s infringement of the ’801 patent, ’649 patent, and the ’908 patent, including pre-judgment and post-judgment interest and costs, pursuant to 35 U.S.C. § 284;

F. Ordering an accounting by Oracle Corporation and Oracle America, Inc. for any infringing activity not presented at trial and an award by the court of additional damages for any such infringing activity to CAS;

G. Ordering that the damages award by increased up to three times the actual amount assessed, pursuant to 35 U.S.C. § 284;

H. Declaring this case exceptional and ordering Oracle Corporation and Oracle America, Inc. to pay the cost of this action, including all disbursements, and attorneys' fees as provided by 35 U.S.C. § 285, together with prejudgment interest; and

I. Awarding such other and further relief as this Court deems just and proper.

Dated: July 27, 2022

Respectfully submitted,

/s/ James A. Shimota by permission Wesley Hill
James A. Shimota – Lead Attorney (*p.h.v.* to be filed)
Patrick D. Richards (*p.h.v.* to be filed)
K&L GATES LLP
70 WEST Madison Street, Suite 3300
Chicago, Illinois 60602
Telephone: (312) 372-1121
Fax: (312) 827-8000
jim.shimota@klgates.com
patrick.richards@klgates.com

Nicholas F. Lenning (*p.h.v.* to be filed)
K&L GATES LLP
925 Fourth Avenue, Suite 2900
Seattle, Washington 98104
Telephone: (206) 370-6685
Fax: (206) 370-6006
nicholas.lenning@klgates.com

Wesley Hill
Texas Bar No. 24032294
E-mail: wh@wsfirm.com

Claire Abernathy Henry
TX State Bar No. 24053063
E-mail: claire@wsfirm.com
Andrea L. Fair
Texas Bar No. 24078488
E-mail: andrea@wsfirm.com
Ward, Smith & Hill, PLLC
1507 Bill Owens Parkway
P.O. Box 1231
Longview, Texas 75606
Telephone: (903) 757-6400
Fax: (903) 757-2323

Counsel for Plaintiff
Competitive Access Systems, Inc.

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The 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, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Competitive Access Systems, Inc.

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Wesley Hill, WARD, SMITH & HILL, PLLC, 1507 Bill Owens Parkway, Longview, Texas 75604, (903) 757-6400

DEFENDANTS

Oracle Corporation and Oracle America, Inc.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☒ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
35 U.S.C. §§ 1 et seq

Brief description of cause:
Patent Infringement

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
7/27/2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ James Shimota (by permission Wesley Hill)

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

EXHIBIT A

US008228801B2

(12) **United States Patent**
Delangis

(10) **Patent No.: US 8,228,801 B2**
(45) **Date of Patent: Jul. 24, 2012**

(54) **BROADBAND COMMUNICATIONS DEVICE**

(76) Inventor: **Eric M. Delangis**, Loveland, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 466 days.

(21) Appl. No.: **12/581,852**

(22) Filed: **Oct. 19, 2009**

(65) **Prior Publication Data**

US 2010/0098058 A1 Apr. 22, 2010

Related U.S. Application Data

(63) Continuation of application No. 10/686,375, filed on Oct. 14, 2003, now Pat. No. 7,606,156.

(60) Provisional application No. 60/418,521, filed on Oct. 15, 2002.

(51) **Int. Cl.**
H04L 12/26 (2006.01)
H04L 12/28 (2006.01)

(52) **U.S. Cl.** **370/235**; 370/401

(58) **Field of Classification Search** 370/235, 370/230, 233, 363, 371, 374, 381, 401, 433, 370/465–468, 470–474, 483–486, 493–495, 370/352, 395, 252

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,307,839	B1 *	10/2001	Gerszberg et al.	370/235
7,257,106	B2 *	8/2007	Chen et al.	370/338
7,385,924	B1 *	6/2008	Riddle	370/235
2006/0079274	A1 *	4/2006	Gallagher et al.	455/552.1

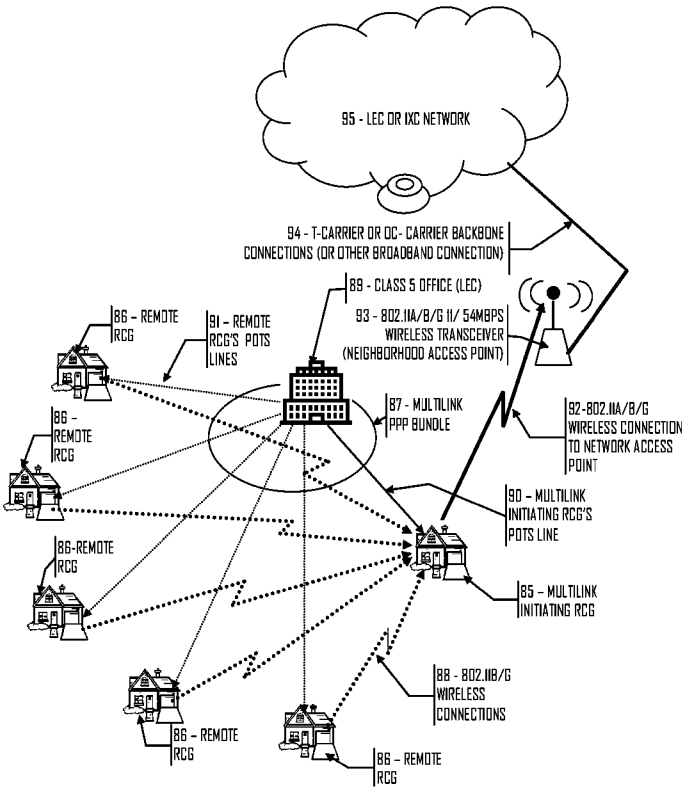
* cited by examiner

Primary Examiner — Hong Cho
(74) *Attorney, Agent, or Firm* — Clay McGurk; The Law Office of Clay McGurk

(57) **ABSTRACT**

The Residential Communications Gateway (RCG) is a broadband communications device that combines all voice, data and video communications to and from a typical residence or small business for transmission over a single, or a plurality of Plain Old Telephone Service (POTS) lines separately or in conjunction with, a wireless broadband backbone. The RCG does this by employing packetized data with Voice over Internet Protocol (VoIP) technologies combined with RF communications technologies. A key consideration to the design of the RCG is that no additional or special transmission equipment must be installed at the Central Office or anywhere else in the network to enable new calling features provided by the RCG as is the case with DSL and Cable systems. By eliminating the requirement for costly infrastructure enhancements, ubiquitous high speed communications and services can be deployed to every POTS subscriber.

17 Claims, 9 Drawing Sheets



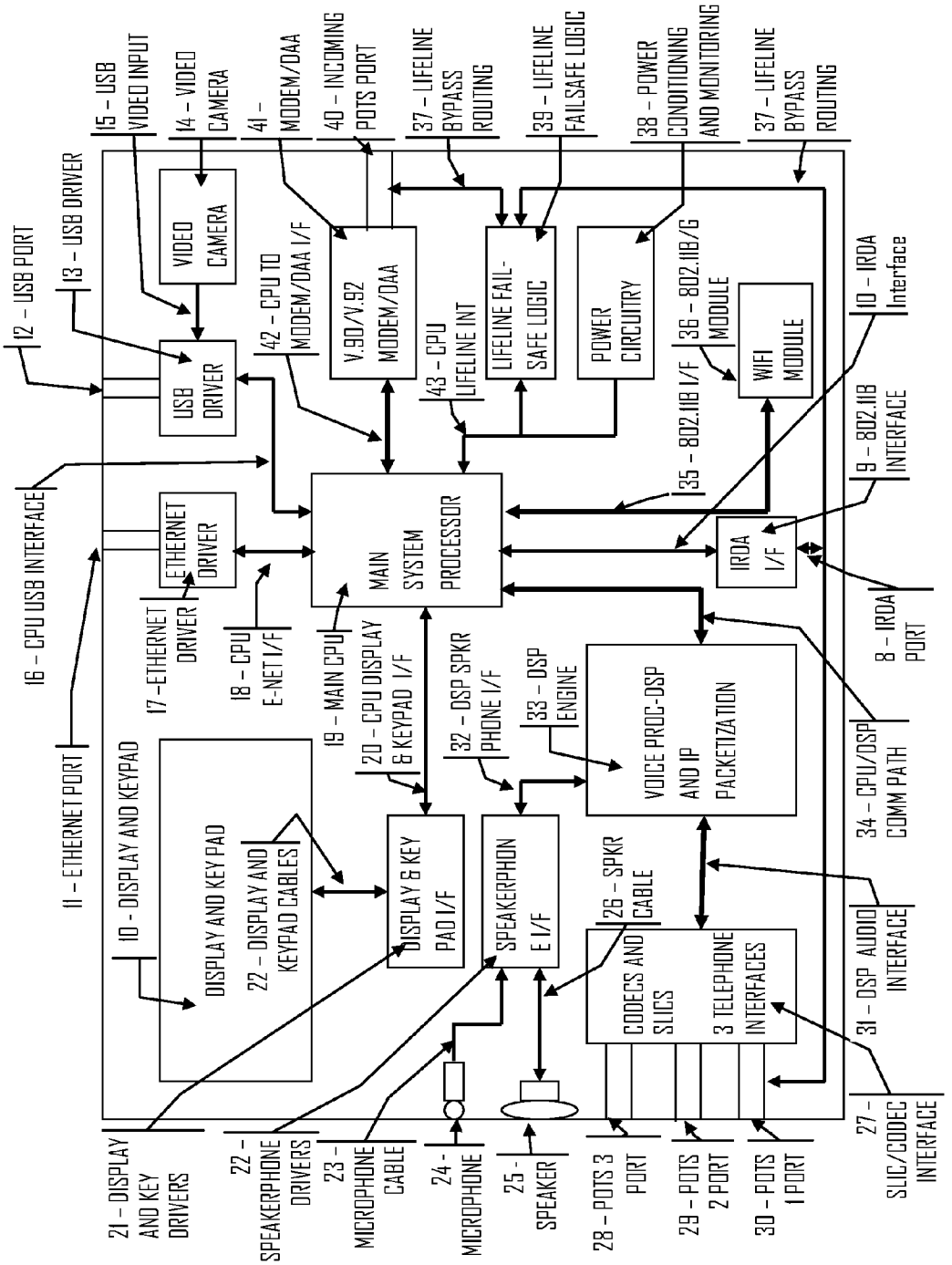

15 – USB VIDEO INPUT
14 – VIDEO CAMERA
41 – MODEM/DAA
40 – INCOMING POTS PORT
37 – LIFELINE BYPASS ROUTING
39 – LIFELINE FAILSAFE LOGIC
38 – POWER CONDITIONING AND MONITORING
37 – LIFELINE BYPASS ROUTING
12 – USB PORT
13 – USB DRIVER
VIDEO CAMERA
USB DRIVER
42 – CPU TO MODEM/DAA I/F
V.90/V.92 MODEM/DAA
43 – CPU LIFELINE INT
LIFELINE FAIL-SAFE LOGIC
POWER CIRCUITRY
36 – 802.11B/G MODULE
WIFI MODULE
10 – IRDA Interface
35 – 802.11B I/F
9 – 802.11B INTERFACE
16 – CPU USB INTERFACE
ETHERNET DRIVER
MAIN SYSTEM PROCESSOR
IRDA I/F
17 – ETHERNET DRIVER
18 – CPU E-NET I/F
19 – MAIN CPU
20 – CPU DISPLAY & KEYPAD I/F
32 – DSP SPKR PHONE I/F
33 – DSP ENGINE
VOICE PROC-DSP AND IP PACKETIZATION
8 – IRDA PORT
11 – ETHERNET PORT
10 – DISPLAY AND KEYPAD
DISPLAY AND KEYPAD
22 – DISPLAY AND KEYPAD CABLES
DISPLAY & KEY PAD I/F
SPEAKERPHON E I/F
26 – SPKR CABLE
CODECS AND SLICS
3 TELEPHONE INTERFACES
34 – CPU/DSP COMM PATH
31 – DSP AUDIO INTERFACE
27 – SLIC/CODEC INTERFACE
21 – DISPLAY AND KEY DRIVERS
22 – SPEAKERPHONE DRIVERS
23 – MICROPHONE CABLE
24 – MICROPHONE
25 – SPEAKER
28 – POTS 3 PORT
29 – POTS 2 PORT
30 – POTS 1 PORT

FIG. 1

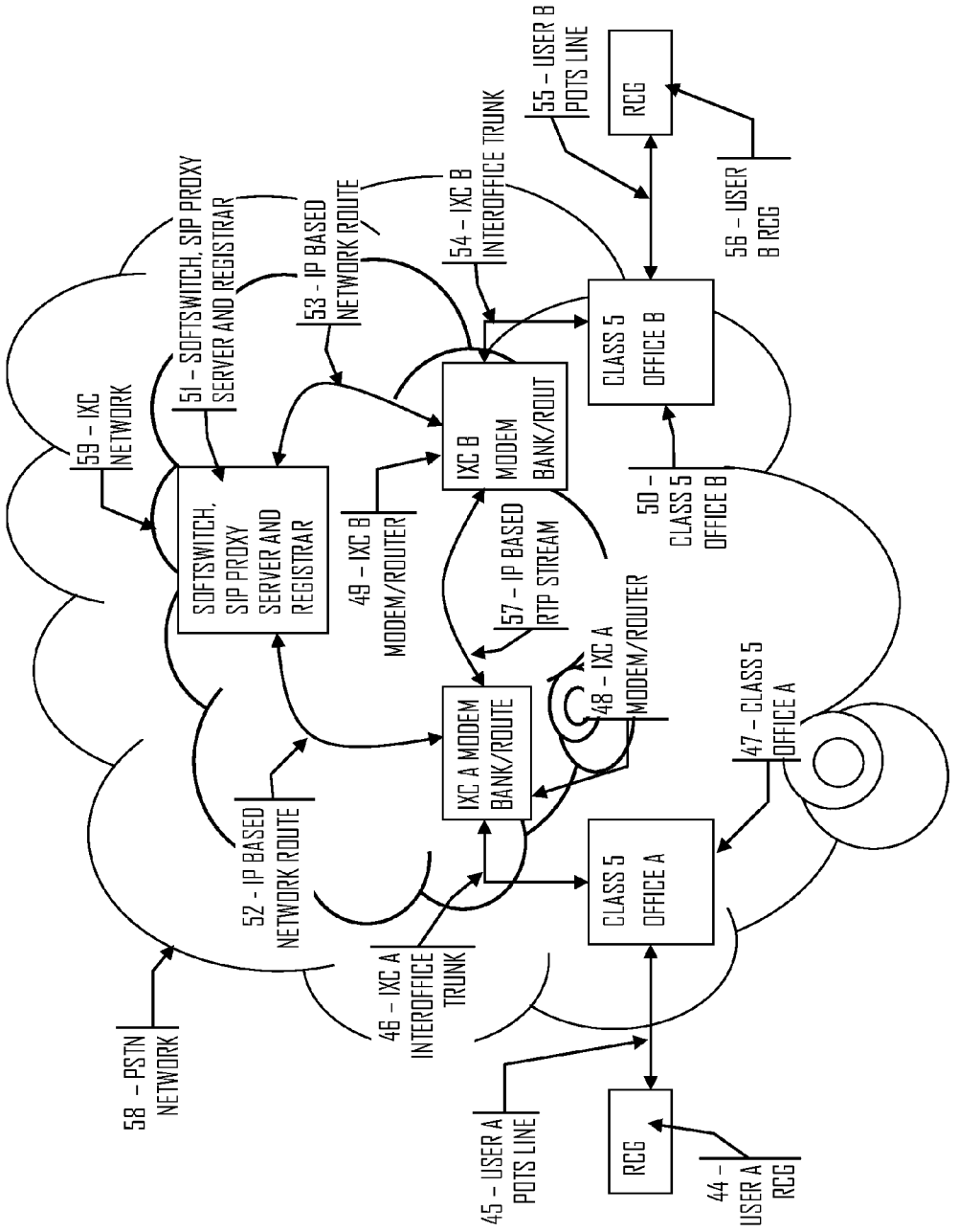

59 – IXC NETWORK
51 – SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
53 - IP BASED NETWORK ROUTE
54 – IXC B INTEROFFICE TRUNK
55 – USER B POTS LINE
RCG
56 – USER B RCG
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
49 – IXC B MODEM/ROUTER
IXC B MODEM BANK/ROUT
CLASS 5 OFFICE B
50 – CLASS 5 OFFICE B
57 – IP BASED RTP STREAM
48 – IXC A MODEM/ROUTER
IXC A MODEM BANK/ROUTE
47 – CLASS 5 OFFICE A
52 - IP BASED NETWORK ROUTE
CLASS 5 OFFICE A
46 – IXC A INTEROFFICE TRUNK
58 – PSTN NETWORK
45 – USER A POTS LINE
RCG
44 – USER A RCG

FIG. 2

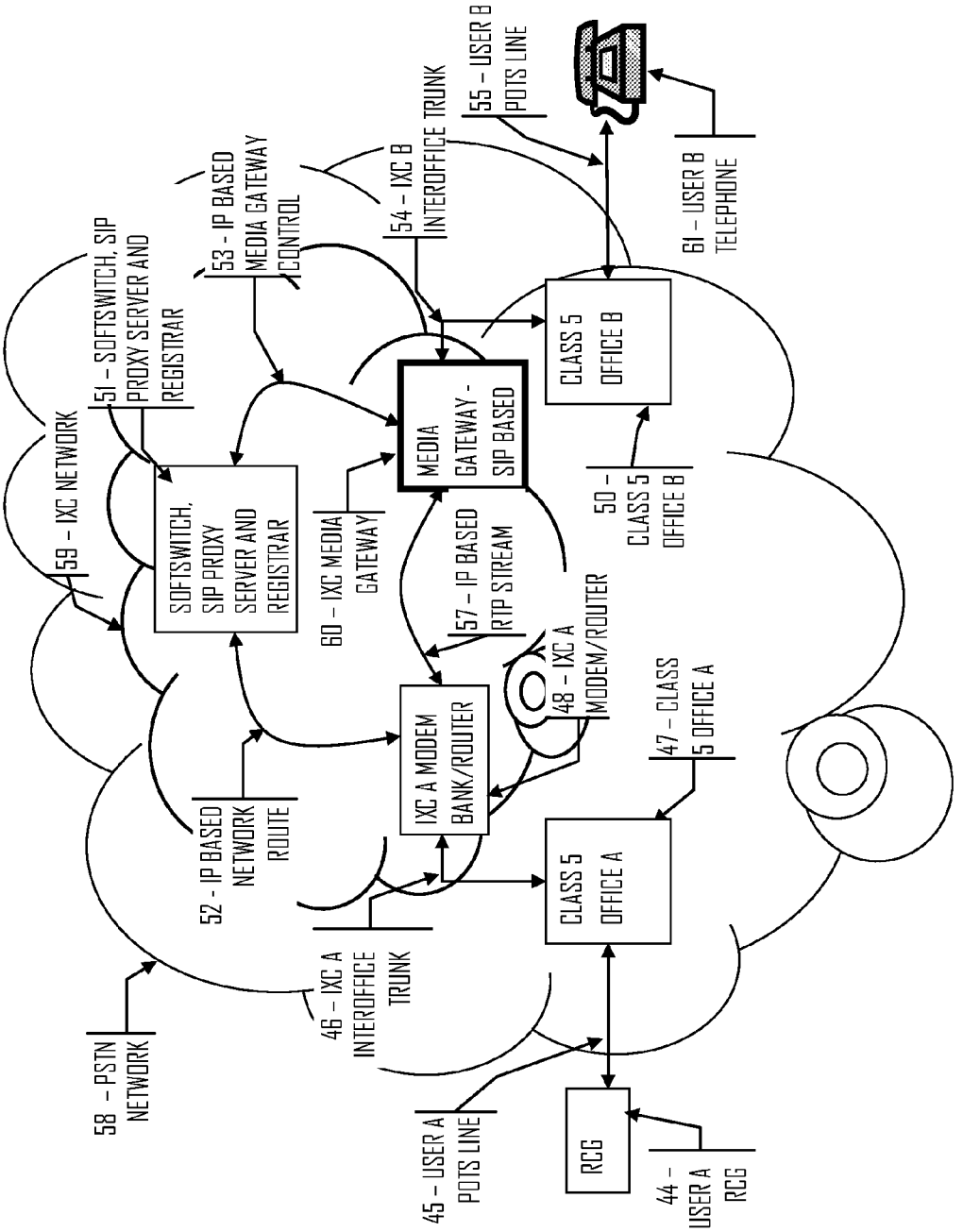

59 – IXC NETWORK
51 – SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
53 - IP BASED MEDIA GATEWAY CONTROL
54 – IXC B INTEROFFICE TRUNK
55 – USER B POTS LINE
61 – USER B TELEPHONE
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
60 – IXC MEDIA GATEWAY
MEDIA GATEWAY - SIP BASED
CLASS 5 OFFICE B
50 – CLASS 5 OFFICE B
57 – IP BASED RTP STREAM
48 – IXC A MODEM/ROUTER
47 – CLASS 5 OFFICE A
52 - IP BASED NETWORK ROUTE
IXC A MODEM BANK/ROUTER
CLASS 5 OFFICE A
46 – IXC A INTEROFFICE TRUNK
58 – PSTN NETWORK
45 – USER A POTS LINE
RCG
44 – USER A RCG

FIG. 3

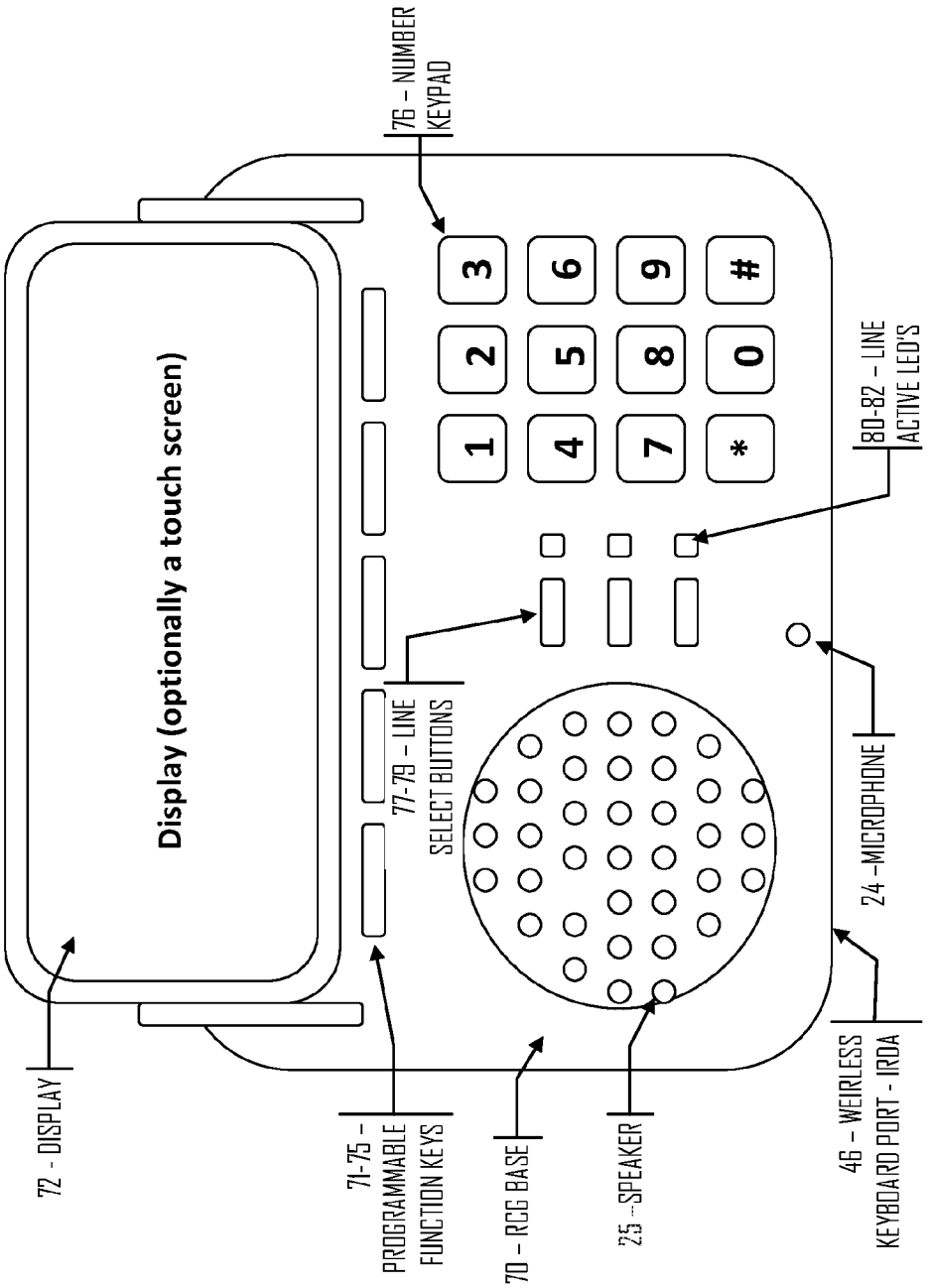

Display (optionally a touch screen)
1
2
3
4
5
6
7
8
9
*
0
#
76 - NUMBER KEYPAD
80-82 - LINE ACTIVE LED'S
77-79 - LINE SELECT BUTTONS
24 -MICROPHONE
72 - DISPLAY
71-75 - PROGRAMMABLE FUNCTION KEYS
70 - RCG BASE
25 -SPEAKER
46 - WEIRLESS KEYBOARD PORT - IRDA

FIG. 4

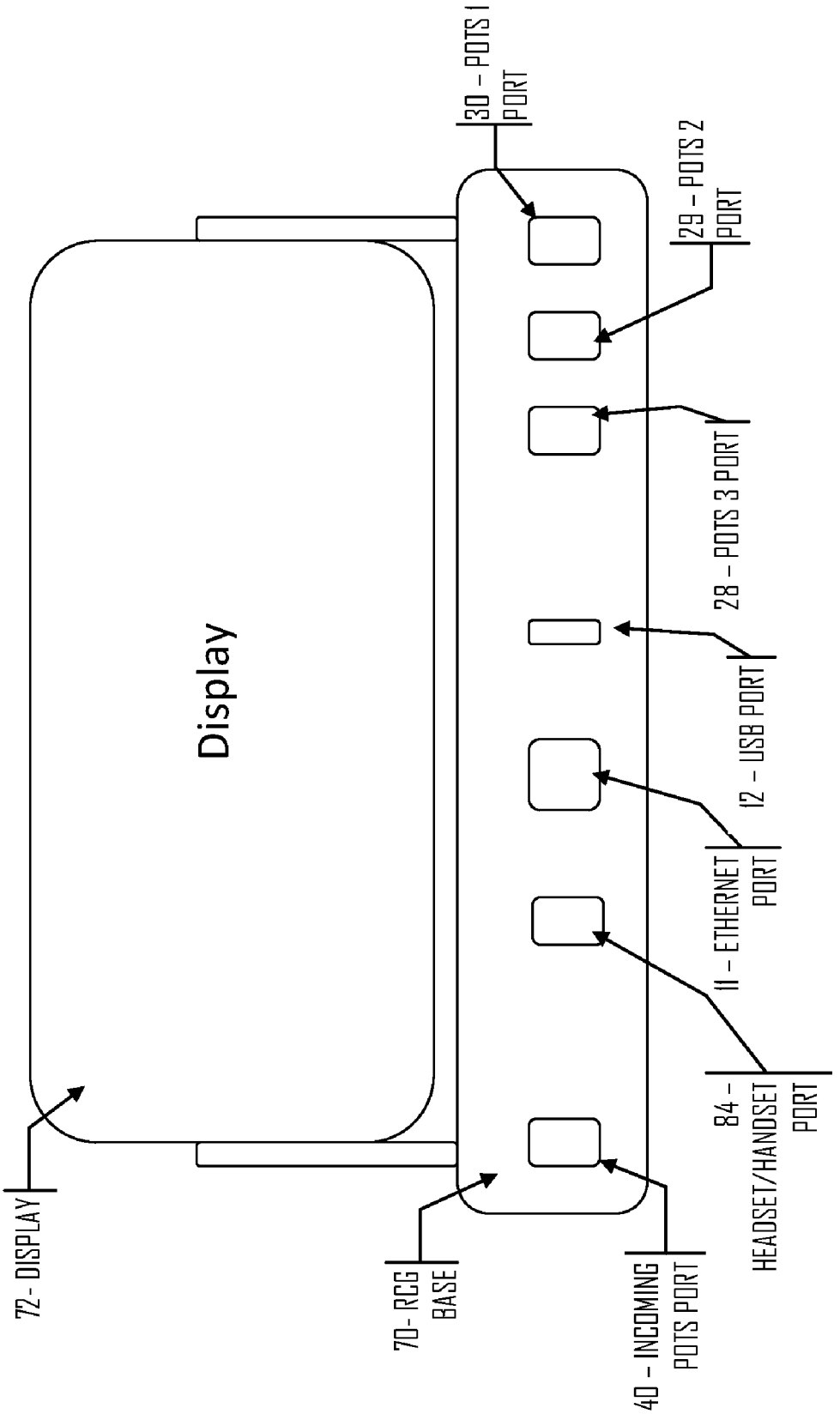

Display
72- DISPLAY
70- RCG BASE
40 – INCOMING POTS PORT
84 – HEADSET/HANDSET PORT
11 – ETHERNET PORT
12 – USB PORT
28 – POTS 3 PORT
29 – POTS 2 PORT
30 – POTS 1 PORT

FIG. 5

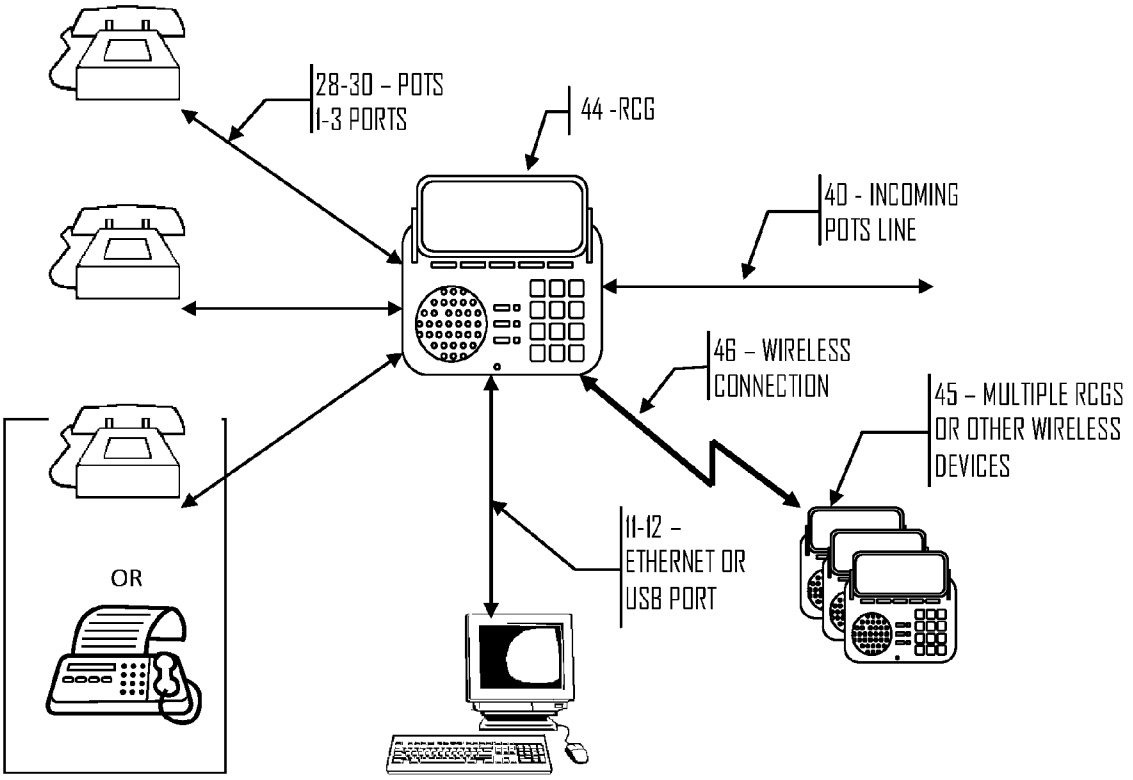

28-30 – POTS
1-3 PORTS
44 -RCG
40 - INCOMING
POTS LINE
46 – WIRELESS
CONNECTION
45 – MULTIPLE RCGS
OR OTHER WIRELESS
DEVICES
11-12 –
ETHERNET OR
USB PORT
OR

FIG. 6

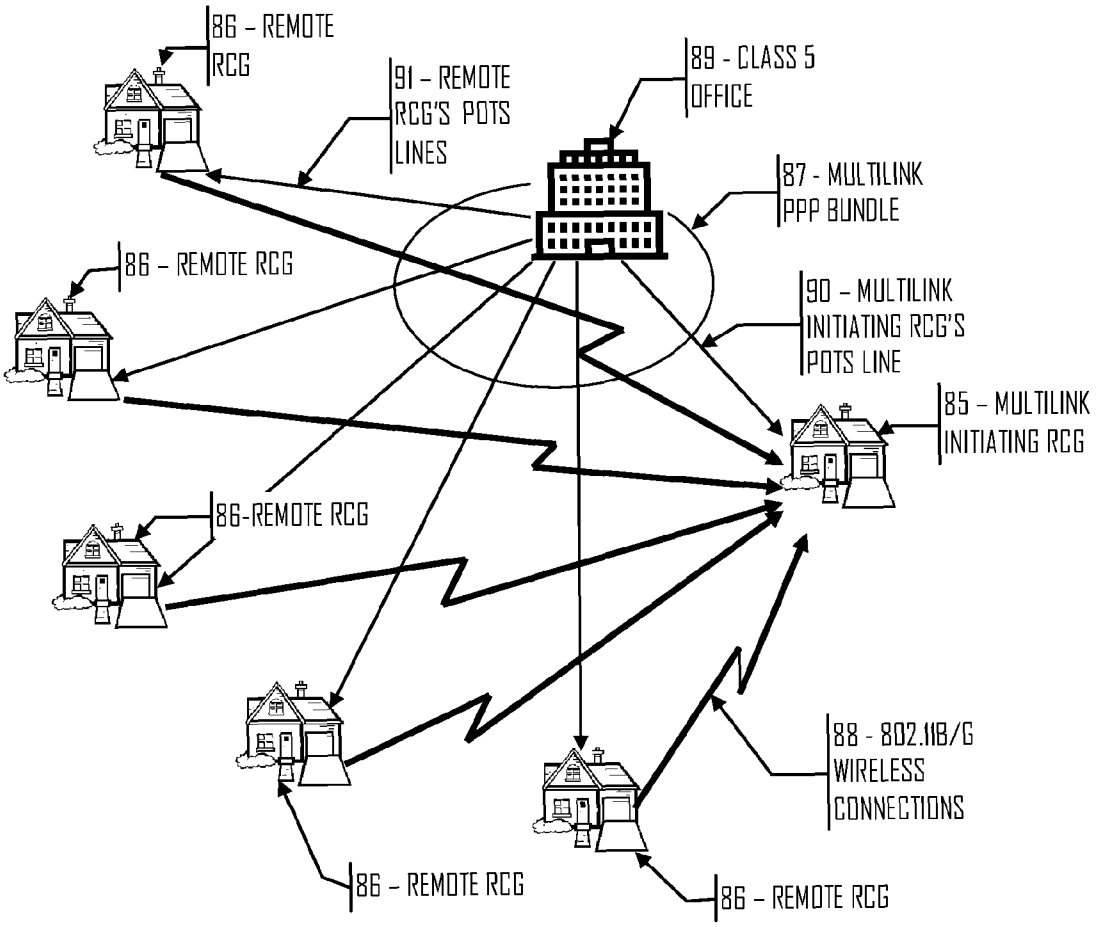

86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
85 – MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG

FIG. 7

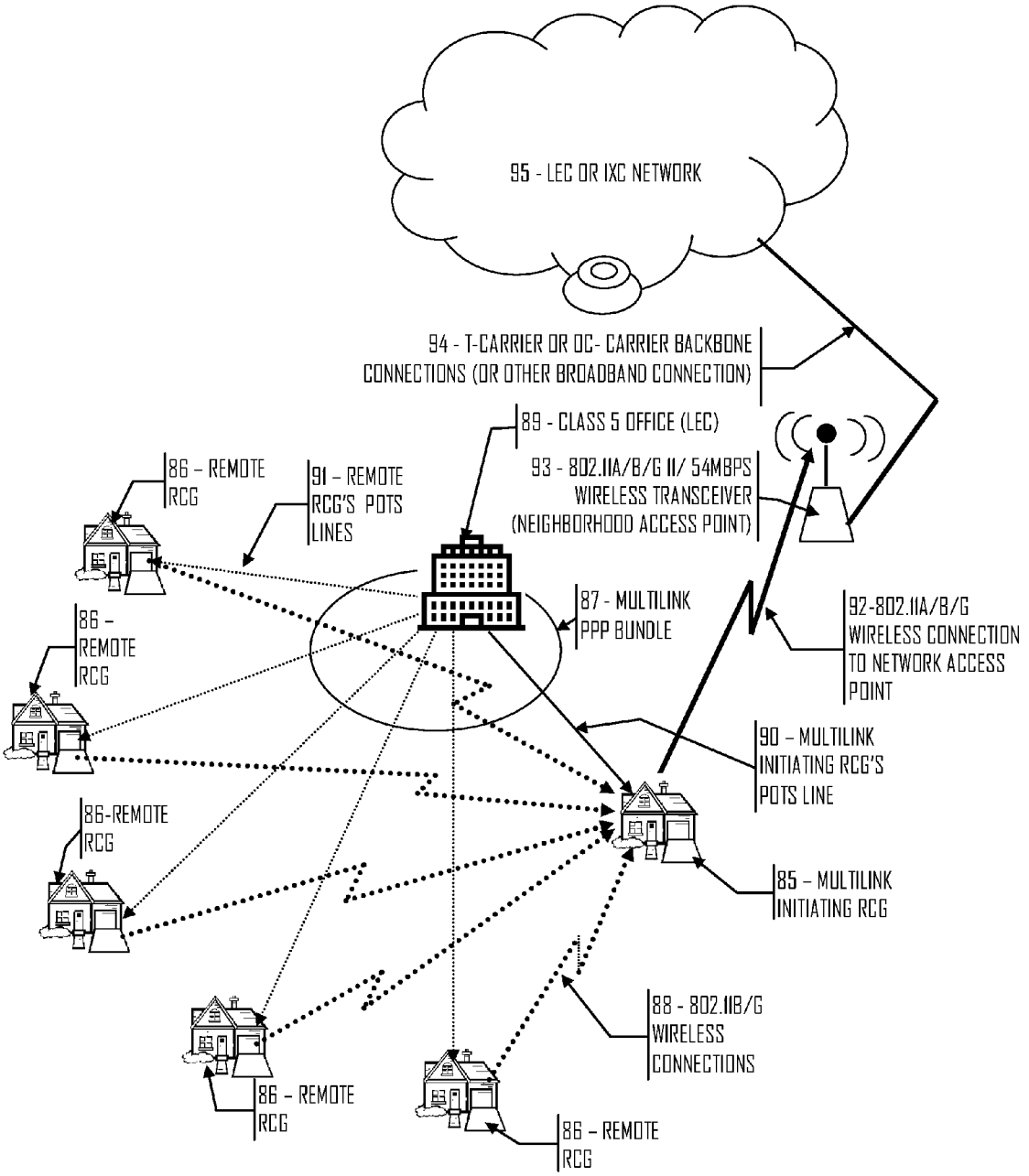

95 - LEC OR IXC NETWORK
94 - T-CARRIER OR OC- CARRIER BACKBONE CONNECTIONS (OR OTHER BROADBAND CONNECTION)
89 - CLASS 5 OFFICE (LEC)
93 - 802.11A/B/G II/ 54MBPS WIRELESS TRANSCEIVER (NEIGHBORHOOD ACCESS POINT)
86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
87 - MULTILINK PPP BUNDLE
92-802.11A/B/G WIRELESS CONNECTION TO NETWORK ACCESS POINT
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
86-REMOTE RCG
85 – MULTILINK INITIATING RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG

FIG. 8

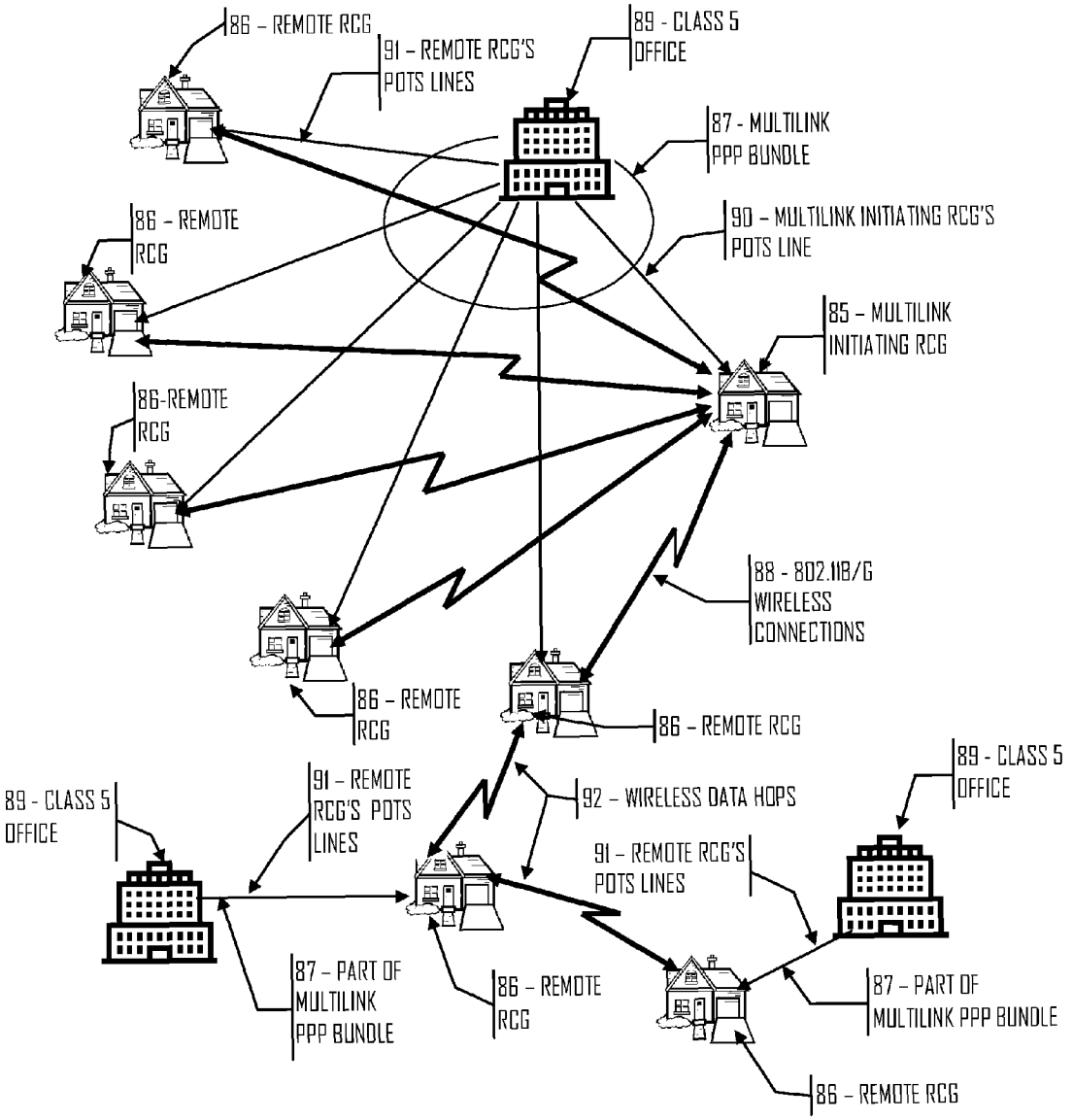

86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
85 – MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG
89 - CLASS 5 OFFICE
91 – REMOTE RCG'S POTS LINES
92 – WIRELESS DATA HOPS
89 - CLASS 5 OFFICE
91 – REMOTE RCG'S POTS LINES
87 – PART OF MULTILINK PPP BUNDLE
86 – REMOTE RCG
87 – PART OF MULTILINK PPP BUNDLE
86 – REMOTE RCG

FIG. 9

BROADBAND COMMUNICATIONS DEVICE

RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 10/686,375 filed Oct. 14, 2003, which claims priority to U.S. Provisional Application Ser. No. 60/418,521, filed Oct. 15, 2002, all of which are incorporated by reference herein.

BACKGROUND OF INVENTION

The primary function of the RCG is to provide a platform for Competitive Local Exchange Companies (CLECs) to compete with the Local Exchange Companies (LECs) for residential voice and data services. The LECs have a strangle hold on the "last mile" of copper over which almost all residential customers receive their communications services. Today, most CLECs resell the existing services that are offered by the LECs. CLECs make their money by purchasing these services from the LECs at a discount and marking them up to the customer. Since these services are regulated and controlled by the Public Utilities Commission (PUC) the pricing for these services to the CLECs is set. The monthly CLEC discount is approximately $5 to $6 per line per month for basic rate services. This means, in practicality, that a CLEC can only charge an additional $5 or $6 to the residential customer for basic rate services otherwise they would be more expensive than the LEC, and no one would buy the services from them; telephone customers would simply stay with the LEC.

To be competitive then, CLECs try to sell additional services such as call waiting, caller ID, etc. where they have as much as a 50% margin. Some CLECs also bundle long distance services with their packages as additional incentive to get residential customers to buy local telephone service from them. Since long distance fees are as low as pennies per minute to the customer, there is little profit in long distance for the CLECs. As it is, the pricing structure is such that the LECs will stay in control of the residential market, and the CLECs are nothing more than a marketing arm of the LEC. This structure also keeps the CLECs at an equal competitive advantage, or disadvantage, with respect to each other. The only thing that one CLEC could do to gain more customers is to be a better marketier. Since the CLECs are unable to discount their services because their margins are too slim as it is, the net effect is that the consumer looses by not really getting competition in the residential markets, and prices are kept artificially high.

For the CLECs to be truly competitive in the local telecommunications markets, they must be able to do more than simply resell the LECs services. CLECs must be able to offer many more features or services than those that the LEC provides, and they must be able to do this at a lower cost, in order to attract new customers.

So, what new services can the CLECs offer? As things stand today there are none, with the exception of DSL or Cable services which require tremendous infrastructure costs on behalf of the CLEC. However, by deploying an RCG in a residence, CLECs can offer advanced new calling features and services over the existing POTS line. Their costs for the POTS line from the LEC remains the same, but they can now

charge for high bandwidth data services as well as additional calling and messaging features that the LECs cannot offer. This is their competitive advantage.

Competition:

Many companies are currently trying to provide VoIP services to residential customers over high-speed or broadband backbones such as DSL and cable modems, over Internet connections via a computer. The high-speed services require expensive infrastructure enhancements to the local telephone companies' facilities and cable plants, as well as expensive modems at the customer's end. These services are also difficult to deploy and too complicated for the average user. Internet based VoIP services suffer from Internet delays caused by a lack of true Quality of Service (QOS) capabilities across the Internet. Existing VoIP services also require access to a computer and a technical knowledge to be able to make it work. Because of these problems, VoIP services are primarily targeted at the corporate market place where private IP networks that can carry VoIP services with a true guaranteed QOS exist, or can be controlled.

The only available alternatives for the residential user for high speed services are DSL and cable modems. DSL and Cable based communications reach only a small segment of the population, and growth has failed to live up to initial expectations. The recent collapse of the internet boom has led to the failure of many DSL service providers and has effectively eliminated DSL as a potential service for most POTS users for the immediate future.

SUMMARY OF THE INVENTION

The RCG combines the capabilities and features of IP routers, Class 5 circuit switches and wireless LANs in a small stand-alone external modem like device. Additional capabilities for a hands-free speakerphone device with a large touch display are also detailed. The RCG can employ a large display with sufficient resolution to provide a functional user interface to access all of the advanced features offered by the RCG, but also to be able to provide video telephone services.

The device is placed in a residence and connected to the primary POTS line coming from the LEC. Up to three standard telephones or FAX machines (or any combination) are typically connected into the RCG. It also has a Universal Serial Bus (USB) and/or a 10-100 Ethernet interface for connection to a computer or a Local Area Network (LAN). In addition, it has an 802.11b/g wireless interface for wireless home networking as well as broadband-to-the-home services.

The system is installed in a customer's home by simply plugging it into the existing incoming telephone line that provides POTS services from the LEC. One or more standard telephones are then plugged into its three line-output jacks. This is the simplest and most basic usage. In this implementation, the user only is interested in gaining additional telephone lines into the household. No computer connection is required in order to use the system. However, if data communications are desired, then there are three additional interfaces for computer connectivity. Typically either an Ethernet port, USB port or firewire (IEEE 1394) port is used to connect to a PC or LAN. The 802.11b/g interface is for wireless communications between the RCG and PCs, other RCGs as well as any other types of compatible wireless devices. A version of the RCG includes a speakerphone and video camera to provided for video telephone services.

Services Provided by the RCG:

The following discussion refers to FIG. **1**. The RCG has a main system processor that is responsible for all house keeping and traffic routing tasks. The Main CPU **19** routes data to

and from the Ethernet Port **11**, USB Port **12**, Modem/DAA **41**, DSP Engine **33**, 802.11b/g Module **36** and the Display and Keypad **10**.

The RCG provides a total telecommunications communications services package for residential and small business customers. With the RCG, a CLEC can offer its customers dialtone for up to three separate telephone numbers per residence (the limit of three telephone numbers is an arbitrary number based upon typical residential usage and is not a limit imposed by the system), all local and long distance services, 24/7 always-on Internet access, a host of custom messaging and calling features, as well as Broadband access and lifeline service. All of these services can be offered over a customer's existing POTS line, and it doesn't require any network infrastructure build out like DSL and Cable services. Because there is no expensive network equipment required, it can be readily deployed throughout the country to expand the CLECs customer base quickly.

The RCG is designed to enhance, not replace, the existing telephone line, enabling it to provide new combined packetized voice and data services. Meanwhile, all existing telecommunications infrastructure and equipment will continue to work seamlessly with the RCG. Aside from simply installing the low cost RCG device in the home telephone wiring, no other equipment needs to be purchased by either the home owner or telephone companies. This eliminates the tremendously expensive infrastructure costs for communications companies that are trying to provide voice services using DSL or cable modems.

The RCG VIP Home Gateway Features:

Up to three telephone lines i.e. numbers, over a single POTS line and/or wireless connection.

Ethernet, USB and IEEE 1394 computer interfaces.

Full G1, G2 and G3 FAX support.

Full support for all CLASS services.

Broadband networking for home computers and appliances as well as wide area networking using a combination of a plurality POTS lines connected to a plurality of RCGs and/or a direct wireless connection to a wireless access point. (These interfaces allow smart devices to communicate to other devices within the home, or over the Internet through the RCG.)

Automated, remote upgradability and configuration. (Requires the customer to do nothing.)

Transparent user operation. (User doesn't have to know that any new technology is being employed)

100% compatible with existing public telephone system.

Video Telephone capabilities.

No local or long distance usage charges.

No Internet access fees.

Lower monthly communication costs.

Multiple telephone calls at the same time.

Voice messaging, follow me features, call forwarding, automatic call back, conferencing, custom call routing. Home networking capabilities, all CLASS calling features, high speed broadband networking, continuous 24/7 internet access and many others.

All of these features are available even while connected to the Internet.

Very low cost of entry into the market, especially as compared to broadband alternatives.

New calling features that are not currently available to home users.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows the RCG functional block diagram with the preferred embodiment of an 802.11 wireless connection.

FIG. **2** shows the network topology for native RCG to RCG communications.

FIG. **3** shows the network topology for an RCG to PSTN call.

FIG. **4** shows the RCG top view with associated functions.

FIG. **5** shows the RCG rear view and associated connections.

FIG. **6** shows a typical application with peripheral equipment connections.

FIG. **7** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity.

FIG. **8** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with connection to a broadband neighborhood access point (Wi-Fi hot spot).

FIG. **9** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with wireless data hopping with POTS connections through numerous different Class 5 offices.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment is detailed herein using the ubiquitous 802.11 wireless protocol. It is by no means insinuated that this is the only wireless scheme that can be used by this device; rather, it is intended that any wireless transmission scheme can be used for wireless communications between this device and other wireless devices as various applications may dictate.

System Initialization

Refer to FIGS. **1**, **2** and **3** for the following discussion. When the RCG is first plugged into an AC power outlet the Main CPU **19**, performs a Power-on Self Test (POST) routine. Once the POST completes and the RCG is connected to an active POTS line, connected to the LEC, by means of the Incoming POTS Port **40**, the RCG automatically initiates a modem connection via the Modem/DAA **41**, to a registration service via a toll free 800 telephone number. The registration service connects directly to the service provider's sales or customer service offices via a VoIP connection. An operator or an automated service answers the call and sets up a new account for the customer. Once the account is set up, the service provider's network automatically sends control information to the device to store the required routing and feature/service information in its non-volatile memory of its Main CPU **19**. As part of this information, a local dialup telephone number is sent to the device that it will use for local network access in the same fashion as a standard ISP connection is made from a home computer. The URL of the Softswitch/SIP Proxy Server and Registrar **51** that will be controlling this particular device is also stored at this time. During the service activation and configuration process, the customer service operator can send test requests to the device, as well as call into it on another telephone number (assuming an additional telephone number is part of the users class of service) or the speakerphone to verify that it is configured and working properly. The final step of the configuration and initialization process is to register the device with the appropriate Softswitch/SIP Proxy Server and Registrar **51** so that the Softswitch/SIP Proxy Server and Registrar **51** knows that it is the controlling SIP Proxy for this RCG. Also configured at this time is the username/password verification server (this is a standard network device and is not shown) that is used to allow the RCG's modem to make a connection onto the service provider's network. Once the RCG configuration is completed, it disconnects the call by hanging up the Modem/DAA **41**, then dials the new local network access number that

had been sent during the configuration process and establishes a constant local network connection. This connection is maintained continuously on a 24/7 basis, and is immediately reestablished whenever it drops. Should the RCG become unable to reestablish this connection after several tries, it will switch over to failsafe mode and inform the user via the Display and Keypad **10**. The RCG will try to reestablish the connection every few minutes until it finally succeeds.

By default, the first telephone port, POTS **1** Port **30**, is assigned as the termination port for the existing POTS service that is connected to Incoming POTS Port **40**. This is the existing telephone service that the user already has as his primary telephone service from his LEC. POTS **1** Port **30**, typically has connected to it a standard telephone set that does not require any power (other than that derived over the POTS interface) to operate properly. POTS **1** Port **30** is the Lifeline telephone port for the user. In the case that all power is lost to the RCG, POTS **1** Port **30** will fail to a direct connection to the Incoming POTS Port **40** telephone line that comes into the RCG from the LEC to provide uninterrupted telephone services to the user. In this state, however, none of the enhanced VoIP services of the RCG are available to the user since the user simply has a stand POTS telephone service to the LEC.

Two additional and unique telephone numbers can be assigned to the other two telephone ports, POTS **2** Port **29** and POTS **3** Port **28**, by the service provider at any time. These numbers are drawn from a pool of available telephone numbers assigned to the service provider. POTS **2** Port **29** and POTS **3** Port **28** must to have standard telephone numbers assigned to them so that the PSTN is able to route calls from its network to these ports. For calls originating from IP based telephones, these numbers are not necessarily needed since POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** are uniquely identifiable to IP networks via their IP addresses assigned through the Dynamic Host Configuration Protocol (DHCP) at the time that the RCG establishes a connection to the service provider's network. Since POTS **2** Port **29** and POTS **3** Port **28** must have a telephone number assigned to them, it is a matter of convenience to use the assigned telephone numbers as part of their SIP address for IP routing of their data. In this way, all three user POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** are all addressed the same manor.

At this point, the user is able to take advantage of all of the RCG's features that have been activated according to his service agreement. The user can at any time connect additional telephones, a computer or a computer network to the RCG. The user will only be able to use those telephone ports (POTS **1** Port **30**, POTS **2** Port **29** or POTS **3** Port **28**) that have been activated, and assigned unique telephone numbers by the service provider. Any type of standard telephone can be connected to the three POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28**. In the event that a cordless telephone or a telephone that derives its power from an AC outlet is connected to POTS **1** Port **30**, the lifeline functionality of this port will be ineffective since the telephone itself will not operate once power is lost.

The speaker phone feature of the RCG, comprised of Speakerphone Drivers **22**, Microphone **24**, Speaker **25** and DSP Engine **33**, can be used on any of the activated telephone numbers and is by default enabled to operate on POTS **1** Port **30**. Once either of the other two telephone ports, POTS **2** Port **29** or POTS **3** Port **28**, is activated, the speakerphone function is activated for those lines as well. To use the speakerphone for any assigned telephone number, the user simply presses either the Line Select Button **79-81** for Line **1**, Line**2** or Line **3** on the face of the RCG, and the speakerphone function is activated on that line. This is convenient for answering any call directly at the RCG. The RCG may or may not have a number keypad for originating calls. This feature may be added or removed based upon the target market price points.

The determination as to which Inter Exchange Carrier (IXC) the RCG will route its data through is determined by any of a number of criteria including, but not limited to, whether the RCG is a private labeled product, or which carrier has the lowest cost routing, or if a specific carrier is specified by the customer, or and number of other considerations. The RCG can be programmed to change its routing path to any IXC at any time by the service provider. Complicated routing algorithms can be programmed into the RCG to control which IXC it will use at any time.

Failsafe Mode

During any time that the RCG is in failsafe mode i.e. Lifeline failsafe logic **39** is activated, the RCG will only be able to receive or initiate telephone calls via the telephone connected to its primary telephone port, POTS **1** Port **30** or through its speakerphone feature. In this condition, all activated telephone numbers are ported via the PSTN to the primary (first) telephone number for delivery to the user's telephone that is connected to POTS **1** Port **30**. While in failsafe mode, the modem is not activated, and the RCG appears to the local Class 5 office as a standard telephone, and the PSTN will route all incoming calls to the RCG as it normally would to any standard telephone.

Call Flow 1:

Dialed call origination from a telephone connected to an RCG POTS port and terminating at another user's RCG POTS port:

When a user picks up a telephone connected to any of the three POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28**, an off hook condition is detected by the SLIC/CODEC Interface **27** that is connected to the DSP Engine **33** by way of the DSP Audio Interface **31**. The DSP Engine **33** responds by sending digitally generated dialtone to the appropriate POTS interface over the DSP Audio Interface **31**. (Note: all BORSCHT telephony functions are performed by the DSP Engine **33** and the SLIC/CODEC Interface **27**.) Upon hearing the dialtone, the user enters the desired telephone number on his telephone keypad. The Dual Tone Multi-Frequency (DTMF) digits that the user dials are decoded within the DSP Engine **33**. The dialed digits are transferred to the Main CPU **19** via the CPU/DSP Communications Path **34**. The Main CPU **19** polls the DSP Engine **33** approximately every two milliseconds looking for data. The Main CPU **19** polling rate varies according to the process that is being performed. The CPU/DSP Communications path **34** also can generate an interrupt to force data transfer between it and the Main CPU **19**.

The Main CPU **19** generates a SIP Invite IP packet using the dialed digits as the called destination address and the URL of its local controlling SIP Proxy Server which was programmed into the RCG during the configuration process. The Main CPU **19** passes this SIP packet off to the Modem/DAA **41** for transmission over the network. The RCG Modem/DAA **41** is connected to and communicating with a modem in a modem bank located in the Inter Exchange Carrier's (IXCs) facility. This facility may actually be located in the LEC's physical plant or it may be physically located at another location.

Referring to FIG. **2**, User A RCG **44** is connected via its modem to the LEC's local Class 5 Office A **47**. In this example, the service provider's connections to the IXC A Modem Bank & Router **48** are through IXC A Inter-Office Trunks **46**. The service provider may or may not be the IXC.

If the service provider does not have its own network, then it will purchase capacity from an IXC and route its traffic to that IXC's facilities. The SIP Invite IP Packet that is sent from User A RCG **44** transits the LEC's Class 5 Office A **47** facilities and is routed to the IXC A Modem Bank/Router **48** via the IXC A Inter-Office Trunks **46**. It is the job of the router to take the IP packet and route it on to its intended destination, in this case the appropriate SIP proxy server **51**. The router uses the URL for the Softswitch/SIP Proxy Server and Registrar **51** contained in the SIP Invite to know where to route the packet. (Note: The Softswitch, SIP Proxy Server and Registrar are logical devices that may reside in a single computer system, or may be implemented as completely separate devices. In this example, the Softswitch, SIP Proxy Server and Registrar are all shown as a single physical device running these three separate processes.) The IXC A Modem Bank/Router **48** sends the SIP Invite IP packet on to Softswitch/SIP Proxy Server and Registrar **51** via an IP based network route **52**.

The SIP Proxy Server process running on Softswitch/SIP Proxy Server and Registrar **51** performs a look up to determine the termination destination for the call using the dialed digits passed along in the SIP Invite IP packet. In this example, the terminating device for User B RCG **56** is via IXC B's Modem Bank/Router **49** then through Class 5 Office B **50** and over User B POTS line **55** and finally to User B RCG **56**. Not covered in detail here is the SIP message handling since it is completely covered in IETF RFC2543. This example shows that both the originating and terminating ends of this call are controlled by the same Softswitch/SIP Proxy Server and Registrar **51** device. Where the originating and terminating ends of a call are controlled by different Softswitch/SIP Proxy Server and Registrar devices, an additional level of SIP messaging is used between the two SIP Proxy Server processes of each of the Softswitch/SIP Proxy Server and Registrar devices to locate and control the terminating location of the call. Again, that information is covered in IETF RFC2543 and is repeated here.

After the call routing is setup using SIP, and User B answers the call, the Softswitch/SIP Proxy Server and Registrar **51** device sends IP address of the originating User A RCG **44** to the User B RCG **56** and the IP address of User B RCG **56** to User A RCG **44**. Once both RCG's have the other's IP address, they then communicate directly to each other using Real Time Protocol (RTP), and the Softswitch/SIP Proxy Server and Registrar **51** device is no longer part of the connection. This direct communication is shown as IP based RTP Stream **57** between IXC A Modem Bank/Router **48** and IXC B Modem Bank/Router **49**.

On the receiving end of the call, referring back to FIG. **2**, User B RCG **56** receives the SIP Invite data stream through its Modem/DAA **41** and passes it on to the Main CPU **19**. The Main CPU **19** reassembles the SIP IP packet and interrogates the header information to determine which POTS port, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** the call is destined for based upon the dialed number contained in the SIP Invite message. The Main CPU **19** commands the DSP Engine **33** to control the SLIC/CODEC Interface **27** to apply ringing voltage to the selected POTS port to ring the phone. A corresponding SIP **180** (ringing) message is sent back to User A RCG **44** in the reverse direction. When the phone attached to the selected POTS port is answered, the off hook condition detected by the SLIC/CODEC Interface **27** is sent through the DSP Engine **33** to the Main CPU **19** that sends the SIP **200** OK message back to User A RCG **44** to let the RCG know that the call was answered by User B RCG **56** and to turn off the audible ringing tone for User B. Once the call is established, User A RCG **44** sends and ACK F12 SIP message to User B RCG **56** indicating that User A RCG **44** understands that the call setup has been completed.

The two RCGs now exchange SIP messages that include the type of voice encoding that will be used such as G.729, G.723.1, G.711 etc to configure their RTP streams so that they can reliably transfer the user information between them. At this point the call (voice data) is sent between both RCGs and a normal telephone conversation takes place between the user A and user B.

Call teardown is accomplished by either user hanging up their telephone. The RCG of the terminating end (the end that hangs up the phone first) detects the on-hook condition and sends a SIP Bye message to the other end. The other end upon receiving the SIP Bye message responds with an OK **200** SIP message and disables the appropriate POTS port that the user was using.

The Speakerphone interface can be used for either end of a telephone conversation in exactly the same way as described above except that the corresponding POTS port that the call was intended for is disabled if the call is answered via the speakerphone.

Call Flow 2:

Calls between an RCG device and a PSTN telephone:

Refer to FIG. **3** for the following discussion.

In the previous call example, the PSTN network had nothing to do since the call was over a previously established modem connection between two RCGs. In the cases where a call originates or terminates to a standard telephone serviced by a Class 5 office, the process is a bit more complicated.

When a call originates from a user via an RCG, such as User A RCG **44**, the call handling practices are exactly the same up to the point that the SIP Proxy Server process in the Softswitch, SIP Proxy Server and Registrar **51** performs a lookup to determine how to route the call. In this case, the SIP Proxy Server process determines that the call terminates at a standard PSTN telephone attached to the Class 5 Office B **50**. Since the call originates as a native VoIP service, it must be converted to a standard switched circuit based service to be able to be delivered to User B's telephone **61**. The conversion is performed by the IXC's Media Gateway **60** device. In this example, the SIP Proxy Server process routes the call via the IXC' s Media Gateway **60** device instead of through the IXC B Modem Bank/Router **49** as before. The SIP Proxy Server process sends a SIP Invite to the IXC's Media Gateway **60** device, as well as other control information, to direct the Media Gateway **60** device to terminate the call and to apply the appropriate voice compression algorithm to the media stream to convert it between switched circuit PCM format and the selected VoIP protocol. At the same time, the Softswitch process of the Softswitch, SIP Proxy Server and Registrar **51** device sends commands to the Media Gateway **60** device to cause it to route the call's PCM data to a specific channel on the IXC B Interoffice Trunk **54**. The Softswitch process then generates an SS7 ISUP message that is sent over the PSTN SS7 signaling network to the Class 5 Office B informing it of the incoming call and on which circuit the call has been placed. It is up to the PSTN at this point to ring the User B telephone **61** and process the call between the IXC's Media Gateway and the User B Telephone **61**. The Softswitch process handles the signaling conversion between the PSTN's SS7 network and the IXC's SIP messaging, as well as any other proprietary signaling schemes utilized by the IXC to control its network. The standard SS7 call control messages, such as ringing, busy, ring back etc., all have a comparable SIP call flow control messages. The Softswitch simply maps

the SS7 messages into SIP messages and visa-versa while routing the messages to the appropriate network equipment.

As in the case of a call between two RCGs, the RTP media stream (the actual call data) is routed directly be the IXC A Modem Bank/Router **48** and the IXC's Media Gateway **60** via an IP based RTP Stream **57**.

Again, call teardown is accomplished by either user hanging up their telephone. Depending which end hangs up the phone first, the associated network will generate the appropriate messages which will eventually make it back to the Softswitch process. The Softswitch process will relay the appropriate call control messages between the PSTN and the IXC's SIP based control system.

A telephone call originating from a PSTN telephone is configured and setup in the same fashion as the above description except that the originating messaging begins within the PSTN network instead of the IXC's network.

Personal Computer based communications:

Where the RCG is connected to a Personal Computer (PC) through either its USB Port **11** or Ethernet Port **12**, the RCG operates exactly as a cable or DSL type modem device. The RCG is simply a pass through for the computer's data. The RCG receives the IP packets (of whatever type) from the computer and sends the information unchanged to the Modem/DAA **41** interface for transmission over the Internet. Received information from the Internet is processed in the reverse way.

Dynamic Bandwidth Allocation:

When a modem connection is established between the RCG and the "Network", the total available bandwidth of this connection is used in a shared/prioritized fashion. Voice services (calls) take precedence over data services. Therefore, when no calls are in progress all of the available bandwidth is used by data type services such as surfing the Internet or uploading/downloading files. However, when a call is to be passed through the RCG, the required bandwidth for the call is deallocated from the data services and prioritized for the telephone call. This necessary because the Quality Of Service (QOS) is important for effective communications over electronic networks. Since the voice data is carried over a "data centric" network topology (an IP based network), call quality can suffer greatly. Every effort must be taken to eliminate or reduce the packet delay through every network element to be able to provide the best call quality. For data applications such as surfing the Internet or downloading files packet delay is acceptable and expected, and it does not affect the "quality" of the data.

Since all voice and data is transmitted as packets, there are no "time slots" or other type of "channelization" associated with the transmission of this data over either the POTS line or the wireless interface. Channelization of the voice data does occur within the SLIC/Codec Interface—**27** but is converted into IP packets by the DSP engine—**33** and is handled as packets from that point on.

Regardless of whether the call is originating or terminating at the RCG, the bandwidth allocation process is the same. When the SIP call setup messages are processed, the type of voice compression that will be used is defined. The RCG Main CPU **19** handles the IP packet flow between the DSP Engine **33**, USB Port **12**, Ethernet Port **11**, 802.11b/g Module **36** and the Modem/DAA **41** devices giving priority to the voice packets to and from the DSP Engine **33** and the Modem/DAA **41** interfaces. Voice compression algorithms create IP packets at a specified number of packets per second. These packets are handled by a timed process in the RCG. This process is started during call setup so that the packets are handled at the correct rate based upon the compression algorithm's packet generation rate. There is no priority assigned between the voice packets of each of the three different POTS Ports **28-30**. When more than one voice call is in progress, they are handled in a round robin fashion based upon the packet rate for the compression algorithm used. If, for example, two calls are using a compression scheme that generates packets every 2 milliseconds, and the third generates packets every 4 milliseconds, then the calls utilizing the faster packet rate will be polled at twice the rate as the call using a slower packet rate but they are not given priority "over" the other call. Only when there are no voice packets ready for transmission to the Modem/DAA **41**, i.e. during the approximately 2 to 4 millisecond packetization period between packets, will any pending data packets received from the USB Port **12**, Ethernet Port **11** or the 802.11b/g Module **36** be sent to the Modem/DAA **41** for transmission over the network.

Thus, the POTS bandwidth is allocated on a per packet basis, not on a "time slot" or "channelization" or even a "frequency" basis as it the case with T-Carrier, DSL or channelized DSL systems. The same is true for the wireless interface, whether it is carrying pure data or voice.

Security is currently a big concern in today's networks, and especially with wireless 802.11 transmissions. For this reason, the RCG defaults to route voice data over the users POTS connection via Incoming POTS Port **40**. As security concerns regarding wireless communications transmissions are addressed and alleviated, voice call data can, and will, be routed over the wireless interface via the 802.11b/g Module **36**.

FAX Transmission:

Group I, 2 and 3 fax transmission is completely supported by the RCG. Fax transmission has the same priority as other voice communications. That is to say that FAX transmission is treated the same as a voice call and takes precedence over native IP data traffic.

Broadband Over POTS:

One of the primary functions of the RCG is to be able to transfer large files such as video files over the POTS lines to a residence. The ability to do this is limited by the maximum of 56 Kbps due to the design of the digital Class 5 office linecards and network transmission schemes based upon T carriers. Typical Class 5 linecard design samples the POTS lines at a rate of 8,000 samples per second. Typically, each sample is digitized into 12 to 16 bits by a codec device. The digitized sample is then companded to an 8 bit sample (1 byte) which makes up the PCM data stream that is transferred over the PSTN. Therefore, each POTS line is sampled at an effective rate of 64 Kbps. Since legacy T1 transmission equipment uses robbed-bit signaling, the maximum guaranteed transmission rate for the PSTN as a whole is 56 Kbps. Because of this limitation, standard POTS lines can only guarantee a maximum of 56 Kbps transfer rate under the best conditions. DSL equipment gets around this problem by installing DSL Access Multiplexing (DSLAM) equipment at the Class 5 office end of the POTS line. By routing around the linecard, as well as routing the data directly over the Internet or other private IP based networks, and therefore the 64 Kbps sampling rate, DSL is not bandwidth limited like PSTN traffic is. DSL, however, suffers from the very high costs associated with the purchase, installation, maintenance, floor lease costs, etc. DSL also suffers from very high deployment costs resulting from the labor intensive process to turn up each line. Each DSL "POTS" line must be inspected, conditioned and all load coils removed.

The RCG gets around the 56 Kbps POTS limitation as well as the DSL problems by using the standard POTS lines as they are, and not requiring any additional equipment to be installed

at the Class 5 end of the POTS line. This technique simplifies deployment and drastically cuts costs.

Multilink PPP Connections:

Referring to FIG. **7**, the RCG implements broadband over POTS by employing an 802.11b/g wireless interface to configure a multilink PPP bundle—**87** (per RFC 1990) comprised of the POTS lines connected to up to 32 RCGs. The limitation of 32 RCGs in a multilink PPP bundle is an arbitrary number and can be scaled up or down as required to support changes in network equipment capabilities. An 802.11b/g interface—**87** is shown as the preferred embodiment, since its 11/54 Mbps interface is considered sufficient bandwidth at this time also, its transmission distances are sufficient for implementation of this device, as opposed to other shorter ranged wireless transmission schemes. However as time goes on, some other wireless interface may be more desirable. There is nothing special or specific to the 802.11 wireless interface that makes it particularly suited to this application. Any wireless interface scheme can be used to implement this device.

The 802.11b/g interface—**88** on an individual RCG is also used to provide a peer-to-peer wireless home networking environment to other 802.11 compatible wireless component within the residence (such as a hand-held computer device) while acting as an always on dialup Internet gateway over the POTS line—**40** for the other wireless devices. An RCG that is transferring a very large file can request the services of 31 (in this embodiment) other RCGs to assist in the file transfer using their respective POTS lines. A single RCG can therefore gain the combined bandwidth of up to 32 POTS lines transferring data at as much as 56 Kbps each to transfer information. This is roughly equivalent to a transfer rate of 1.79 Mpbs in the inbound direction (towards the RCG) and approximately 1.075 Mbps in the outbound direction (towards the PSTN).

The multilink PPP connection—**87** is initiated by an RCG when it determines that the file (or streaming service) that it is to download (receive) is of sufficient size or requires a minimum amount of bandwidth to justify the use of a multilink PPP connection. This determination can be made on many different criteria such as the file size, type of data being transmitted, the type of compression if any, a Quality-of-Service requirement or any other pertinent information. (Since a certain amount of overhead is required to set up a Multilink PPP connection, it doesn't make sense to use it for small or low data rate transfers.)

Multilink PPP Bandwidth Allocation and Initialization:

Referring to FIG. **7**, an RCG—**85** that decides to initiate a multilink PPP session with a remote computer i.e. internet URL, requests a multilink PPP session with that URL resource via Link Control Protocol (LCP) session management. The initiating RCG—**85** and the remote server computer (not shown) will negotiate the pertinent multilink parameters such as compression, packet size, sync/async, link quality monitoring, bit stuffing etc. As part of a successful multilink PPP session setup, the initiating RCG—**85** receives a multilink PPP session ID, or "magic number", which is used to identify this particular multilink PPP session and is also used for adding or removing links from the multilink bundle—**87**. Once the multilink bundle is setup, the initiating RCG—**85** begins data transfer across its POTS interface-**90** with the far end computer system. The initiating RCG—**85** then looks up the addresses of up to 31 (in this embodiment) other RCGs in its router tables to use for the multilink PPP transfer. (If a Neighborhood Access Point is available the RCG could request service through it instead of setting up a Multilink PPP connection—see FIG. **8**.) The initiating RCG—**85** determines the number of remote RCGs—**86** that it wants to use to get the desired bandwidth for the transfer and sends multilink PPP service requests via the 802.11b/g wireless connections—**88** to the selected remote RCGs—**86**. The selected remote RCGs—**86** respond back to the initiating RCG with either an acceptance or denial of multilink PPP service request. This decision is made based upon the remote RCG's currently available POTS bandwidth and the current local demands for that bandwidth. The remote RCG—**86** makes a decision to participate in a multilink PPP service for an initiating RCG if its POTS line—**91** has a current average bandwidth utilization of less than some arbitrary limit such as 8 Kbps to 16 Kbps. This 8 Kbps to 16 Kbps bandwidth utilization represents about two concurrent voice conversations using standard voice compression techniques, or some small amount of data transmission occurring on the remote RCG's POTS interface—**91** or a combination thereof. Assuming that the remote RCG—**86** has a modem connection speed somewhere between 33 Kbps to 56 Kbps, this would leave approximately 17 Kbps to 40 Kbps of POTS bandwidth that the remote RCG—**86** could offer to the initiating RCG—**85** for use in its multilink PPP bundle—**87**. Of course, if there is no activity on the remote RCG—**86** POTS line, then the entire bandwidth will be used for the multilink transfer. If the remote RCG—**86** accepts the multilink PPP service request from the initiating RCG—**85** it also sends its currently available bandwidth on its POTS line—**91** that the initiating RCG—**85** will have available to it for the multilink PPP transfers. The initiating RCG then selects which of the responding remote RCGs—**86** it will use for the multilink PPP bundle—**87** and sends them a multilink initialization packet containing the URL of the destination as well as the multilink PPP session ID (magic number) and any other pertinent information required for the remote RCG to join in the existing multilink PPP bundle—**87**. Each remote RCG POTS interface—**91** participating in a multilink PPP bundle, represents a logical "link" in the initiating RCG's multilink PPP bundle—**87**. The remote RCGs—**86** then send a multilink PPP packet (over their respective POTS lines—**91**) to the destination URL with the multilink PPP session ID and request to be added to that multilink PPP bundle—**87**. The destination URL accepts the request of each of the remote RCGs—**86** and begins sending data packets to each over their respective POTS lines—**91**. When the remote RCGs—**86** receive data packets sent over their respective POTS lines—**91**, that are destined for the multilink PPP bundle—**87**, they simply relay the data packets over their 802.11b/g interface—**88** to the initiating RCG—**85**. It is the responsibility of the initiating RCG—**85** to perform all housekeeping tasks associated with the multilink transfer such as detection of lost packets and data packet reassembly, if those functions are required. Typically, lost packet detection and retransmission and reassembly are performed at higher OSI layers by the requesting software such as a browser. The remote RCGs—**86** are simply data transport nodes and do not perform any data processing on data received over a multilink PPP bundle destined for another RCG.

The initiating RCG—**85** of the multilink PPP bundle—**87** continually monitors the bandwidth of each remote RCG's—**86** multilink link which together comprise its multilink bundle—**87**. When the available bandwidth for the multilink PPP link of an individual remote RCG—**86** falls below an arbitrary minimum set by the initiating RCG—**85**, the initiating RCG—**85** instructs the offending remote RCG, via its 802.11b/g wireless interface—**88**, to remove itself from the multilink bundle. The remote RCG—**86** will then notify the remote computer (URL) to be removed as a link in the current

multilink bundle on which it is participating. Alternatively, a remote RCG—**86** can inform the initiating RCG—**85** of local demands on its POTS bandwidth, and request that the initiating RCG—**85** remove it (the remote RCG—**86**) from the participation in the initiating RCG's multilink bundle—**87**. The remote RCG—**86** will not unilaterally remove itself from participation in a multilink bundle without prior notification to the Initiating RCG—**85**. The remote RCG—**86** must get authorization from the initiating RCG—**85** to remove itself from the bundle, since the initiating RCG—**85** will have no way of knowing if the loss of data from that remote RCG is due to some sort of failure or from the remote RCG simply removing itself from participation in the multilink bundle—**87**. Also, for services that require a minimum Quality of Service (QOS) such as streaming video, the initiating RCG—**85** needs to control the multilink bundle—**87** bandwidth, and it can not do that if remote RCGs—**86** drop out of the multilink bundle—**87** at will. When a remote RCG—**86** requests to be removed from participation in a multilink bundle—**87**, the initiating RCG—**85** must immediately grant the request. If the initiating RCG—**85** were to not grant the request, then the remote RCG—**86** could, in worst case, delay or drop incoming multilink packets destined for the initiating RCG—**85**. If this were to happen, the initiating RCG—**85** will have missing packets and could over run its reassembly buffer (if reassembly is being performed by the RCG) causing catastrophic data loss and potentially have to restart the entire transmission. In the least case, the initiating RCG—**85** would have to initiate retransmission of potentially many packets which it assumes to be lost, but may simply be delayed by the remote RCG—**86**. Once a remote RCG—**86** has been removed from participating in a multilink bundle—**87**, the initiating RCG—**85** will then look up another remote RCG in its router tables that can be used to participate in the multilink PPP bundle—**87**, and request that the new remote RCG—**86** to join the existing multilink bundle—**87**. This is necessary to maintain a minimum Quality of Service. Since RCGs prioritize their bandwidth requirements based upon their own "local" service requirements, their participation in any multilink PPP service is available only to bandwidth that is not required for its own current local demands. Therefore, a remote RCG's—**86** bandwidth that is available for multilink services can change at any time. The dynamic reassignment of remote RCGs that participate in a multilink bundle is also required to prevent a remote RCG—**86** from receiving packets so slowly that the originating RCG—**85** interprets this delay as lost packets. When the initiating RCG—**85** determines that a packet has been lost, and it is performing packet reassembly, it will, itself, request that the remote computer retransmit the lost packet. The initiating RCG will not ask any remote RCG—**86** to perform retransmissions or any other kind of data computations or manipulations.

Refer to FIG. **8** for the following discussion. In areas where there are existing 802.11 network equipment such as Neighborhood Access Point—**93**, or where there is sufficient bandwidth requirements from an installed base of RCGs to warrant the deployment of a Neighborhood Access Point—**93**, the RCGs will automatically detect the presence of the compatible neighborhood access points and register with that equipment for transport services. In this case, an RCG has an alternative broadband service route in addition to the multilink option. An RCG can communicate directly with a local 802.11 Network Access Point—**93** that is connected to the PSTN or another carrier's network via some sort of high bandwidth backbone such as a T-Carrier or optical carrier connection (T1, T3, OC3, OC12 etc.). The RCGs can communicate directly with neighborhood access points at their full 11/54 Mbps data rates to provide up to that full bandwidth to the user. This functionality is, of course, subject to the Network Access Point—**93** allowing access to its resources to the RCG according to the 802.11 wireless protocol.

This architecture is important since it provides an avenue to relieve the local class 5 offices of congestion that can be caused by a wide spread deployment of RCGs within the class 5 service area. Since each RCG requires a constant 24/7 modem connection, this ties up the class 5 switch in a fashion that it was not designed for. This could lead to wholesale class 5 office expansions which would be extremely expensive, and potentially prohibitive for the Local Exchange Carriers (LECs). By deploying neighborhood access points that operate at 54 Mbps (802.11a/g), in areas where the RCG concentration starts placing too high of a demand on the local class 5 office, the bandwidth from the RCGs can be aggregated by the neighborhood access points into large capacity backbones to relieve the switch congestion. In this case, the RCG POTS interface—**40** can be used solely as a lifeline connection, or when the 802.11 wireless LAN in which the RCG resides is congested. With this implementation, voice calls will be carried over the wireless interface as opposed to the POTS interface on which they would normally be carried. Also, the RCG modem—**41** connected to the POTS interface—**40** would not need to maintain a constant always on connection, it could be a dialed on demand connection and thereby relieving the local class 5 office switch.

Bouncing or Hopping Traffic:

Refer to FIG. **9**. In areas where the density of RCGs is less than the arbitrary number of 32 RCGs within its transmission radius for multilink connections, the RCGs can bounce, or relay, the data traffic between each other to reach other RCGs located farther than the RCGs wireless transmission area. Since the POTS data rate of 56 Kbps is miniscule as compared to the 11/54 Mbps 802.11b/g transfer rate, the overhead associated with bouncing data traffic is not a concern. This will allow for the fastest possible data transfer across POTS lines for every RCG user.

RCGs can also communicate directly with an 802.11a Neighborhood Access Point—**93** device (such as that used in WI-FI networks) that is connected to a data network connection such as a DS3 or OC3 service via a Metro Access Point. Where an RCG has access to a broadband device such as an 802.11a type device, either directly or via a bounced signal across several RCGs, a direct high speed data connection can be used to transfer large files. When an RCG is communicating directly with an 802.11a device, data transfer speeds up to the full 11/54 Mbps can be achieved to speed video transfers for such applications as video on demand.

RCG Router Tables:

The RCG continually monitors its 802.11b/g wireless interface for transmissions from other RCGs or 802.11a Access Points as well as other 802.11b/g wireless devices within the residence. The RCG provides a means to identify and store the addresses of other RCGs and Neighborhood Access Points within its local area. The RCG creates routing tables, much like an IP router device, so that it knows which RCGs are local to itself, and how many hops will be needed to reach the maximum of 32 POTS lines or a Neighborhood Access Point. The RCG can then determine how to route its data transfers to gain the most efficient routing and network efficiencies.

The router tables in each RCG are continually updated by monitoring the 802.11 frames received from other RCGs or Network Access Points. The number of entries in the router tables can be limited to an arbitrary number of other RCGs but contains room for at least 32 entries. For each RCG listed in

the router tables, certain information is kept such as signal strength, if the other device is another RCG or some other 802.11 compatible device, if the other RCG is reachable directly, or if it is accessed via another RCGs by hopping. In the case there RCG hopping is used, the address of each RCG that is hopped is stored in the routing table. When an RCG is first powered up, it monitors its 802.11 interface for a period of time to identify other RCGs or Neighborhood Access Point devices, or other Wi-Fi devices within its transmission area. When first deployed, the RCG will not have any entries in its routing tables. This condition can persist for some time, until another RCG or other 802.11 device is deployed within the former RCGs transmission range. In this state, the RCG can be used for wireless networking within the residence, connecting the local computer to the RCGs always on Internet connection as well as to other wireless devices within the home. When an 802.11 frame is received by an RCG that contains the address of an RCG whose address does not exist in the receiving RCG's router table (as is the case when a new RCG is first installed), the receiving RCG polls the transmitting RCG for its router table information. The received router information is reviewed for other RCG's or other 802.11 compatible devices that are not listed in its own router tables. A decision is made to use some, all, or none of the new route information in its router tables. There is no real limitation on the number of RCGs that can be "hopped" in order to build a complete router table or to reach many more RCGs, Neighborhood Access Points or Metro Access Points.

Equipment and Services Priorities:

Just as voice has priority over data transfers within a single RCG, local RCG traffic (both voice and data) has priority over remote transfer requests by other RCGs. If an RCG is currently using all of its available POTS bandwidth for its own purposes, it will deny any remote RCG's request for access to its POTS line. Only when there is available POTS bandwidth available will an RCG allow other RCGs access to its POTS line. It will, however, bounce the traffic to other RCGs within its transmission area if requested by the originating RCG. In this case, available wireless bandwidth of any RCG (that amount of the 11/54 Mbps not currently used for its own traffic) can be used to relay traffic between other RCGs that do have available POTS bandwidth. In the same fashion, excess wireless bandwidth of any RCG can be by other RCGs to access high speed backbones via Neighborhood or Metro Access Points. RCGs can also access other 802.11 wireless networks (Wi-Fi for example) that happen to be deployed within their service areas. In this case, access agreements between the RCG service provider and the wireless network operator must be put into place. By remaining compatible with the 802.11 standards, the RCGs capabilities will benefit by the growing WI-FI network infrastructure, an the WI-FI network will benefit by the RCG network.

Voice Over POTS and Data Over Wireless:

Normally, all communications from an RCG will be transmitted over the local POTS line, or a multilink bundle made up of many remote RCG POTS lines. By default, all voice calls will be carried over the "local" POTS line—**40** to alleviate security/privacy concerns and only "data" will be transmitted via multilink bundles. Generally, since voice "data" is compressed locally by the RCG, the required bandwidth for a voice call is so small that it does not make for a good choice to route it over a multilink connection. However, it is possible to route voice calls entirely over another RCGs POTS line. It is also possible for an RCG to transmit voice data over POTS lines connected to other RCGs via multilink bundles or directly over its 802.11 wireless interface, and since the 802.11 specification does support the Wired Equivalent Privacy (WEP) specification, a secured connection can be made in this fashion.

Remote Upgradability

The RCG is designed with the capability for unassisted remote upgradability. The remote upgradability feature is not the same as the storing of operational parameters during the configuration process. This feature allows the system operator to add new features as they are developed, or to correct bugs remotely and without the users knowledge or involvement. This feature can also be used to install a complete new operating system (OS).

Key to the successful implementation of the Remote upgradability feature is that a completely fail-safe routine be implemented that can recover from any failure during the upgrade process and to re-initiate and monitor the upgrade process until it has successfully completed. This process is carried out by loading a boot loader program that is stored in non-volatile memory. The boot loader program provides the minimum capabilities to start up the RCG and connect into the system operator's diagnostics network to download fixes or a new OS. The boot loader program is technically part of the OS, but it cannot be over written by any upgrade process. It is responsible for detecting failure of the RCG and initiating a connection to the diagnostics network. Once connected with the diagnostics network, the boot loader will provide diagnostics support to help correct the RCG's operation and reconfigure the OS.

What is claimed is:

1. A communications device that is capable of providing broadband communications services, comprising:

at least one connection for connecting to a communications network;

at least one wireless interface for connecting wirelessly to at least one remote communications device; and

a processor that requests the at least one remote communications device to assist in transferring data, sends a request to the at least one remote communications device for requesting use of a portion of unused bandwidth of the at least one remote communications device, receives a response from the at least one remote communications device, the response containing information about the portion of unused bandwidth, selects the at least one remote communications device with unused bandwidth, sends control information to the at least one remote communications device for participating in a multilink connection, receives packets from the at least one remote communications device and aggregates the data from the at least one remote communications device with data transfers from the at least one connection to increase data bandwidth for the communications device.

2. The communications device of claim **1**, wherein the processor combines the data bandwidth of the at least one connection with the at least one remote communications device.

3. The communications device of claim **1**, wherein the at least one remote communications device is at least one of a residential communications gateway, a cable modem, a digital subscriber line, a wireless device, a neighborhood access point device, a Wi-Fi device and a cellular phone.

4. The communications device of claim **1**, wherein the processor allocates the at least one remote communications device into a multilink group transfer.

5. The communications device of claim **1**, wherein the processor creates and updates routing tables with the at least one remote communications device.

6. The communications device of claim **5**, wherein the processor uses the routing tables to determine routing efficiencies based on at least one of quality of service, total connection speed of the at least one remote communication device, a number of data hops, available unused bandwidth of the at least one remote communication device, wireless transfer speeds and signal strength between the at least one remote communication device and the communication device.

7. The communications device of claim **1**, wherein the processor determines how many remote communications devices are located in a transmission range.

8. The communications device of claim **1**, wherein the communications network is at least one of a public wired network, a private wired network, a public wireless network, and a private wireless network.

9. The communications device of claim **1**, wherein the communications network is at least one of a public switched telephone network, a cable network, a wireless network and a fiber network.

10. A communications device that is capable of providing broadband communications services, comprising:

at least one connection for connecting to a network;

at least one wireless interface for connecting wirelessly to remote communications devices; and

a processor that requests the remote communications devices to transfer portions of data, sends a request to the remote communications devices for requesting use of a portion of unused bandwidth of each of the remote communications devices, receives a response from each of the remote communications devices, the response containing information about the portion of unused bandwidth for each of the remote communications devices, selects a group of the remote communications devices with a larger, combined, unused bandwidth, sends control information to the selected remote communications devices for participating in a multilink transfer, and receiving packets from the selected remote communications devices and combines and sequences the portions of the data from the remote communications devices with second data transferred from the at least one connection to increase data bandwidth for the communications device.

11. The communications device of claim **10**, wherein the processor creates and updates routing tables for each of the remote communications devices.

12. The communications device of claim **10**, wherein the processor uses the routing tables to determine routing efficiencies based on quality of service and selects a group of the remote communications devices for optimizing the routing efficiencies.

13. The communications device of claim **10**, wherein the processor uses the routing tables to determine routing efficiencies based on at least one of quality of service, total connection speed of the remote communication devices, a number of data hops, available unused bandwidth of the remote communication devices, wireless transfer speeds and signal strength between the remote communication devices and the communication device.

14. The communications device of claim **10**, wherein the processor receives information whether each of the remote communications devices wants to participate in a multilink group transfer, and configures a multilink group for all the participating remote communications devices to optimize routing efficiency.

15. A communications device that is capable of providing broadband communications services, comprising:

at least one connection for connecting to a communications network;

at least one wireless interface for connecting wirelessly to at least one cellular phone; and

a processor that requests the at least one cellular phone to assist in transferring data, sends a request to the at least one cellular phone for requesting use of a portion of unused bandwidth of the at least one cellular phone, receives a response from the at least one cellular phone, the response containing information about the portion of unused bandwidth, selects the at least one cellular phone with unused bandwidth, sends control information to the at least one cellular phone for participating in a multilink connection, receiving packets from the at least one cellular phone and aggregates the data from the at least one cellular phone with data transfers from the at least one connection to increase data bandwidth for the communications device.

16. The communications device of claim **15**, wherein the processor creates and updates routing tables with the at least one cellular phone.

17. The communications device of claim **15**, wherein the processor uses the routing tables to determine routing efficiencies based on at least one of quality of service, total connection speed of the at least one cellular phone, a number of data hops, available unused bandwidth of the at least one cellular phone, wireless transfer speeds and signal strength between the at least one cellular phone and the communication device.

* * * * *

EXHIBIT B

US009350649B2

(12) **United States Patent**
Delangis

(10) **Patent No.: US 9,350,649 B2**
(45) **Date of Patent: May 24, 2016**

(54) **MULTIPATH COMMUNICATION DEVICES AND METHODS**

(71) Applicant: **Eric M. Delangis**, Huntsville, AL (US)

(72) Inventor: **Eric M. Delangis**, Huntsville, AL (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.

(21) Appl. No.: **14/512,414**

(22) Filed: **Oct. 11, 2014**

(65) **Prior Publication Data**

US 2015/0032860 A1 Jan. 29, 2015

Related U.S. Application Data

(63) Continuation of application No. 13/531,294, filed on Jun. 22, 2012, now Pat. No. 8,861,349, which is a continuation of application No. 12/581,852, filed on Oct. 19, 2009, now Pat. No. 8,228,801, which is a continuation of application No. 10/686,375, filed on Oct. 14, 2003, now Pat. No. 7,606,156.

(60) Provisional application No. 60/418,521, filed on Oct. 15, 2002.

(51) **Int. Cl.**

H04L 12/54	(2013.01)
H04W 88/16	(2009.01)
H04W 28/06	(2009.01)
H04L 12/707	(2013.01)
H04W 8/26	(2009.01)
H04W 40/02	(2009.01)
H04W 72/04	(2009.01)
H04W 80/00	(2009.01)
H04W 84/12	(2009.01)
H04W 84/18	(2009.01)

(52) **U.S. Cl.**

CPC ***H04L 45/24*** (2013.01); ***H04L 12/5692*** (2013.01); ***H04W 88/16*** (2013.01); *H04W 8/26* (2013.01); *H04W 28/06* (2013.01); *H04W 40/02* (2013.01); *H04W 72/04* (2013.01); *H04W 80/00* (2013.01); *H04W 84/12* (2013.01); *H04W 84/18* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,483,522 A * 1/1996 Derby et al. 370/400
5,487,069 A 1/1996 O'Sullivan et al.

(Continued)

OTHER PUBLICATIONS

Fisk et al., "Dynamic Right-Sizing in TCP, Proceedings of the Los Alamos Computer Science Institute Symposium", pp. 01-5460 (2001).

(Continued)

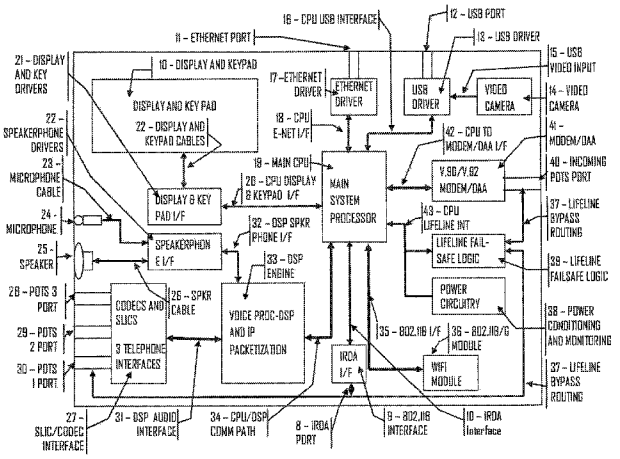
Primary Examiner — Hong Cho

(74) *Attorney, Agent, or Firm* — Clay McGurk; The Law Office of Clay McGurk

(57) **ABSTRACT**

The Residential Communications Gateway (RCG) is a broadband communications device that combines all voice, data and video communications to and from a typical residence or small business for transmission over a single, or a plurality of Plain Old Telephone Service (POTS) lines separately or in conjunction with, a wireless broadband backbone. The RCG does this by employing packetized data with Voice over Internet Protocol (VoIP) technologies combined with RF communications technologies. A key consideration to the design of the RCG is that no additional or special transmission equipment must be installed at the Central Office or anywhere else in the network to enable new calling features provided by the RCG as is the case with DSL and Cable systems. By eliminating the requirement for costly infrastructure enhancements, ubiquitous high speed communications and services can be deployed to every POTS subscriber.

23 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,249,669	B1 *	6/2001	Ogino et al.	455/63.1
6,496,477	B1 *	12/2002	Perkins et al.	370/228
7,068,623	B1 *	6/2006	Barany et al.	370/329
7,224,964	B2	5/2007	Souissi et al.	
7,257,106	B2 *	8/2007	Chen et al.	370/338
7,917,129	B2	3/2011	Souisse et al.	
8,370,507	B1 *	2/2013	Cain	H04N 21/25816 709/225
8,442,504	B2	5/2013	Souissi et al.	
8,521,142	B2	8/2013	Souissi et al.	
2001/0037472	A1 *	11/2001	Li	H04L 12/66 714/4.1
2002/0150099	A1 *	10/2002	Pung et al.	370/390
2003/0137959	A1 *	7/2003	Nebiker et al.	370/338

OTHER PUBLICATIONS

Hsieh et al., "pTCP: An End-to-End Transport Layer Protocol for Striped Connections", ICNP, pp. 24-33 IEEE Computer Society (2002).

"End-to-End Approach to Host Mobility", by Alex C. Snoeren and Had Balakrishnan, MIT Laboratory for Computer Science, MobiCom (2000).

"Multi-homed TCP", by Huitema, C. (Internet Draft) IETF, (1995).

"TCP extensions for high performance", by Jacobson V., Braden R., and Borman D., RFC 1323, IETF, (1992).

"A New Multicasting-based Architecture for Internet Host Mobility", by Mysore, J., and Bharghavan, V., Proc. ACM/IEEE Mobicom '97 (1997).

"Mobile IPv4 Challenge/Response Extensions", by Perkins, C., and Calhoun, P., RFC 3012, IETF, (2000).

"Mobility Support in IPv6", by Perkins, C., and Johnson, D, Proc. ACM/IEEE Mobicom '96 (1996).

"Route Optimization in Mobile IP", by Perkins C., and Johnson, D., Cluster Computing 1, (1998).

"IP Mobility Support", by Perkins, C., RFC 2002, IETF, (1996).

"Transmission Control Protocol", RFC 793, IETF (1981).

"Multiple Paths Protocol for a Cluster Type Network", Hiroshi Mineno et al., 7 pages (1999).

"The PPP Multilink Protocol (MP)", RFC 1990, 24 pages (1996).

* cited by examiner

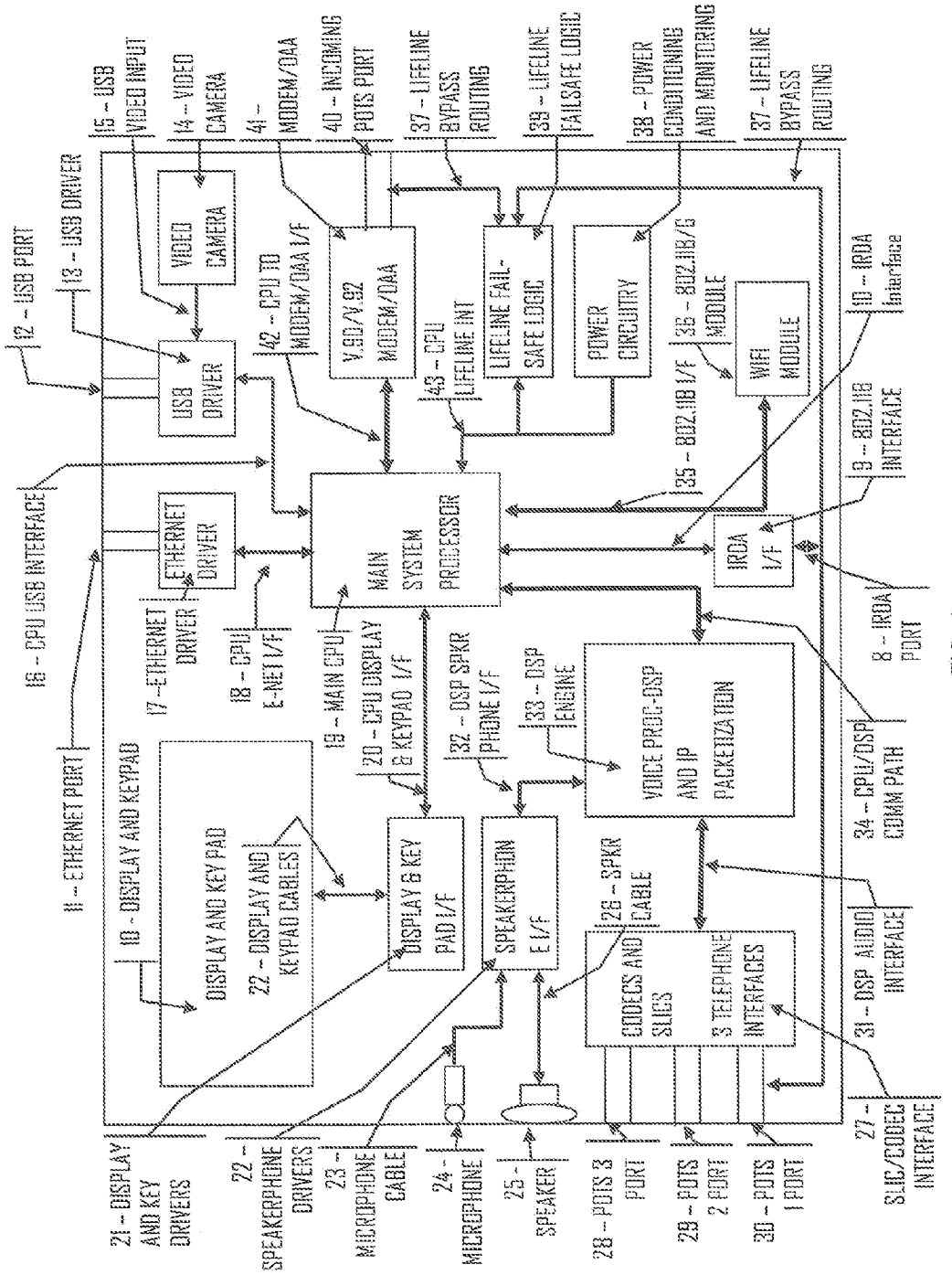

15 – USB VIDEO INPUT
14 – VIDEO CAMERA
41 – MODEM/DAA
40 – INCOMING POTS PORT
37 – LIFELINE BYPASS ROUTING
39 – LIFELINE FAILSAFE LOGIC
38 – POWER CONDITIONING AND MONITORING
37 – LIFELINE BYPASS ROUTING
12 – USB PORT
13 – USB DRIVER
VIDEO CAMERA
42 – CPU TO MODEM/DAA I/F
V.90/V.92 MODEM/DAA
43 – CPU LIFELINE INT
LIFELINE FAIL-SAFE LOGIC
POWER CIRCUITRY
36 – 802.11B/G MODULE
WIFI MODULE
10 – IRDA Interface
USB DRIVER
35 – 802.11B I/F
9 – 802.11B INTERFACE
16 – CPU USB INTERFACE
ETHERNET DRIVER
MAIN SYSTEM PROCESSOR
IRDA I/F
17 – ETHERNET DRIVER
18 – CPU E-NET I/F
19 – MAIN CPU
20 – CPU DISPLAY & KEYPAD I/F
32 – DSP SPKR PHONE I/F
33 – DSP ENGINE
VOICE PROC-DSP AND IP PACKETIZATION
8 – IRDA PORT
11 – ETHERNET PORT
10 – DISPLAY AND KEYPAD
DISPLAY AND KEY PAD
22 – DISPLAY AND KEYPAD CABLES
DISPLAY & KEY PAD I/F
SPEAKERPHONE E I/F
26 – SPKR CABLE
34 – CPU/DSP COMM PATH
CODECS AND SLICS
3 TELEPHONE INTERFACES
31 – DSP AUDIO INTERFACE
21 – DISPLAY AND KEY DRIVERS
22 – SPEAKERPHONE DRIVERS
23 – MICROPHONE CABLE
24 – MICROPHONE
25 – SPEAKER
28 – POTS 3 PORT
29 – POTS 2 PORT
30 – POTS 1 PORT
27 – SLIC/CODEC INTERFACE

FIG. 1

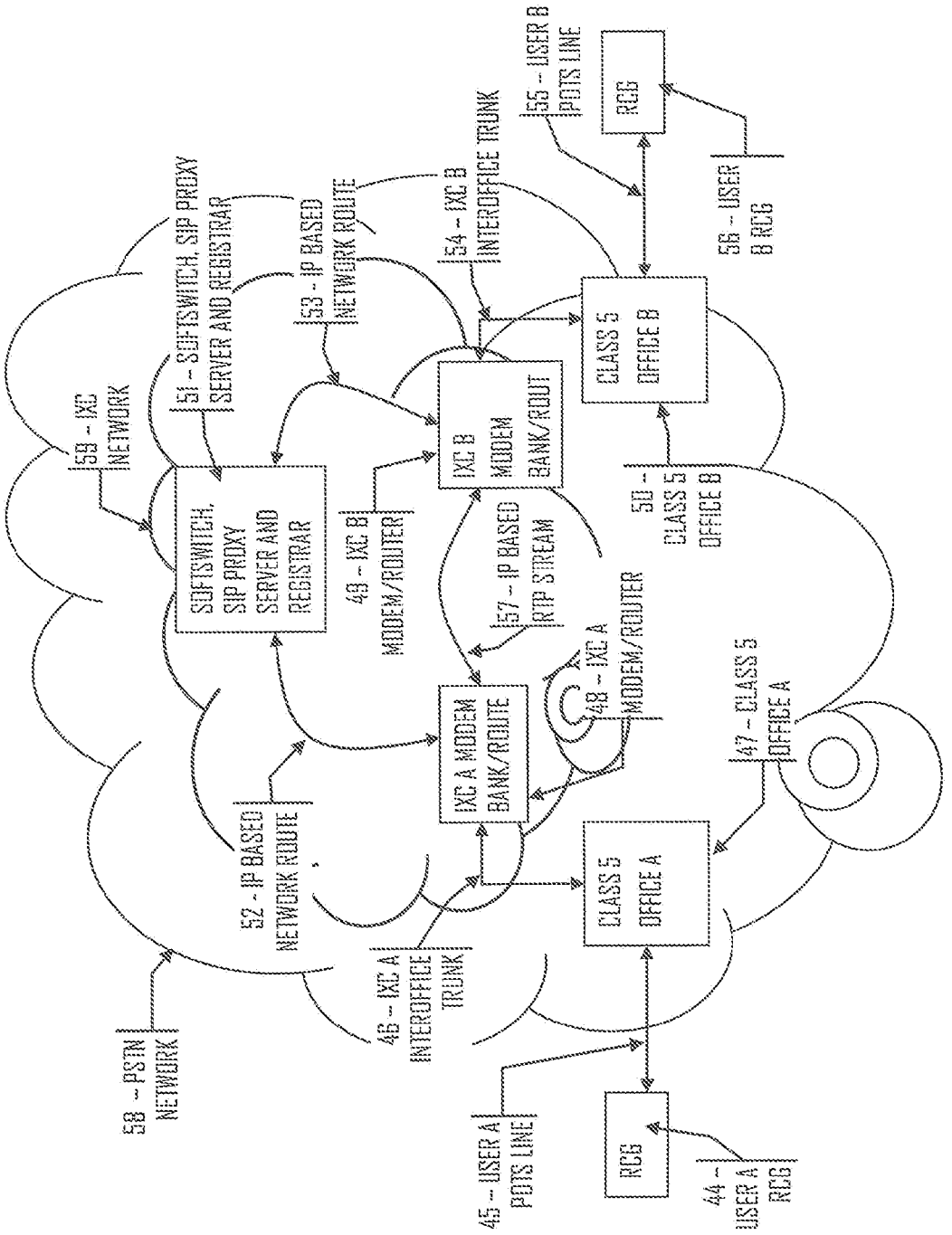

59 - IXC NETWORK
51 - SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
53 - IP BASED NETWORK ROUTE
54 - IXC B INTEROFFICE TRUNK
55 - USER B POTS LINE
RCB
56 - USER B RCB
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
49 - IXC B MODEM/ROUTER
IXC B MODEM BANK/ROUT
CLASS 5 OFFICE B
50 - CLASS 5 OFFICE B
57 - IP BASED RTP STREAM
48 - IXC A MODEM/ROUTER
IXC A MODEM BANK/ROUTE
47 - CLASS 5 OFFICE A
52 - IP BASED NETWORK ROUTE
CLASS 5 OFFICE A
46 - IXC A INTEROFFICE TRUNK
58 - PSTN NETWORK
45 - USER A POTS LINE
RCB
44 - USER A RCB

FIG. 2

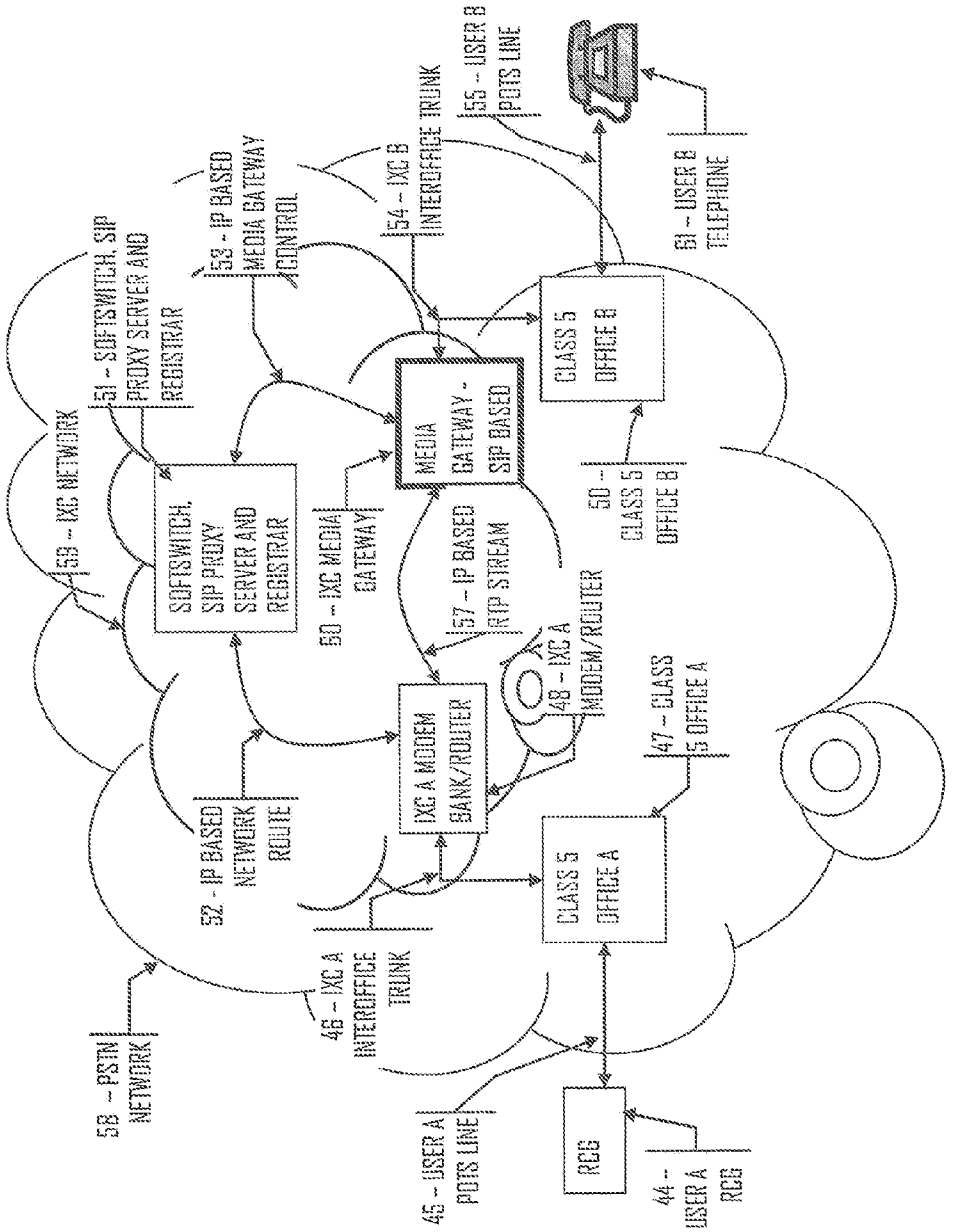

58 – PSTN NETWORK
59 – IXC NETWORK
51 – SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
52 – IP BASED NETWORK ROUTE
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
46 – IXC A INTEROFFICE TRUNK
IXC A MODEM BANK/ROUTER
53 – IP BASED MEDIA GATEWAY CONTROL
60 – IXC MEDIA GATEWAY
MEDIA GATEWAY - SIP BASED
57 – IP BASED RTP STREAM
54 – IXC B INTEROFFICE TRUNK
48 – IXC A MODEM/ROUTER
45 – USER A POTS LINE
RCB
44 – USER A RCB
CLASS 5 OFFICE A
47 – CLASS 5 OFFICE A
CLASS 5 OFFICE B
50 – CLASS 5 OFFICE B
55 – USER B POTS LINE
61 – USER B TELEPHONE

FIG. 3

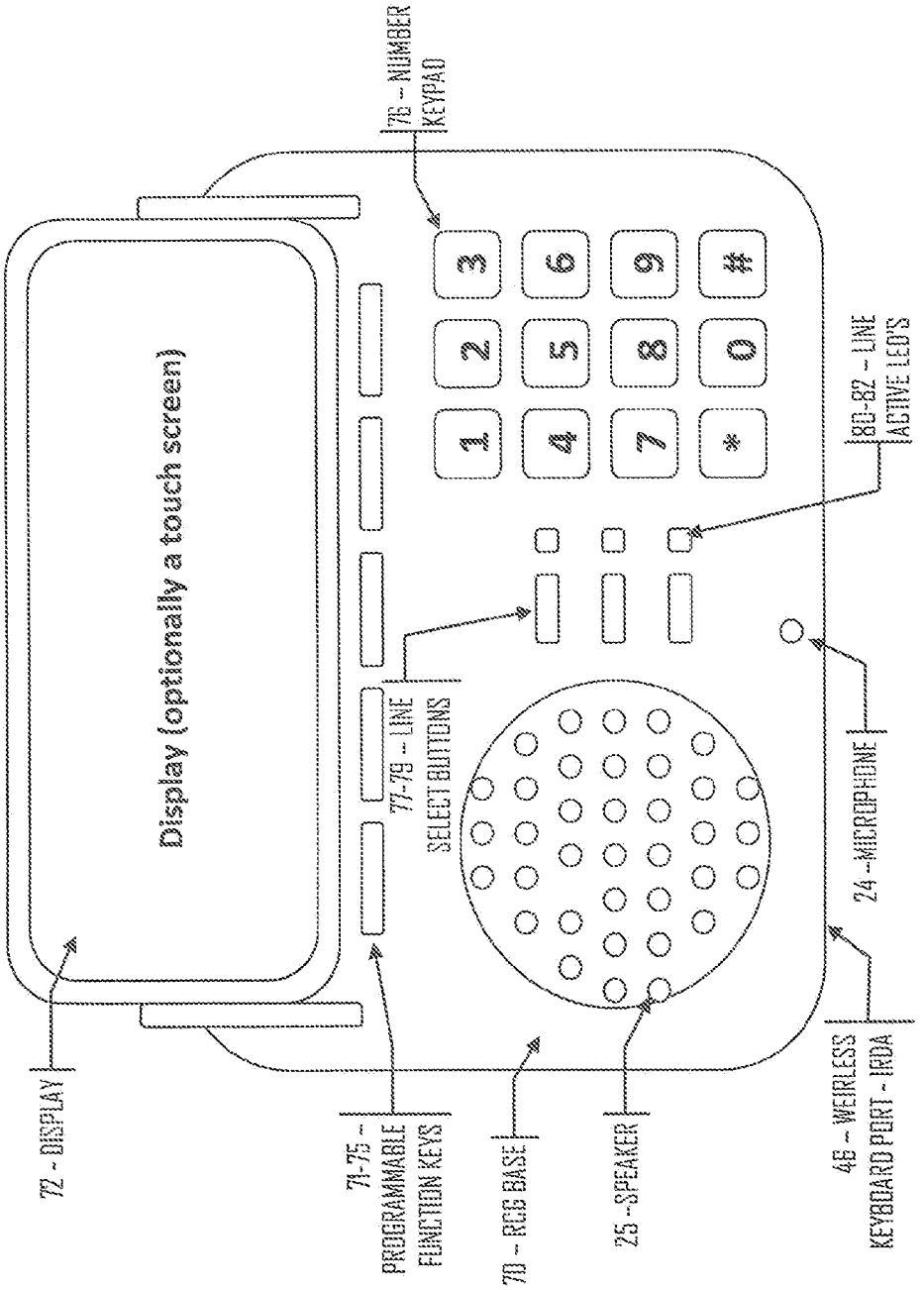

Display (optionally a touch screen)
1
2
3
4
5
6
7
8
9
*
0
#
76 – NUMBER KEYPAD
80-82 – LINE ACTIVE LED'S
77-79 – LINE SELECT BUTTONS
24 – MICROPHONE
72 – DISPLAY
71-75 – PROGRAMMABLE FUNCTION KEYS
70 – RCB BASE
26 – SPEAKER
46 – WEIRLESS KEYBOARD PORT – IRDA

FIG. 4

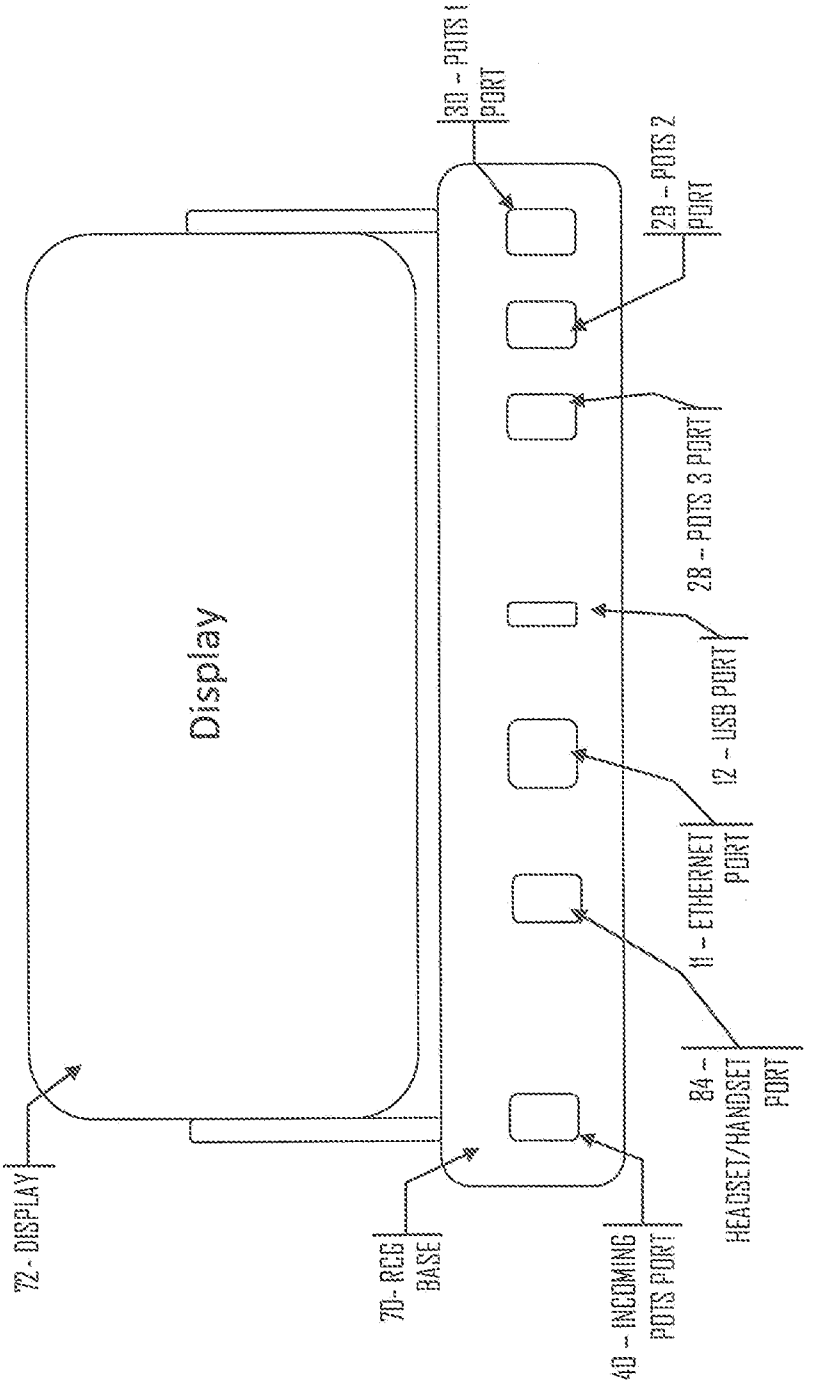

Display
72- DISPLAY
70- REG BASE
40 - INCOMING POTS PORT
84 - HEADSET/HANDSET PORT
11 - ETHERNET PORT
12 - USB PORT
28 - POTS 3 PORT
28 - POTS 2 PORT
30 - POTS 1 PORT

FIG. 5

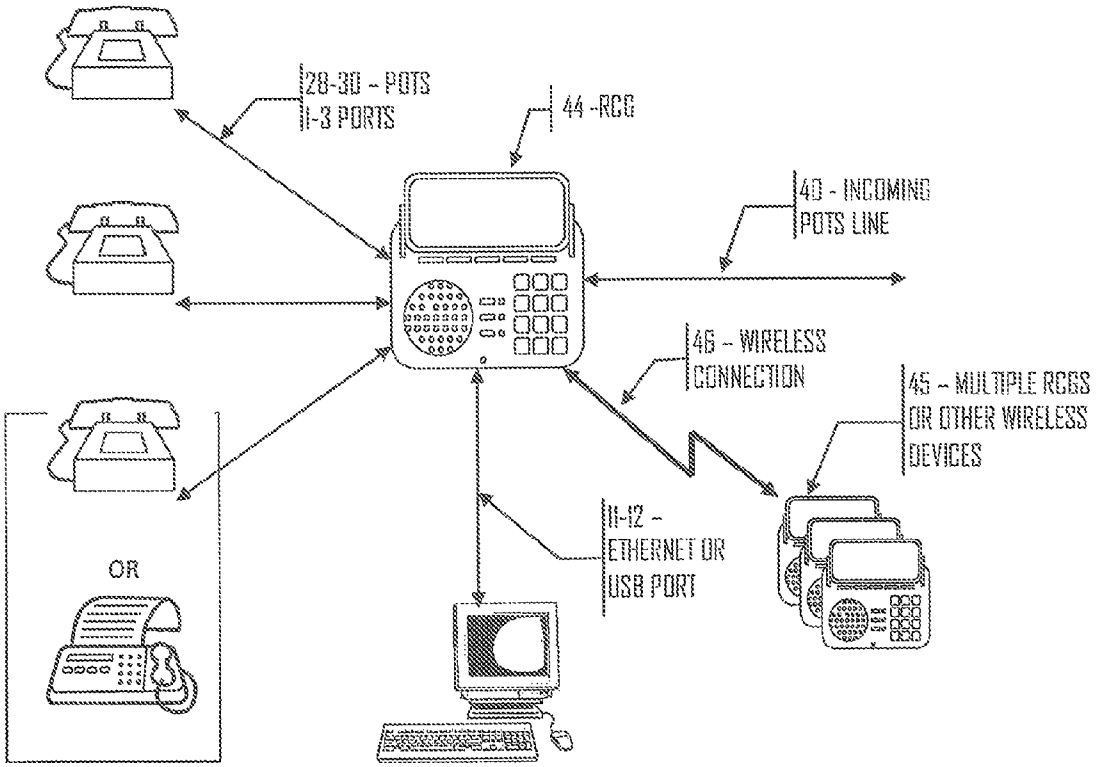

28-30 - POTS
1-3 PORTS
44 -RCG
40 - INCOMING
POTS LINE
46 - WIRELESS
CONNECTION
45 - MULTIPLE RCGS
OR OTHER WIRELESS
DEVICES
11-12 -
ETHERNET OR
USB PORT
OR

FIG. 6

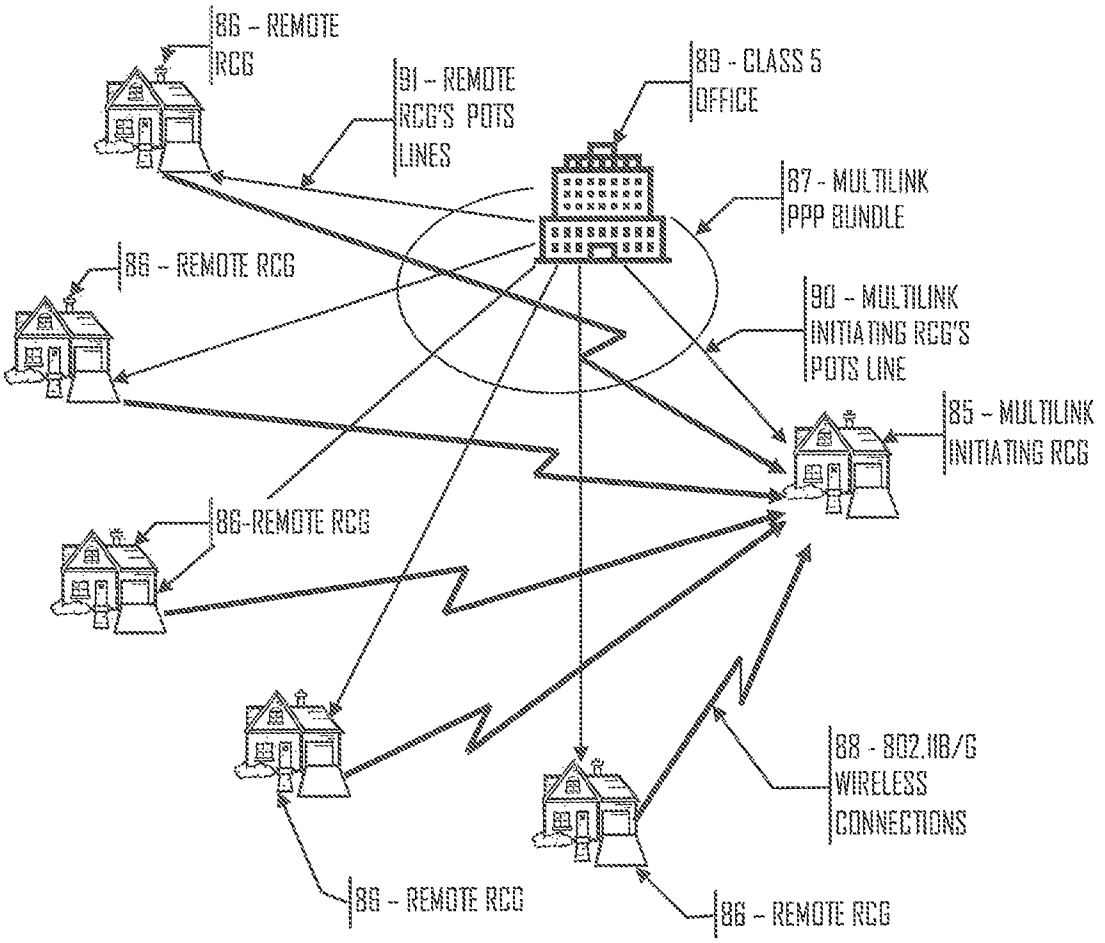

86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
85 – MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG

FIG. 7

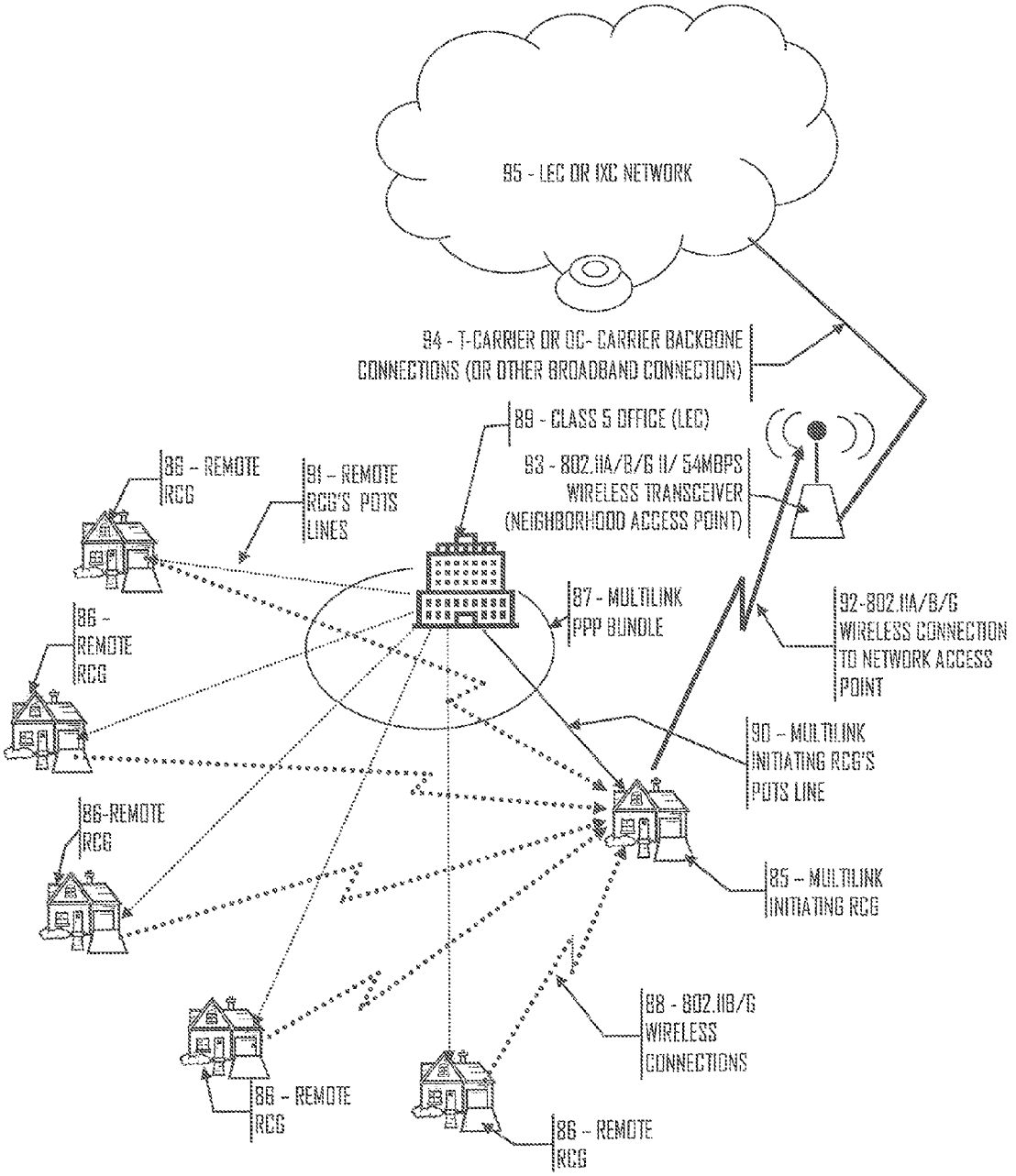

95 - LEC OR IXC NETWORK
94 - T-CARRIER OR OC- CARRIER BACKBONE CONNECTIONS (OR OTHER BROADBAND CONNECTION)
89 - CLASS 5 OFFICE (LEC)
93 - 802.11A/B/G II/ 54MBPS WIRELESS TRANSCEIVER (NEIGHBORHOOD ACCESS POINT)
86 - REMOTE RCG
91 - REMOTE RCG'S POTS LINES
87 - MULTILINK PPP BUNDLE
92-802.11A/B/G WIRELESS CONNECTION TO NETWORK ACCESS POINT
86 - REMOTE RCG
90 - MULTILINK INITIATING RCG'S POTS LINE
86-REMOTE RCG
85 - MULTILINK INITIATING RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 - REMOTE RCG
86 - REMOTE RCG

FIG. 8

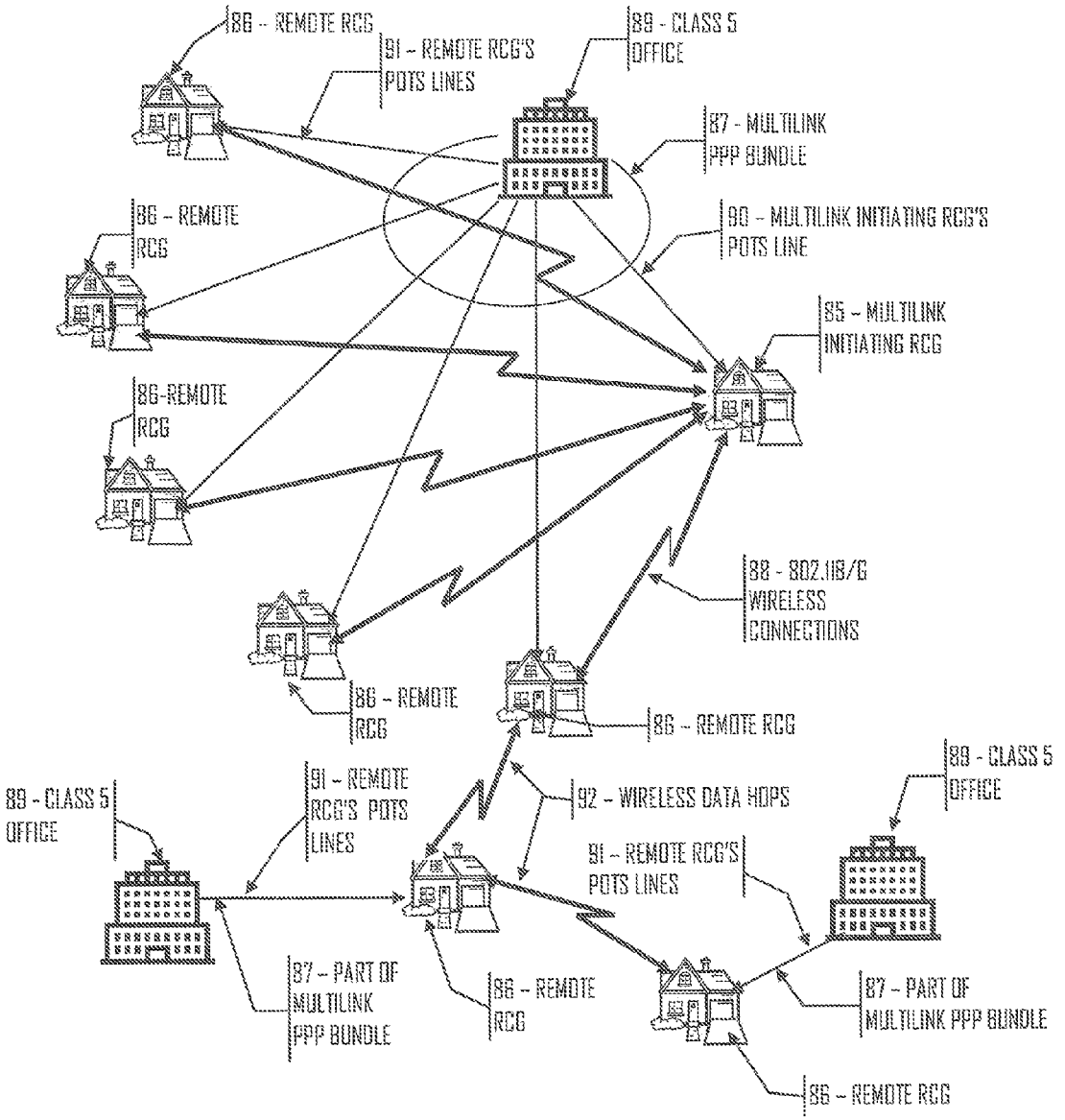

86 - REMOTE RCG
91 - REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 - REMOTE RCG
90 - MULTILINK INITIATING RCG'S POTS LINE
85 - MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 - REMOTE RCG
86 - REMOTE RCG
89 - CLASS 5 OFFICE
91 - REMOTE RCG'S POTS LINES
92 - WIRELESS DATA HOPS
89 - CLASS 5 OFFICE
91 - REMOTE RCG'S POTS LINES
87 - PART OF MULTILINK PPP BUNDLE
86 - REMOTE RCG
87 - PART OF MULTILINK PPP BUNDLE
86 - REMOTE RCG

FIG. 9

MULTIPATH COMMUNICATION DEVICES AND METHODS

RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 13/531,294 filed Jun. 12, 2012, which is a continuation of U.S. patent application Ser. No. 12/581,852 filed Oct. 19, 2009, which is a continuation of U.S. patent application Ser. No. 10/686,375 filed Oct. 14, 2003, which claims priority to U.S. Provisional Application Ser. No. 60/418,521, filed Oct. 15, 2002, all of which are incorporated by reference herein.

BACKGROUND OF INVENTION

The primary function of the RCG is to provide a platform for Competitive Local Exchange Companies (CLECs) to compete with the Local Exchange Companies (LECs) for residential voice and data services. The LECs have a strangle hold on the "last mile" of copper over which almost all residential customers receive their communications services. Today, most CLECs resell the existing services that are offered by the LECs. CLECs make their money by purchasing these services from the LECs at a discount and marking them up to the customer. Since these services are regulated and controlled by the Public Utilities Commission (PUC) the pricing for these services to the CLECs is set. The monthly CLEC discount is approximately $5 to $6 per line per month for basic rate services. This means, in practicality, that a CLEC can only charge an additional $5 or $6 to the residential customer for basic rate services otherwise they would be more expensive than the LEC, and no one would buy the services from them; telephone customers would simply stay with the LEC.

To be competitive then, CLECs try to sell additional services such as call waiting, caller ID, etc. where they have as much as a 50% margin. Some CLECs also bundle long distance services with their packages as additional incentive to get residential customers to buy local telephone service from them. Since long distance fees are as low as pennies per minute to the customer, there is little profit in long distance for the CLECs. As it is, the pricing structure is such that the LECs will stay in control of the residential market, and the CLECs are nothing more than a marketing arm of the LEC. This structure also keeps the CLECs at an equal competitive advantage, or disadvantage, with respect to each other. The only thing that one CLEC could do to gain more customers is to be a better marketier. Since the CLECs are unable to discount their services because their margins are too slim as it is, the net effect is that the consumer looses by not really getting competition in the residential markets, and prices are kept artificially high.

For the CLECs to be truly competitive in the local telecommunications markets, they must be able to do more than simply resell the LECs services. CLECs must be able to offer many more features or services than those that the LEC provides, and they must be able to do this at a lower cost, in order to attract new customers.

So, what new services can the CLECs offer? As things stand today there are none, with the exception of DSL or Cable services which require tremendous infrastructure costs on behalf of the CLEC. However, by deploying an RCG in a residence, CLECs can offer advanced new calling features and services over the existing POTS line. Their costs for the POTS line from the LEC remains the same, but they can now charge for high bandwidth data services as well as additional

calling and messaging features that the LECs cannot offer. This is their competitive advantage.

Competition:

Many companies are currently trying to provide VoIP services to residential customers over high-speed or broadband backbones such as DSL and cable modems, over Internet connections via a computer. The high-speed services require expensive infrastructure enhancements to the local telephone companies' facilities and cable plants, as well as expensive modems at the customer's end. These services are also difficult to deploy and too complicated for the average user. Internet based VoIP services suffer from Internet delays caused by a lack of true Quality of Service (QOS) capabilities across the Internet. Existing VoIP services also require access to a computer and a technical knowledge to be able to make it work. Because of these problems, VoIP services are primarily targeted at the corporate market place where private IP networks that can carry VoIP services with a true guaranteed QOS exist, or can be controlled.

The only available alternatives for the residential user for high speed services are DSL and cable modems. DSL and Cable based communications reach only a small segment of the population, and growth has failed to live up to initial expectations. The recent collapse of the internet boom has led to the failure of many DSL service providers and has effectively eliminated DSL as a potential service for most POTS users for the immediate future.

SUMMARY OF THE INVENTION

The RCG combines the capabilities and features of IP routers, Class 5 circuit switches and wireless LANs in a small stand-alone external modem like device. Additional capabilities for a hands-free speakerphone device with a large touch display are also detailed. The RCG can employ a large display with sufficient resolution to provide a functional user interface to access all of the advanced features offered by the RCG, but also to be able to provide video telephone services.

The device is placed in a residence and connected to the primary POTS line coming from the LEC. Up to three standard telephones or FAX machines (or any combination) are typically connected into the RCG. It also has a Universal Serial Bus (USB) and/or a 10-100 Ethernet interface for connection to a computer or a Local Area Network (LAN). In addition, it has an 802.11b/g wireless interface for wireless home networking as well as broadband-to-the-home services.

The system is installed in a customer's home by simply plugging it into the existing incoming telephone line that provides POTS services from the LEC. One or more standard telephones are then plugged into its three line-output jacks. This is the simplest and most basic usage. In this implementation, the user only is interested in gaining additional telephone lines into the household. No computer connection is required in order to use the system. However, if data communications are desired, then there are three additional interfaces for computer connectivity. Typically either an Ethernet port, USB port or firewire (IEEE 1394) port is used to connect to a PC or LAN. The 802.11b/g interface is for wireless communications between the RCG and PCs, other RCGs as well as any other types of compatible wireless devices. A version of the RCG includes a speakerphone and video camera to provided for video telephone services.

Services Provided by the RCG:

The following discussion refers to FIG. **1**. The RCG has a main system processor that is responsible for all house keeping and traffic routing tasks. The Main CPU **19** routes data to

and from the Ethernet Port **11**, USB Port **12**, Modem/DAA **41**, DSP Engine **33**, 802.11b/g Module **36** and the Display and Keypad **10**.

The RCG provides a total telecommunications communications services package for residential and small business customers. With the RCG, a CLEC can offer its customers dialtone for up to three separate telephone numbers per residence (the limit of three telephone numbers is an arbitrary number based upon typical residential usage and is not a limit imposed by the system), all local and long distance services, 24/7 always-on Internet access, a host of custom messaging and calling features, as well as Broadband access and lifeline service. All of these services can be offered over a customer's existing POTS line, and it doesn't require any network infrastructure build out like DSL and Cable services. Because there is no expensive network equipment required, it can be readily deployed throughout the country to expand the CLECs customer base quickly.

The RCG is designed to enhance, not replace, the existing telephone line, enabling it to provide new combined packetized voice and data services. Meanwhile, all existing telecommunications infrastructure and equipment will continue to work seamlessly with the RCG. Aside from simply installing the low cost RCG device in the home telephone wiring, no other equipment needs to be purchased by either the home owner or telephone companies. This eliminates the tremendously expensive infrastructure costs for communications companies that are trying to provide voice services using DSL or cable modems.

The RCG VIP Home Gateway Features:

Up to three telephone lines i.e. numbers, over a single POTS line and/or wireless connection.

Ethernet, USB and IEEE 1394 computer interfaces.

Full G1, G2 and G3 FAX support.

Full support for all CLASS services.

Broadband networking for home computers and appliances as well as wide area networking using a combination of a plurality POTS lines connected to a plurality of RCGs and/or a direct wireless connection to a wireless access point. (These interfaces allow smart devices to communicate to other devices within the home, or over the Internet through the RCG.)

Automated, remote upgradability and configuration. (Requires the customer to do nothing.)

Transparent user operation. (User doesn't have to know that any new technology is being employed)

100% compatible with existing public telephone system.

Video Telephone capabilities.

No local or long distance usage charges.

No Internet access fees.

Lower monthly communication costs.

Multiple telephone calls at the same time.

Voice messaging, follow me features, call forwarding, automatic call back, conferencing, custom call routing. Home networking capabilities, all CLASS calling features, high speed broadband networking, continuous 24/7 internet access. and many others.

All of these features are available even while connected to the Internet.

Very low cost of entry into the market, especially as compared to broadband alternatives.

New calling features that are not currently available to home users.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows the RCG functional block diagram with the preferred embodiment of an 802.11 wireless connection.

FIG. **2** shows the network topology for native RCG to RCG communications.

FIG. **3** shows the network topology for an RCG to PSTN call.

FIG. **4** shows the RCG top view with associated functions.

FIG. **5** shows the RCG rear view and associated connections.

FIG. **6** shows a typical application with peripheral equipment connections.

FIG. **7** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity.

FIG. **8** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with connection to a broadband neighborhood access point (Wi-Fi hot spot).

FIG. **9** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with wireless data hopping with POTS connections through numerous different Class 5 offices.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment is detailed herein using the ubiquitous 802.11 wireless protocol. It is by no means insinuated that this is the only wireless scheme that can be used by this device; rather, it is intended that any wireless transmission scheme can be used for wireless communications between this device and other wireless devices as various applications may dictate.

System Initialization

Refer to FIGS. **1**, **2** and **3** for the following discussion. When the RCG is first plugged into an AC power outlet the Main CPU **19**, performs a Power-on Self Test (POST) routine. Once the POST completes and the RCG is connected to an active POTS line, connected to the LEC, by means of the Incoming POTS Port **40**, the RCG automatically initiates a modem connection via the Modem/DAA **41**, to a registration service via a toll free 800 telephone number. The registration service connects directly to the service provider's sales or customer service offices via a VoIP connection. An operator or an automated service answers the call and sets up a new account for the customer. Once the account is set up, the service provider's network automatically sends control information to the device to store the required routing and feature/service information in its non-volatile memory of its Main CPU **19**. As part of this information, a local dialup telephone number is sent to the device that it will use for local network access in the same fashion as a standard ISP connection is made from a home computer. The URL of the Softswitch/SIP Proxy Server and Registrar **51** that will be controlling this particular device is also stored at this time. During the service activation and configuration process, the customer service operator can send test requests to the device, as well as call into it on another telephone number (assuming an additional telephone number is part of the users class of service) or the speakerphone to verify that it is configured and working properly. The final step of the configuration and initialization process is to register the device with the appropriate Softswitch/SIP Proxy Server and Registrar **51** so that the Softswitch/SIP Proxy Server and Registrar **51** knows that it is the controlling SIP Proxy for this RCG. Also configured at this time is the username/password verification server (this is a standard network device and is not shown) that is used to allow the RCG's modem to make a connection onto the service provider's network. Once the RCG configuration is completed, it disconnects the call by hanging up the Modem/DAA **41**, then dials the new local network access number that

had been sent during the configuration process and establishes a constant local network connection. This connection is maintained continuously on a 24/7 basis, and is immediately reestablished whenever it drops. Should the RCG become unable to reestablish this connection after several tries, it will switch over to failsafe mode and inform the user via the Display and Keypad **10**. The RCG will try to reestablish the connection every few minutes until it finally succeeds.

By default, the first telephone port, POTS 1 Port **30**, is assigned as the termination port for the existing POTS service that is connected to Incoming POTS Port **40**. This is the existing telephone service that the user already has as his primary telephone service from his LEC. POTS 1 Port **30**, typically has connected to it a standard telephone set that does not require any power (other than that derived over the POTS interface) to operate properly. POTS 1 Port **30** is the Lifeline telephone port for the user. In the case that all power is lost to the RCG, POTS 1 Port **30** will fail to a direct connection to the Incoming POTS Port **40** telephone line that comes into the RCG from the LEC to provide uninterrupted telephone services to the user. In this state, however, none of the enhanced VoIP services of the RCG are available to the user since the user simply has a stand POTS telephone service to the LEC.

Two additional and unique telephone numbers can be assigned to the other two telephone ports, POTS 2 Port **29** and POTS 3 Port **28**, by the service provider at any time. These numbers are drawn from a pool of available telephone numbers assigned to the service provider. POTS 2 Port **29** and POTS 3 Port **28** must to have standard telephone numbers assigned to them so that the PSTN is able to route calls from its network to these ports. For calls originating from IP based telephones, these numbers are not necessarily needed since POTS 1 Port **30**, POTS 2 Port **29** and POTS 3 Port **28** are uniquely identifiable to IP networks via their IP addresses assigned through the Dynamic Host Configuration Protocol (DHCP) at the time that the RCG establishes a connection to the service provider's network. Since POTS 2 Port **29** and POTS 3 Port **28** must have a telephone number assigned to them, it is a matter of convenience to use the assigned telephone numbers as part of their SIP address for IP routing of their data. In this way, all three user POTS ports, POTS 1 Port **30**, POTS 2 Port **29** and POTS 3 Port **28** are all addressed the same manor.

At this point, the user is able to take advantage of all of the RCG's features that have been activated according to his service agreement. The user can at any time connect additional telephones, a computer or a computer network to the RCG. The user will only be able to use those telephone ports (POTS 1 Port **30**, POTS 2 Port **29** or POTS 3 Port **28**) that have been activated, and assigned unique telephone numbers by the service provider. Any type of standard telephone can be connected to the three POTS ports, POTS 1 Port **30**, POTS 2 Port **29** and POTS 3 Port **28**. In the event that a cordless telephone or a telephone that derives its power from an AC outlet is connected to POTS 1 Port **30**, the lifeline functionality of this port will be ineffective since the telephone itself will not operate once power is lost.

The speaker phone feature of the RCG, comprised of Speakerphone Drivers **22**, Microphone **24**, Speaker **25** and DSP Engine **33**, can be used on any of the activated telephone numbers and is by default enabled to operate on POTS 1 Port **30**. Once either of the other two telephone ports, POTS 2 Port **29** or POTS 3 Port **28**, is activated, the speakerphone function is activated for those lines as well. To use the speakerphone for any assigned telephone number, the user simply presses either the Line Select Button **79-81** for Line 1, Line 2 or Line 3 on the face of the RCG, and the speakerphone function is activated on that line. This is convenient for answering any call directly at the RCG. The RCG may or may not have a number keypad for originating calls. This feature may be added or removed based upon the target market price points.

The determination as to which Inter Exchange Carrier (IXC) the RCG will route its data through is determined by any of a number of criteria including, but not limited to, whether the RCG is a private labeled product, or which carrier has the lowest cost routing, or if a specific carrier is specified by the customer, or and number of other considerations. The RCG can be programmed to change its routing path to any IXC at any time by the service provider. Complicated routing algorithms can be programmed into the RCG to control which IXC it will use at any time.

Failsafe Mode

During any time that the RCG is in failsafe mode i.e. Lifeline failsafe logic **39** is activated, the RCG will only be able to receive or initiate telephone calls via the telephone connected to its primary telephone port, POTS 1 Port **30** or through its speakerphone feature. In this condition, all activated telephone numbers are ported via the PSTN to the primary (first) telephone number for delivery to the user's telephone that is connected to POTS 1 Port **30**. While in failsafe mode, the modem is not activated, and the RCG appears to the local Class 5 office as a standard telephone, and the PSTN will route all incoming calls to the RCG as it normally would to any standard telephone.

Call Flow 1:

Dialed call origination from a telephone connected to an RCG POTS port and terminating at another user's RCG POTS port:

When a user picks up a telephone connected to any of the three POTS ports, POTS 1 Port **30**, POTS 2 Port **29** and POTS 3 Port **28**, an off hook condition is detected by the SLIC/CODEC Interface **27** that is connected to the DSP Engine **33** by way of the DSP Audio Interface **31**. The DSP Engine **33** responds by sending digitally generated dialtone to the appropriate POTS interface over the DSP Audio Interface **31**. (Note: all BORSCHT telephony functions are performed by the DSP Engine **33** and the SLIC/CODEC Interface **27**.) Upon hearing the dialtone, the user enters the desired telephone number on his telephone keypad. The Dual Tone Multi-Frequency (DTMF) digits that the user dials are decoded within the DSP Engine **33**. The dialed digits are transferred to the Main CPU **19** via the CPU/DSP Communications Path **34**. The Main CPU **19** polls the DSP Engine **33** approximately every two milliseconds looking for data. The Main CPU **19** polling rate varies according to the process that is being performed. The CPU/DSP Communications path **34** also can generate an interrupt to force data transfer between it and the Main CPU **19**.

The Main CPU **19** generates a SIP Invite IP packet using the dialed digits as the called destination address and the URL of its local controlling SIP Proxy Server which was programmed into the RCG during the configuration process. The Main CPU **19** passes this SIP packet off to the Modem/DAA **41** for transmission over the network. The RCG Modem/DAA **41** is connected to and communicating with a modem in a modem bank located in the Inter Exchange Carrier's (IXCs) facility. This facility may actually be located in the LEC's physical plant or it may be physically located at another location.

Referring to FIG. **2**, User A RCG **44** is connected via its modem to the LEC's local Class 5 Office A **47**. In this example, the service provider's connections to the IXC A Modem Bank & Router **48** are through IXC A Inter-Office Trunks **46**. The service provider may or may not be the IXC.

If the service provider does not have its own network, then it will purchase capacity from an IXC and route its traffic to that IXC's facilities. The SIP Invite IP Packet that is sent from User A RCG **44** transits the LEC's Class 5 Office A **47** facilities and is routed to the IXC A Modem Bank/Router **48** via the IXC A Inter-Office Trunks **46**. It is the job of the router to take the IP packet and route it on to its intended destination, in this case the appropriate SIP proxy server **51**. The router uses the URL for the Softswitch/SIP Proxy Server and Registrar **51** contained in the SIP Invite to know where to route the packet. (Note: The Softswitch, SIP Proxy Server and Registrar are logical devices that may reside in a single computer system, or may be implemented as completely separate devices. In this example, the Softswitch, SIP Proxy Server and Registrar are all shown as a single physical device running these three separate processes.) The IXC A Modem Bank/Router **48** sends the SIP Invite IP packet on to Softswitch/SIP Proxy Server and Registrar **51** via an IP based network route **52**.

The SIP Proxy Server process running on Softswitch/SIP Proxy Server and Registrar **51** performs a look up to determine the termination destination for the call using the dialed digits passed along in the SIP Invite IP packet. In this example, the terminating device for User B RCG **56** is via IXC B's Modem Bank/Router **49** then through Class 5 Office B **50** and over User B POTS line **55** and finally to User B RCG **56**. Not covered in detail here is the SIP message handling since it is completely covered in IETF RFC2543. This example shows that both the originating and terminating ends of this call are controlled by the same Softswitch/SIP Proxy Server and Registrar **51** device. Where the originating and terminating ends of a call are controlled by different Softswitch/SIP Proxy Server and Registrar devices, an additional level of SIP messaging is used between the two SIP Proxy Server processes of each of the Softswitch/SIP Proxy Server and Registrar devices to locate and control the terminating location of the call. Again, that information is covered in IETF RFC2543 and is repeated here.

After the call routing is setup using SIP, and User B answers the call, the Softswitch/SIP Proxy Server and Registrar **51** device sends IP address of the originating User A RCG **44** to the User B RCG **56** and the IP address of User B RCG **56** to User A RCG **44**. Once both RCG's have the other's IP address, they then communicate directly to each other using Real Time Protocol (RTP), and the Softswitch/SIP Proxy Server and Registrar **51** device is no longer part of the connection. This direct communication is shown as IP based RTP Stream **57** between IXC A Modem Bank/Router **48** and IXC B Modem Bank/Router **49**.

On the receiving end of the call, referring back to FIG. **2**, User B RCG **56** receives the SIP Invite data stream through its Modem/DAA **41** and passes it on to the Main CPU **19**. The Main CPU **19** reassembles the SIP IP packet and interrogates the header information to determine which POTS port, POTS 1 Port **30**, POTS 2 Port **29** and POTS 3 Port **28** the call is destined for based upon the dialed number contained in the SIP Invite message. The Main CPU **19** commands the DSP Engine **33** to control the SLIC/CODEC Interface **27** to apply ringing voltage to the selected POTS port to ring the phone. A corresponding SIP 180 (ringing) message is sent back to User A RCG **44** in the reverse direction. When the phone attached to the selected POTS port is answered, the off hook condition detected by the SLIC/CODEC Interface **27** is sent through the DSP Engine **33** to the Main CPU **19** that sends the SIP 200 OK message back to User A RCG **44** to let the RCG know that the call was answered by User B RCG **56** and to turn off the audible ringing tone for User B. Once the call is established, User A RCG **44** sends and ACK F12 SIP message to User B RCG **56** indicating that User A RCG **44** understands that the call setup has been completed.

The two RCGs now exchange SIP messages that include the type of voice encoding that will be used such as G.729, G.723.1, G.711 etc to configure their RTP streams so that they can reliably transfer the user information between them. At this point the call (voice data) is sent between both RCGs and a normal telephone conversation takes place between the user A and user B.

Call teardown is accomplished by either user hanging up their telephone. The RCG of the terminating end (the end that hangs up the phone first) detects the on-hook condition and sends a SIP Bye message to the other end. The other end upon receiving the SIP Bye message responds with an OK 200 SIP message and disables the appropriate POTS port that the user was using.

The Speakerphone interface can be used for either end of a telephone conversation in exactly the same way as described above except that the corresponding POTS port that the call was intended for is disabled if the call is answered via the speakerphone.

Call Flow 2:

Calls between an RCG device and a PSTN telephone:

Refer to FIG. **3** for the following discussion.

In the previous call example, the PSTN network had nothing to do since the call was over a previously established modem connection between two RCGs. In the cases where a call originates or terminates to a standard telephone serviced by a Class 5 office, the process is a bit more complicated.

When a call originates from a user via an RCG, such as User A RCG **44**, the call handling practices are exactly the same up to the point that the SIP Proxy Server process in the Softswitch, SIP Proxy Server and Registrar **51** performs a lookup to determine how to route the call. In this case, the SIP Proxy Server process determines that the call terminates at a standard PSTN telephone attached to the Class 5 Office B **50**. Since the call originates as a native VoIP service, it must be converted to a standard switched circuit based service to be able to be delivered to User B's telephone **61**. The conversion is performed by the IXC's Media Gateway **60** device. In this example, the SIP Proxy Server process routes the call via the IXC's Media Gateway **60** device instead of through the IXC B Modem Bank/Router **49** as before. The SIP Proxy Server process sends a SIP Invite to the IXC's Media Gateway **60** device, as well as other control information, to direct the Media Gateway **60** device to terminate the call and to apply the appropriate voice compression algorithm to the media stream to convert it between switched circuit PCM format and the selected VoIP protocol. At the same time, the Softswitch process of the Softswitch, SIP Proxy Server and Registrar **51** device sends commands to the Media Gateway **60** device to cause it to route the call's PCM data to a specific channel on the IXC B Interoffice Trunk **54**. The Softswitch process then generates an SS7 ISUP message that is sent over the PSTN SS7 signaling network to the Class 5 Office B informing it of the incoming call and on which circuit the call has been placed. It is up to the PSTN at this point to ring the User B telephone **61** and process the call between the IXC's Media Gateway and the User B Telephone **61**. The Softswitch process handles the signaling conversion between the PSTN's SS7 network and the IXC's SIP messaging, as well as any other proprietary signaling schemes utilized by the IXC to control its network. The standard SS7 call control messages, such as ringing, busy, ring back etc., all have a comparable SIP call flow control messages. The Softswitch simply maps

the SS7 messages into SIP messages and visa-versa while routing the messages to the appropriate network equipment.

As in the case of a call between two RCGs, the RTP media stream (the actual call data) is routed directly be the IXC A Modem Bank/Router **48** and the IXC's Media Gateway **60** via an IP based RTP Stream **57**.

Again, call teardown is accomplished by either user hanging up their telephone. Depending which end hangs up the phone first, the associated network will generate the appropriate messages which will eventually make it back to the Softswitch process. The Softswitch process will relay the appropriate call control messages between the PSTN and the IXC's SIP based control system.

A telephone call originating from a PSTN telephone is configured and setup in the same fashion as the above description except that the originating messaging begins within the PSTN network instead of the IXC's network.

Personal Computer based communications:

Where the RCG is connected to a Personal Computer (PC) through either its USB Port **11** or Ethernet Port **12**, the RCG operates exactly as a cable or DSL type modem device. The RCG is simply a pass through for the computer's data. The RCG receives the IP packets (of whatever type) from the computer and sends the information unchanged to the Modem/DAA **41** interface for transmission over the Internet. Received information from the Internet is processed in the reverse way.

Dynamic Bandwidth Allocation:

When a modem connection is established between the RCG and the "Network", the total available bandwidth of this connection is used in a shared/prioritized fashion. Voice services (calls) take precedence over data services. Therefore, when no calls are in progress all of the available bandwidth is used by data type services such as surfing the Internet or uploading/downloading files. However, when a call is to be passed through the RCG, the required bandwidth for the call is deallocated from the data services and prioritized for the telephone call. This necessary because the Quality Of Service (QOS) is important for effective communications over electronic networks. Since the voice data is carried over a "data centric" network topology (an IP based network), call quality can suffer greatly. Every effort must be taken to eliminate or reduce the packet delay through every network element to be able to provide the best call quality. For data applications such as surfing the Internet or downloading files packet delay is acceptable and expected, and it does not affect the "quality" of the data.

Since all voice and data is transmitted as packets, there are no "time slots" or other type of "channelization" associated with the transmission of this data over either the POTS line or the wireless interface. Channelization of the voice data does occur within the SLIC/Codec Interface—**27** but is converted into IP packets by the DSP engine—**33** and is handled as packets from that point on.

Regardless of whether the call is originating or terminating at the RCG, the bandwidth allocation process is the same. When the SIP call setup messages are processed, the type of voice compression that will be used is defined. The RCG Main CPU **19** handles the IP packet flow between the DSP Engine **33**, USB Port **12**, Ethernet Port **11**, 802.11b/g Module **36** and the Modem/DAA **41** devices giving priority to the voice packets to and from the DSP Engine **33** and the Modem/DAA **41** interfaces. Voice compression algorithms create IP packets at a specified number of packets per second. These packets are handled by a timed process in the RCG. This process is started during call setup so that the packets are handled at the correct rate based upon the compression algorithm's packet generation rate. There is no priority assigned between the voice packets of each of the three different POTS Ports **28-30**. When more than one voice call is in progress, they are handled in a round robin fashion based upon the packet rate for the compression algorithm used. If, for example, two calls are using a compression scheme that generates packets every 2 milliseconds, and the third generates packets every 4 milliseconds, then the calls utilizing the faster packet rate will be polled at twice the rate as the call using a slower packet rate but they are not given priority "over" the other call. Only when there are no voice packets ready for transmission to the Modem/DAA **41**, i.e. during the approximately 2 to 4 millisecond packetization period between packets, will any pending data packets received from the USB Port **12**, Ethernet Port **11** or the 802.11b/g Module **36** be sent to the Modem/DAA **41** for transmission over the network.

Thus, the POTS bandwidth is allocated on a per packet basis, not on a "time slot" or "channelization" or even a "frequency" basis as it the case with T-Carrier, DSL or channelized DSL systems. The same is true for the wireless interface, whether it is carrying pure data or voice.

Security is currently a big concern in today's networks, and especially with wireless 802.11 transmissions. For this reason, the RCG defaults to route voice data over the users POTS connection via Incoming POTS Port **40**. As security concerns regarding wireless communications transmissions are addressed and alleviated, voice call data can, and will, be routed over the wireless interface via the 802.11b/g Module **36**.

FAX Transmission:

Group I, 2 and 3 fax transmission is completely supported by the RCG. Fax transmission has the same priority as other voice communications. That is to say that FAX transmission is treated the same as a voice call and takes precedence over native IP data traffic.

Broadband Over POTS:

One of the primary functions of the RCG is to be able to transfer large files such as video files over the POTS lines to a residence. The ability to do this is limited by the maximum of 56 Kbps due to the design of the digital Class 5 office linecards and network transmission schemes based upon T carriers. Typical Class 5 linecard design samples the POTS lines at a rate of 8,000 samples per second. Typically, each sample is digitized into 12 to 16 bits by a codec device. The digitized sample is then companded to an 8 bit sample (1 byte) which makes up the PCM data stream that is transferred over the PSTN. Therefore, each POTS line is sampled at an effective rate of 64 Kbps. Since legacy T1 transmission equipment uses robbed-bit signaling, the maximum guaranteed transmission rate for the PSTN as a whole is 56 Kbps. Because of this limitation, standard POTS lines can only guarantee a maximum of 56 Kbps transfer rate under the best conditions. DSL equipment gets around this problem by installing DSL Access Multiplexing (DSLAM) equipment at the Class 5 office end of the POTS line. By routing around the linecard, as well as routing the data directly over the Internet or other private IP based networks, and therefore the 64 Kbps sampling rate, DSL is not bandwidth limited like PSTN traffic is. DSL, however, suffers from the very high costs associated with the purchase, installation, maintenance, floor lease costs, etc. DSL also suffers from very high deployment costs resulting from the labor intensive process to turn up each line. Each DSL "POTS" line must be inspected, conditioned and all load coils removed.

The RCG gets around the 56 Kbps POTS limitation as well as the DSL problems by using the standard POTS lines as they are, and not requiring any additional equipment to be installed

at the Class 5 end of the POTS line. This technique simplifies deployment and drastically cuts costs.

Multilink PPP Connections:

Referring to FIG. **7**, the RCG implements broadband over POTS by employing an 802.11b/g wireless interface to configure a multilink PPP bundle—**87** (per RFC 1990) comprised of the POTS lines connected to up to 32 RCGs. The limitation of 32 RCGs in a multilink PPP bundle is an arbitrary number and can be scaled up or down as required to support changes in network equipment capabilities. An 802.11b/g interface—**87** is shown as the preferred embodiment, since its 11/54 Mbps interface is considered sufficient bandwidth at this time also, its transmission distances are sufficient for implementation of this device, as opposed to other shorter ranged wireless transmission schemes. However as time goes on, some other wireless interface may be more desirable. There is nothing special or specific to the 802.11 wireless interface that makes it particularly suited to this application. Any wireless interface scheme can be used to implement this device.

The 802.11b/g interface—**88** on an individual RCG is also used to provide a peer-to-peer wireless home networking environment to other 802.11 compatible wireless component within the residence (such as a hand-held computer device) while acting as an always on dialup Internet gateway over the POTS line—**40** for the other wireless devices. An RCG that is transferring a very large file can request the services of 31 (in this embodiment) other RCGs to assist in the file transfer using their respective POTS lines. A single RCG can therefore gain the combined bandwidth of up to 32 POTS lines transferring data at as much as 56 Kbps each to transfer information. This is roughly equivalent to a transfer rate of 1.79 Mpbs in the inbound direction (towards the RCG) and approximately 1.075 Mbps in the outbound direction (towards the PSTN).

The multilink PPP connection—**87** is initiated by an RCG when it determines that the file (or streaming service) that it is to download (receive) is of sufficient size or requires a minimum amount of bandwidth to justify the use of a multilink PPP connection. This determination can be made on many different criteria such as the file size, type of data being transmitted, the type of compression if any, a Quality-of-Service requirement or any other pertinent information. (Since a certain amount of overhead is required to set up a Multilink PPP connection, it doesn't make sense to use it for small or low data rate transfers.)

Multilink PPP Bandwidth Allocation and Initialization:

Referring to FIG. **7**, an RCG—**85** that decides to initiate a multilink PPP session with a remote computer i.e. internet URL, requests a multilink PPP session with that URL resource via Link Control Protocol (LCP) session management. The initiating RCG—**85** and the remote server computer (not shown) will negotiate the pertinent multilink parameters such as compression, packet size, sync/async, link quality monitoring, bit stuffing etc. As part of a successful multilink PPP session setup, the initiating RCG—**85** receives a multilink PPP session ID, or "magic number", which is used to identify this particular multilink PPP session and is also used for adding or removing links from the multilink bundle—**87**. Once the multilink bundle is setup, the initiating RCG—**85** begins data transfer across its POTS interface—**90** with the far end computer system. The initiating RCG—**85** then looks up the addresses of up to 31 (in this embodiment) other RCGs in its router tables to use for the multilink PPP transfer. (If a Neighborhood Access Point is available the RCG could request service through it instead of setting up a Multilink PPP connection—see FIG. **8**.) The initiating RCG—**85** determines the number of remote RCGs—**86** that it wants to use to get the desired bandwidth for the transfer and sends multilink PPP service requests via the 802.11b/g wireless connections—**88** to the selected remote RCGs—**86**. The selected remote RCGs—**86** respond back to the initiating RCG with either an acceptance or denial of multilink PPP service request. This decision is made based upon the remote RCG's currently available POTS bandwidth and the current local demands for that bandwidth. The remote RCG—**86** makes a decision to participate in a multilink PPP service for an initiating RCG if its POTS line—**91** has a current average bandwidth utilization of less than some arbitrary limit such as 8 Kbps to 16 Kbps. This 8 Kbps to 16 Kbps bandwidth utilization represents about two concurrent voice conversations using standard voice compression techniques, or some small amount of data transmission occurring on the remote RCG's POTS interface—**91** or a combination thereof. Assuming that the remote RCG—**86** has a modem connection speed somewhere between 33 Kbps to 56 Kbps, this would leave approximately 17 Kbps to 40 Kbps of POTS bandwidth that the remote RCG—**86** could offer to the initiating RCG—**85** for use in its multilink PPP bundle—**87**. Of course, if there is no activity on the remote RCG—**86** POTS line, then the entire bandwidth will be used for the multilink transfer. If the remote RCG—**86** accepts the multilink PPP service request from the initiating RCG—**85** it also sends its currently available bandwidth on its POTS line—**91** that the initiating RCG—**85** will have available to it for the multilink PPP transfers. The initiating RCG then selects which of the responding remote RCGs—**86** it will use for the multilink PPP bundle—**87** and sends them a multilink initialization packet containing the URL of the destination as well as the multilink PPP session ID (magic number) and any other pertinent information required for the remote RCG to join in the existing multilink PPP bundle—**87**. Each remote RCG POTS interface—**91** participating in a multilink PPP bundle, represents a logical "link" in the initiating RCG's multilink PPP bundle—**87**. The remote RCGs—**86** then send a multilink PPP packet (over their respective POTS lines—**91**) to the destination URL with the multilink PPP session ID and request to be added to that multilink PPP bundle—**87**. The destination URL accepts the request of each of the remote RCGs—**86** and begins sending data packets to each over their respective POTS lines—**91**. When the remote RCGs—**86** receive data packets sent over their respective POTS lines—**91**, that are destined for the multilink PPP bundle—**87**, they simply relay the data packets over their 802.11b/g interface—**88** to the initiating RCG—**85**. It is the responsibility of the initiating RCG—**85** to perform all housekeeping tasks associated with the multilink transfer such as detection of lost packets and data packet reassembly, if those functions are required. Typically, lost packet detection and retransmission and reassembly are performed at higher OSI layers by the requesting software such as a browser. The remote RCGs—**86** are simply data transport nodes and do not perform any data processing on data received over a multilink PPP bundle destined for another RCG.

The initiating RCG—**85** of the multilink PPP bundle—**87** continually monitors the bandwidth of each remote RCG's—**86** multilink link which together comprise its multilink bundle—**87**. When the available bandwidth for the multilink PPP link of an individual remote RCG—**86** falls below an arbitrary minimum set by the initiating RCG—**85**, the initiating RCG—**85** instructs the offending remote RCG, via its 802.11b/g wireless interface—**88**, to remove itself from the multilink bundle. The remote RCG—**86** will then notify the remote computer (URL) to be removed as a link in the current

multilink bundle on which it is participating. Alternatively, a remote RCG—**86** can inform the initiating RCG—**85** of local demands on its POTS bandwidth, and request that the initiating RCG—**85** remove it (the remote RCG—**86**) from the participation in the initiating RCG's multilink bundle—**87**. The remote RCG—**86** will not unilaterally remove itself from participation in a multilink bundle without prior notification to the Initiating RCG—**85**. The remote RCG—**86** must get authorization from the initiating RCG—**85** to remove itself from the bundle, since the initiating RCG—**85** will have no way of knowing if the loss of data from that remote RCG is due to some sort of failure or from the remote RCG simply removing itself from participation in the multilink bundle—**87**. Also, for services that require a minimum Quality of Service (QOS) such as streaming video, the initiating RCG—**85** needs to control the multilink bundle—**87** bandwidth, and it can not do that if remote RCGs—**86** drop out of the multilink bundle—**87** at will. When a remote RCG—**86** requests to be removed from participation in a multilink bundle—**87**, the initiating RCG—**85** must immediately grant the request. If the initiating RCG—**85** were to not grant the request, then the remote RCG—**86** could, in worst case, delay or drop incoming multilink packets destined for the initiating RCG—**85**. If this were to happen, the initiating RCG—**85** will have missing packets and could over run its reassembly buffer (if reassembly is being performed by the RCG) causing catastrophic data loss and potentially have to restart the entire transmission. In the least case, the initiating RCG—**85** would have to initiate retransmission of potentially many packets which it assumes to be lost, but may simply be delayed by the remote RCG—**86**. Once a remote RCG—**86** has been removed from participating in a multilink bundle—**87**, the initiating RCG—**85** will then look up another remote RCG in its router tables that can be used to participate in the multilink PPP bundle—**87**, and request that the new remote RCG—**86** to join the existing multilink bundle—**87**. This is necessary to maintain a minimum Quality of Service. Since RCGs prioritize their bandwidth requirements based upon their own "local" service requirements, their participation in any multilink PPP service is available only to bandwidth that is not required for its own current local demands. Therefore, a remote RCG's—**86** bandwidth that is available for multilink services can change at any time. The dynamic reassignment of remote RCGs that participate in a multilink bundle is also required to prevent a remote RCG—**86** from receiving packets so slowly that the originating RCG—**85** interprets this delay as lost packets. When the initiating RCG—**85** determines that a packet has been lost, and it is performing packet reassembly, it will, itself, request that the remote computer retransmit the lost packet. The initiating RCG will not ask any remote RCG—**86** to perform retransmissions or any other kind of data computations or manipulations.

Refer to FIG. **8** for the following discussion. In areas where there are existing 802.11 network equipment such as Neighborhood Access Point—**93**, or where there is sufficient bandwidth requirements from an installed base of RCGs to warrant the deployment of a Neighborhood Access Point—**93**, the RCGs will automatically detect the presence of the compatible neighborhood access points and register with that equipment for transport services. In this case, an RCG has an alternative broadband service route in addition to the multilink option. An RCG can communicate directly with a local 802.11 Network Access Point—**93** that is connected to the PSTN or another carrier's network via some sort of high bandwidth backbone such as a T-Carrier or optical carrier connection (T1, T3, OC3, OC12 etc.). The RCGs can communicate directly with neighborhood access points at their full 11/54 Mbps data rates to provide up to that full bandwidth to the user. This functionality is, of course, subject to the Network Access Point—**93** allowing access to its resources to the RCG according to the 802.11 wireless protocol.

This architecture is important since it provides an avenue to relieve the local class 5 offices of congestion that can be caused by a wide spread deployment of RCGs within the class 5 service area. Since each RCG requires a constant 24/7 modem connection, this ties up the class 5 switch in a fashion that it was not designed for. This could lead to wholesale class 5 office expansions which would be extremely expensive, and potentially prohibitive for the Local Exchange Carriers (LECs). By deploying neighborhood access points that operate at 54 Mbps (802.11a/g), in areas where the RCG concentration starts placing too high of a demand on the local class 5 office, the bandwidth from the RCGs can be aggregated by the neighborhood access points into large capacity backbones to relieve the switch congestion. In this case, the RCG POTS interface—**40** can be used solely as a lifeline connection, or when the 802.11 wireless LAN in which the RCG resides is congested. With this implementation, voice calls will be carried over the wireless interface as opposed to the POTS interface on which they would normally be carried. Also, the RCG modem—**41** connected to the POTS interface—**40** would not need to maintain a constant always on connection, it could be a dialed on demand connection and thereby relieving the local class 5 office switch.

Bouncing or Hopping Traffic:

Refer to FIG. **9**. In areas where the density of RCGs is less than the arbitrary number of 32 RCGs within its transmission radius for multilink connections, the RCGs can bounce, or relay, the data traffic between each other to reach other RCGs located farther than the RCGs wireless transmission area. Since the POTS data rate of 56 Kbps is miniscule as compared to the 11/54 Mbps 802.11b/g transfer rate, the overhead associated with bouncing data traffic is not a concern. This will allow for the fastest possible data transfer across POTS lines for every RCG user.

RCGs can also communicate directly with an 802.11a Neighborhood Access Point—**93** device (such as that used in WI-FI networks) that is connected to a data network connection such as a DS3 or OC3 service via a Metro Access Point. Where an RCG has access to a broadband device such as an 802.11a type device, either directly or via a bounced signal across several RCGs, a direct high speed data connection can be used to transfer large files. When an RCG is communicating directly with an 802.11a device, data transfer speeds up to the full 11/54 Mbps can be achieved to speed video transfers for such applications as video on demand.

RCG Router Tables:

The RCG continually monitors its 802.11b/g wireless interface for transmissions from other RCGs or 802.11a Access Points as well as other 802.11b/g wireless devices within the residence. The RCG provides a means to identify and store the addresses of other RCGs and Neighborhood Access Points within its local area. The RCG creates routing tables, much like an IP router device, so that it knows which RCGs are local to itself, and how many hops will be needed to reach the maximum of 32 POTS lines or a Neighborhood Access Point. The RCG can then determine how to route its data transfers to gain the most efficient routing and network efficiencies.

The router tables in each RCG are continually updated by monitoring the 802.11 frames received from other RCGs or Network Access Points. The number of entries in the router tables can be limited to an arbitrary number of other RCGs but contains room for at least 32 entries. For each RCG listed in

the router tables, certain information is kept such as signal strength, if the other device is another RCG or some other 802.11 compatible device, if the other RCG is reachable directly, or if it is accessed via another RCGs by hopping. In the case there RCG hopping is used, the address of each RCG that is hopped is stored in the routing table. When an RCG is first powered up, it monitors its 802.11 interface for a period of time to identify other RCGs or Neighborhood Access Point devices, or other Wi-Fi devices within its transmission area. When first deployed, the RCG will not have any entries in its routing tables. This condition can persist for some time, until another RCG or other 802.11 device is deployed within the former RCGs transmission range. In this state, the RCG can be used for wireless networking within the residence, connecting the local computer to the RCGs always on Internet connection as well as to other wireless devices within the home. When an 802.11 frame is received by an RCG that contains the address of an RCG whose address does not exist in the receiving RCG's router table (as is the case when a new RCG is first installed), the receiving RCG polls the transmitting RCG for its router table information. The received router information is reviewed for other RCG's or other 802.11 compatible devices that are not listed in its own router tables. A decision is made to use some, all, or none of the new route information in its router tables. There is no real limitation on the number of RCGs that can be "hopped" in order to build a complete router table or to reach many more RCGs, Neighborhood Access Points or Metro Access Points.

Equipment and Services Priorities:

Just as voice has priority over data transfers within a single RCG, local RCG traffic (both voice and data) has priority over remote transfer requests by other RCGs. If an RCG is currently using all of its available POTS bandwidth for its own purposes, it will deny any remote RCG's request for access to its POTS line. Only when there is available POTS bandwidth available will an RCG allow other RCGs access to its POTS line. It will, however, bounce the traffic to other RCGs within its transmission area if requested by the originating RCG. In this case, available wireless bandwidth of any RCG (that amount of the 11/54 Mbps not currently used for its own traffic) can be used to relay traffic between other RCGs that do have available POTS bandwidth. In the same fashion, excess wireless bandwidth of any RCG can be by other RCGs to access high speed backbones via Neighborhood or Metro Access Points.

RCGs can also access other 802.11 wireless networks (Wi-Fi for example) that happen to be deployed within their service areas. In this case, access agreements between the RCG service provider and the wireless network operator must be put into place. By remaining compatible with the 802.11 standards, the RCGs capabilities will benefit by the growing WI-FI network infrastructure, an the WI-FI network will benefit by the RCG network.

Voice Over POTS and Data Over Wireless:

Normally, all communications from an RCG will be transmitted over the local POTS line, or a multilink bundle made up of many remote RCG POTS lines. By default, all voice calls will be carried over the "local" POTS line—**40** to alleviate security/privacy concerns and only "data" will be transmitted via multilink bundles. Generally, since voice "data" is compressed locally by the RCG, the required bandwidth for a voice call is so small that it does not make for a good choice to route it over a multilink connection. However, it is possible to route voice calls entirely over another RCGs POTS line. It is also possible for an RCG to transmit voice data over POTS lines connected to other RCGs via multilink bundles or directly over its 802.11 wireless interface, and since the 802.11 specification does support the Wired Equivalent Privacy (WEP) specification, a secured connection can be made in this fashion.

Remote Upgradability

The RCG is designed with the capability for unassisted remote upgradability. The remote upgradability feature is not the same as the storing of operational parameters during the configuration process. This feature allows the system operator to add new features as they are developed, or to correct bugs remotely and without the users knowledge or involvement. This feature can also be used to install a complete new operating system (OS).

Key to the successful implementation of the Remote upgradability feature is that a completely fail-safe routine be implemented that can recover from any failure during the upgrade process and to re-initiate and monitor the upgrade process until it has successfully completed. This process is carried out by loading a boot loader program that is stored in non-volatile memory. The boot loader program provides the minimum capabilities to start up the RCG and connect into the system operator's diagnostics network to download fixes or a new OS. The boot loader program is technically part of the OS, but it cannot be over written by any upgrade process. It is responsible for detecting failure of the RCG and initiating a connection to the diagnostics network. Once connected with the diagnostics network, the boot loader will provide diagnostics support to help correct the RCG's operation and reconfigure the OS.

What is claimed is:

1. A method for establishing and sending data during a multipath connection comprising:

a data-source device receiving multipath information about each of a plurality of network-edge devices that is capable of joining a multipath connection with a data-requesting device, each of the network-edge devices being connected to one or more networks, and each of the network-edge devices being connected to the data-requesting device over a different connection; and

the data-source device performing at least one of (i) sending different groups of data packets to different network-edge devices that are participating in the multipath connection, (ii) sending different streams of data to one or more of the network-edge devices that are participating in the multipath connection, and (iii) sending combinations of different streams and different groups of data packets to one or more of the network-edge devices that are participating in the multipath connection.

2. The method of claim **1**, wherein the multipath information includes a connection ID that is generated by one of the data-source device, one of the plurality of network-edge devices, the data-requesting device and a network device.

3. The method of claim **1**, further comprising:

the data-source device receiving second multipath information about a second network-edge device that is capable of joining the multipath connection; and

the data-source device joining the second network-edge device to the multipath connection.

4. The method of claim **1**, further comprising:

the data-source device receiving multipath information about which network-edge devices are to be removed from the multipath connection; and

the data-source device removing the network-edge devices from being associated with the multipath connection.

5. The method of claim **1**, further comprising at least one of the data-source device, the network-edge devices and the

data-requesting device determining which of the network-edge devices are to be removed from the multipath connection.

6. The method of claim **1**, wherein the data-source device is one of a multipath link aggregator, a network relay, a multipath link server, a server, a network switch, a network router and a device capable of providing multipath services.

7. A method for establishing and sending data during a multipath connection, comprising:

the data-source device receiving multipath connection requests from a plurality of data-requesting devices, each of the multipath connection requests involving a particular multipath connection to a data-requesting device;

the data-source device associating a connection ID to each multipath connection request;

the data-source device using multipath information about each of a plurality of network-edge devices that is capable of joining in a particular multipath connection to a particular data-requesting device, the particular multipath connection having a particular connection ID;

the data-source device notifying each of the network-edge devices that is participating in the particular multipath connection associated with the particular connection ID; and

the data-source device sending data associated with the particular connection ID to the network-edge devices participating in the particular multipath connection associated with the particular connection ID.

8. The method of claim **7**, further comprising: the data-source device sending different groups of data packets to different network-edge devices that are participating in the particular multipath connection associated with the particular connection ID.

9. The method of claim **7**, further comprising:

the data-source device receiving identification of the network-edge devices to be removed from the particular multipath connection; and

the data-source device removing the identified network-edge devices from the particular multipath connection.

10. The method of claim **7**, further comprising the data-source device notifying the data-requesting device when all data has been sent over the particular multilink connection.

11. The method of claim **7**, wherein the data-source device is one of a multipath link aggregator, a network relay, a multipath link server, a server, a network switch, a network router and a device capable of providing multipath services.

12. The method of claim **7**, wherein the connection ID is generated by one of the data-source device, one of the plurality of network-edge devices, the data-requesting device, and a network device.

13. A method for establishing and sending data during a multipath connection, comprising:

a data-requesting device sending a multipath request to a network-edge device where the multipath request indicates that the network-edge device will join a multipath connection associated with the data-requesting device, the data-requesting device being connected over a first connection to a network and over a second connection to the network-edge device, the multipath connection comprising the first connection and the second connection which are capable of receiving data at the same time;

the data-requesting device receiving first data over the first connection from the network; and

after the network-edge device joins the multipath connection, the data-requesting device receiving second data over the second connection from the network-edge device.

14. The method of claim **13**, wherein the first connection and the second connection are each a wireless connection, a wired connection or a combination of wired and wireless connections.

15. The method of claim **13**, wherein the data-requesting device is one of a cell phone, a tablet, a switch, a network device, a router, a computer, a Wi-Fi device, a Wi-Max device, a communications device, a mobile communications device, a near-field communications device, and a Bluetooth device.

16. The method of claim **13**, wherein the network-edge device comprises one or more routers, modems, cell phones, tablets, computers, cellular towers, wireless towers, base stations, wireless base stations, repeaters, wireless repeaters, Wi-Fi devices, networking devices, hot spot devices, Wi-MAX devices, LTE devices, GSM devices, consumer electronic devices, an Internet-ready device, a network switch, a network router, a multipath server and a device capable of providing multipath services.

17. The method of claim **13**, wherein the data-requesting device is capable of connecting to another network device which is capable of joining the multipath connection, and further comprising the data-requesting device receiving data from the another network device after the another network device joins the multipath connection.

18. A data-requesting device comprising:

at least one interface capable of connecting concurrently to a plurality of network-edge devices during a multipath connection, the multipath connection comprising the connections between the data-requesting device and each of the network-edge devices; and

at least one processor coupled to the at least one interface that

sends multipath information to each of the network-edge devices that is capable of joining the multipath connection; and

receives different data at the data-requesting device from different ones of the network-edge devices that are able to join the multipath connection.

19. The data-requesting device of claim **18**, wherein the data-requesting device is one of a cell phone, a tablet, a switch, a network device, a router, a computer, a Wi-Fi device, a Wi-Max device, a mobile communications device, a near-field communications device, and a Bluetooth device.

20. The data-requesting device of claim **18**, wherein each of the network-edge devices comprises one or more network devices, communications devices, cellular devices, tablet devices, router devices, computer devices, satellite devices, Wi-MAX devices, wireless devices, mobile communications devices, Bluetooth devices, and Wi-Fi devices, a network switch, a network router, a multipath server and a device capable of providing multipath services.

21. A method for creating and using a multipath connection, comprising the steps of:

a data-requesting device sending first multipath control information to or through a first network-edge device, the first multipath control information indicates that the first network-edge device will join the multipath connection, the data-requesting device being connected over a first connection to the first network-edge device;

the data-requesting device sending a second multipath control information to or through a second network-edge device, the second multipath control information indicates that the second network-edge device will join the

multipath connection, the data-requesting device being connected over a second connection to the second network-edge device, the data-requesting device capable of receiving different data over the first connection and the second connection at the same time; and

after the first network-edge device joins the multipath connection, the data-requesting device receiving first data over the first connection from the first network-edge device; and

after the second network-edge device joins the multipath connection, receiving second data at the data-requesting device over the second path from the second network-edge device.

22. The method as in claim **21**, wherein the first network-edge device is connected to a network, and wherein the second network-edge device is connected to the network or a different network.

23. The method as in claim **21**, wherein the first connection and the second connection are wireless connections, a wired connection or a combination of wired and wireless connections.

* * * * *

EXHIBIT C

US010868908B2

(12) **United States Patent**
Delangis

(10) **Patent No.: US 10,868,908 B2**
(45) **Date of Patent: Dec. 15, 2020**

(54) **DEVICES AND METHODS FOR MULTIPATH COMMUNICATIONS**

(71) Applicant: **Eric M. Delangis**, Huntsville, AL (US)

(72) Inventor: **Eric M. Delangis**, Huntsville, AL (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.

(21) Appl. No.: **15/161,787**

(22) Filed: **May 23, 2016**

(65) **Prior Publication Data**

US 2016/0269547 A1 Sep. 15, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/512,414, filed on Oct. 11, 2014, now Pat. No. 9,350,649, which is a

(Continued)

(51) **Int. Cl.**

H04M 3/00	(2006.01)
H04L 12/707	(2013.01)
H04L 12/54	(2013.01)
H04W 40/02	(2009.01)
H04L 12/911	(2013.01)
H04W 88/16	(2009.01)
H04L 12/741	(2013.01)
H04L 29/12	(2006.01)
H04L 29/06	(2006.01)
H04M 1/60	(2006.01)

(Continued)

(52) **U.S. Cl.**

CPC ***H04M 3/007*** (2013.01); ***H04L 12/5692*** (2013.01); ***H04L 45/24*** (2013.01); ***H04L 45/54*** (2013.01); ***H04L 47/821*** (2013.01); ***H04L 61/2015*** (2013.01); ***H04L 69/168*** (2013.01); ***H04M 1/6033*** (2013.01); ***H04W 88/16*** (2013.01); *H04M 2203/052* (2013.01); *H04M 2203/60* (2013.01); *H04M 2250/06* (2013.01); *H04W 8/26* (2013.01); *H04W 28/06* (2013.01); *H04W 40/02* (2013.01); *H04W 72/04* (2013.01); *H04W 80/00* (2013.01); *H04W 84/12* (2013.01); *H04W 84/18* (2013.01); *Y02D 30/70* (2020.08)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,487,069 A 1/1996 O'Sullivan et al.
6,470,453 B1 * 10/2002 Vilhuber G06F 21/577 709/225

(Continued)

OTHER PUBLICATIONS

802.3 IEEE Standard for Information Technology, Part 3, Mar. 2002, starting at p. 232 "43. Link Aggregation."

(Continued)

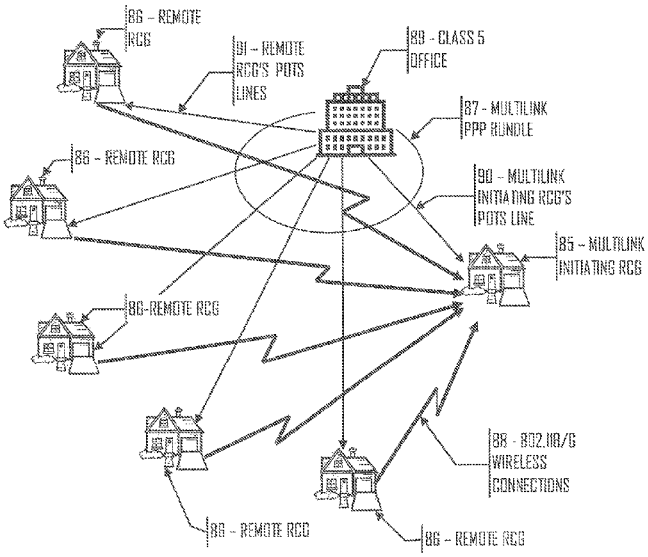
Primary Examiner — Hong S Cho

(74) *Attorney, Agent, or Firm* — Clay McGurk; The Law Office of Clay McGurk

(57) **ABSTRACT**

The broadband network-edge router is a broadband communications device that receives broadband packetized data and then wirelessly communicates to and from a router located in a typical residence or small business or other device. The broadband network-edge router can be for example, a Wi-Fi device or a cellular device or tower, and routes data to the data-requesting devices during multipath or multilink connections.

17 Claims, 9 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/531,294, filed on Jun. 22, 2012, now Pat. No. 8,861,349, which is a continuation of application No. 12/581,852, filed on Oct. 19, 2009, now Pat. No. 8,228,801, which is a continuation of application No. 10/686,375, filed on Oct. 14, 2003, now Pat. No. 7,606,156.

(60) Provisional application No. 60/418,521, filed on Oct. 15, 2002.

(51) **Int. Cl.**

H04W 8/26	(2009.01)
H04W 28/06	(2009.01)
H04W 72/04	(2009.01)
H04W 80/00	(2009.01)
H04W 84/12	(2009.01)
H04W 84/18	(2009.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,502,135	B1	12/2002	Munger et al.	
6,628,617	B1	9/2003	Karol et al.	
6,704,794	B1 *	3/2004	Kejriwal	H04L 29/06 370/392
6,775,235	B2	8/2004	Datta et al.	
7,406,048	B2	7/2008	Datta et al.	
2001/0007557	A1 *	7/2001	Yamada	H04L 45/00 370/389
2001/0036161	A1 *	11/2001	Eidenschink	H04B 7/18584 370/316
2002/0055982	A1 *	5/2002	Goddard	H04L 29/06 709/217
2002/0106065	A1 *	8/2002	Joyce	G06Q 20/00 379/114.02
2002/0150099	A1 *	10/2002	Pung	H04L 12/1886 370/390
2003/0016664	A1 *	1/2003	MeLampy	H04L 29/06027 370/389
2003/0135578	A1 *	7/2003	Banga	H04L 29/06 709/215
2003/0202468	A1 *	10/2003	Cain	H04L 45/00 370/229
2014/0122656	A1 *	5/2014	Baldwin	H04L 65/4084 709/219

OTHER PUBLICATIONS

Link Aggregation according to IEEE 802.3ad, by SysKonnect GmbH, 2002.

802.3 IEEE Standard for Information Technology, Part 3, Mar. 2002 (specifically, starting at p. 232 "43. Link Aggregation").

M-TCP: TCP for Mobile Cellular Network, Kevin Brown and Suresh Singh, University of South Carolina, 1997.

* cited by examiner

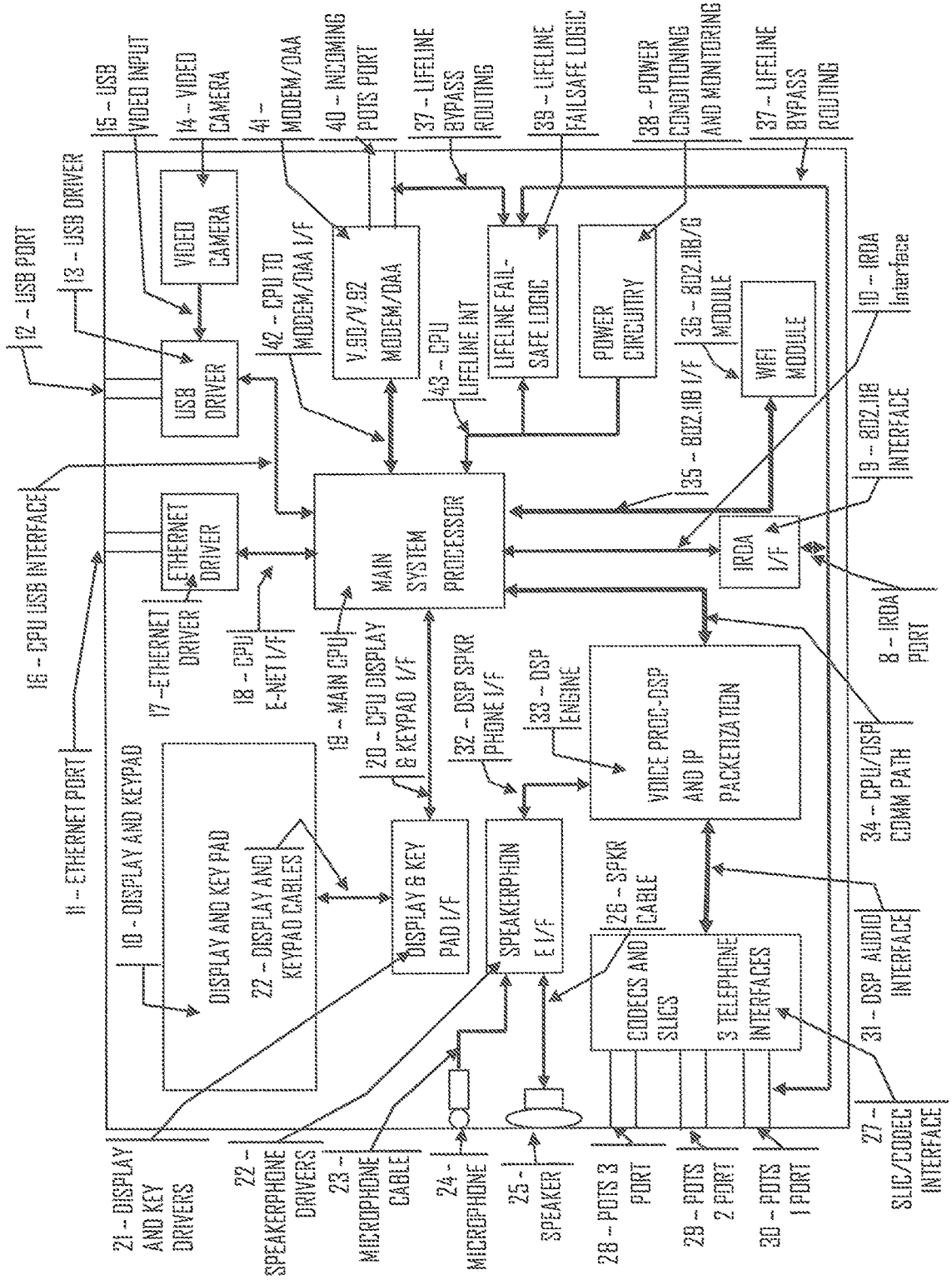

12 – USB PORT
13 – USB DRIVER
15 – USB VIDEO INPUT
14 – VIDEO CAMERA
41 – MODEM/DAA
40 – INCOMING POTS PORT
37 – LIFELINE BYPASS ROUTING
39 – LIFELINE FAILSAFE LOGIC
38 – POWER CONDITIONING AND MONITORING
37 – LIFELINE BYPASS ROUTING
VIDEO CAMERA
USB DRIVER
42 – CPU TO MODEM/DAA I/F
V.90/V.92 MODEM/DAA
43 – CPU LIFELINE INT
LIFELINE FAIL-SAFE LOGIC
POWER CIRCUITRY
36 – 802.11B/G MODULE
WIFI MODULE
10 – IRDA interface
35 – 802.11B I/F
9 – 802.11B INTERFACE
16 – CPU USB INTERFACE
ETHERNET DRIVER
MAIN SYSTEM PROCESSOR
IRDA I/F
8 – IRDA PORT
17 – ETHERNET DRIVER
18 – CPU E-NET I/F
19 – MAIN CPU
20 – CPU DISPLAY & KEYPAD I/F
32 – DSP SPKR PHONE I/F
33 – DSP ENGINE
VOICE PROC-DSP AND IP PACKETIZATION
34 – CPU/DSP COMM PATH
11 – ETHERNET PORT
10 – DISPLAY AND KEYPAD
DISPLAY AND KEY PAD
22 – DISPLAY AND KEYPAD CABLES
DISPLAY & KEY PAD I/F
SPEAKERPHONE E I/F
26 – SPKR CABLE
CODECS AND SLICS
3 TELEPHONE INTERFACES
31 – DSP AUDIO INTERFACE
21 – DISPLAY AND KEY DRIVERS
22 – SPEAKERPHONE DRIVERS
23 – MICROPHONE CABLE
24 – MICROPHONE
25 – SPEAKER
28 – POTS 3 PORT
29 – POTS 2 PORT
30 – POTS 1 PORT
27 – SLIC/CODEC INTERFACE

FIG. 1

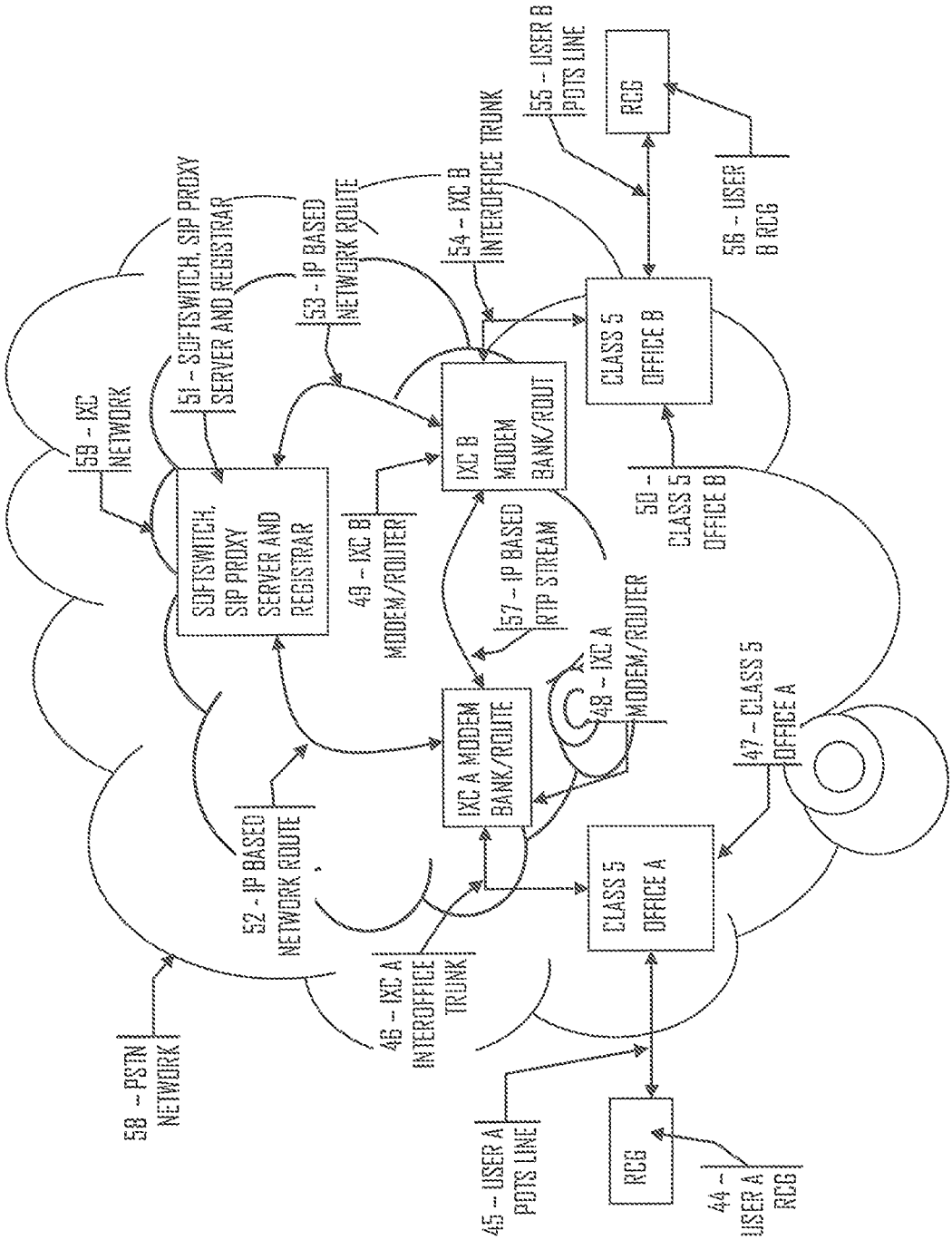

59 – IXC NETWORK
51 – SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
53 – IP BASED NETWORK ROUTE
54 – IXC B INTEROFFICE TRUNK
55 – USER B POTS LINE
RCB
56 – USER B RCB
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
49 – IXC B MODEM/ROUTER
IXC B MODEM BANK/ROUT
CLASS 5 OFFICE B
50 – CLASS 5 OFFICE B
57 – IP BASED RTP STREAM
48 – IXC A MODEM/ROUTER
IXC A MODEM BANK/ROUTE
47 – CLASS 5 OFFICE A
52 – IP BASED NETWORK ROUTE
CLASS 5 OFFICE A
46 – IXC A INTEROFFICE TRUNK
58 – PSTN NETWORK
45 – USER A POTS LINE
RCB
44 – USER A RCB

FIG. 2

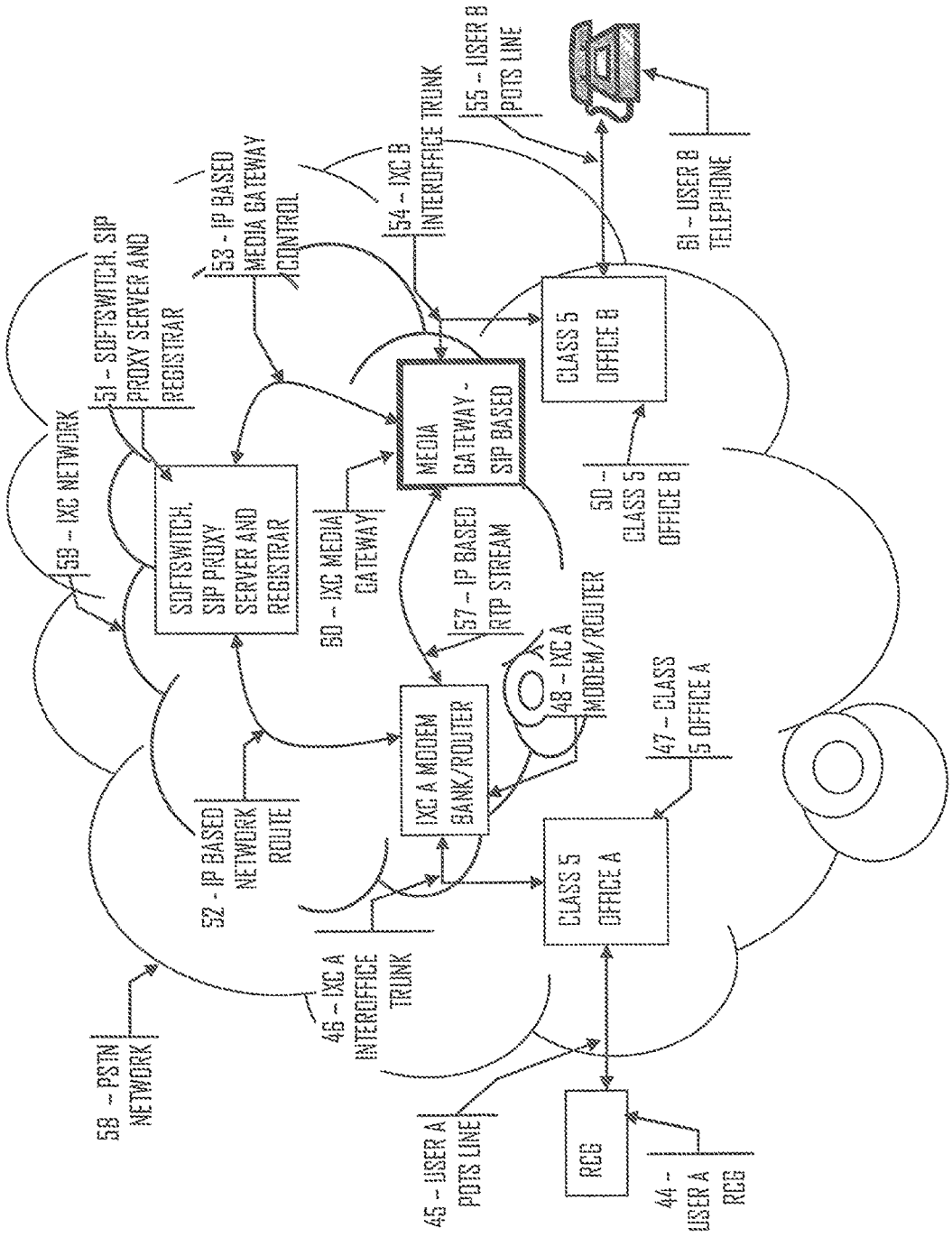

58 – PSTN NETWORK
56 – IXC NETWORK
51 – SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
53 - IP BASED MEDIA GATEWAY CONTROL
52 - IP BASED NETWORK ROUTE
SOFTSWITCH, SIP PROXY SERVER AND REGISTRAR
46 – IXC A INTEROFFICE TRUNK
50 – IXC MEDIA GATEWAY
IXC A MODEM BANK/ROUTER
MEDIA GATEWAY - SIP BASED
57 – IP BASED RTP STREAM
54 – IXC B INTEROFFICE TRUNK
48 – IXC A MODEM/ROUTER
CLASS 5 OFFICE A
CLASS 5 OFFICE B
55 – USER B POTS LINE
47 – CLASS 5 OFFICE A
50 – CLASS 5 OFFICE B
61 – USER B TELEPHONE
45 – USER A POTS LINE
RGB
44 – USER A RGB

FIG. 3

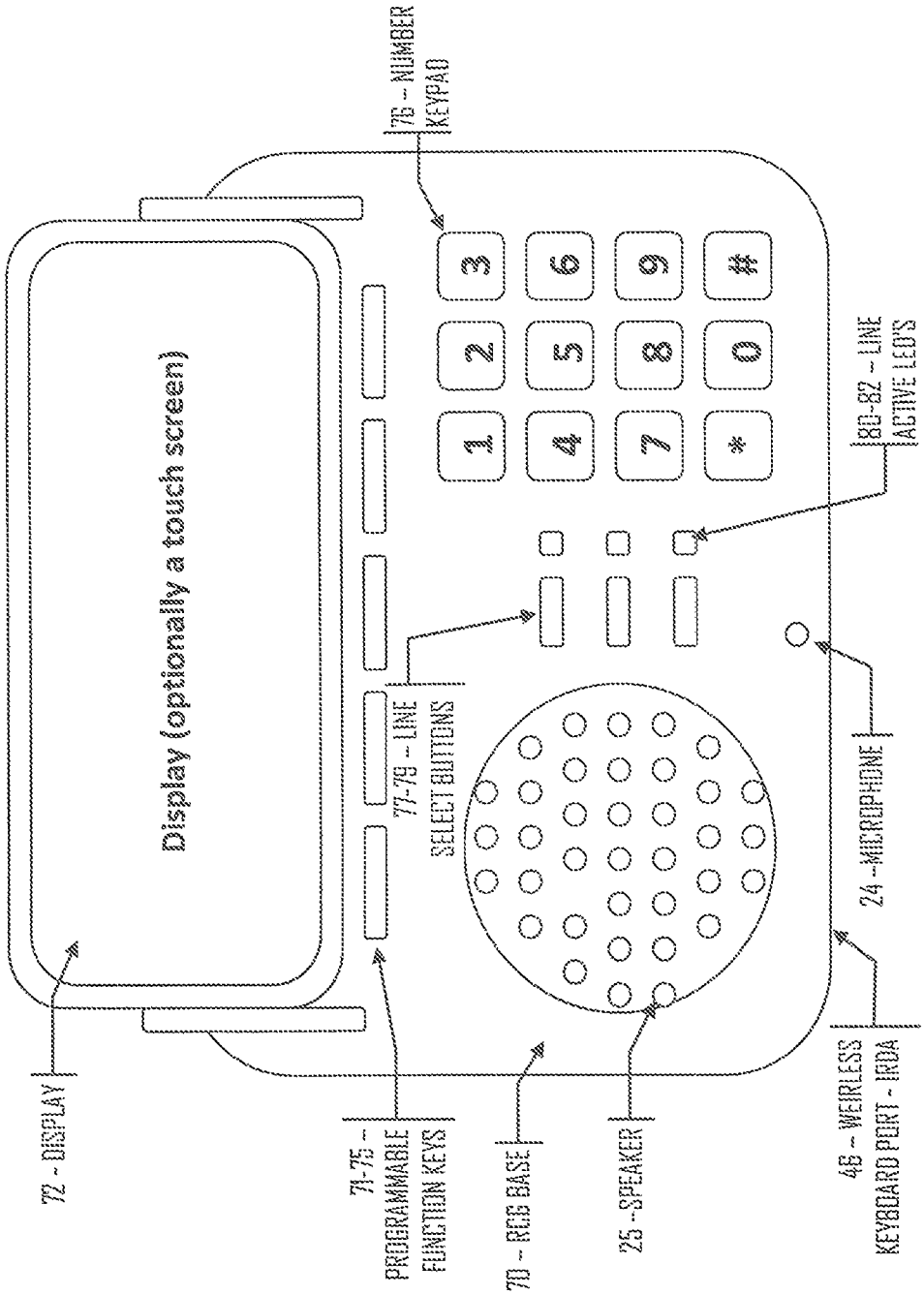

Display (optionally a touch screen)
1
2
3
4
5
6
7
8
9
*
0
#
76 – NUMBER KEYPAD
80-82 – LINE ACTIVE LED'S
77-79 – LINE SELECT BUTTONS
24 – MICROPHONE
72 – DISPLAY
71-75 – PROGRAMMABLE FUNCTION KEYS
70 – RCB BASE
25 – SPEAKER
46 – WEIRLESS KEYBOARD PORT – IRDA

FIG. 4

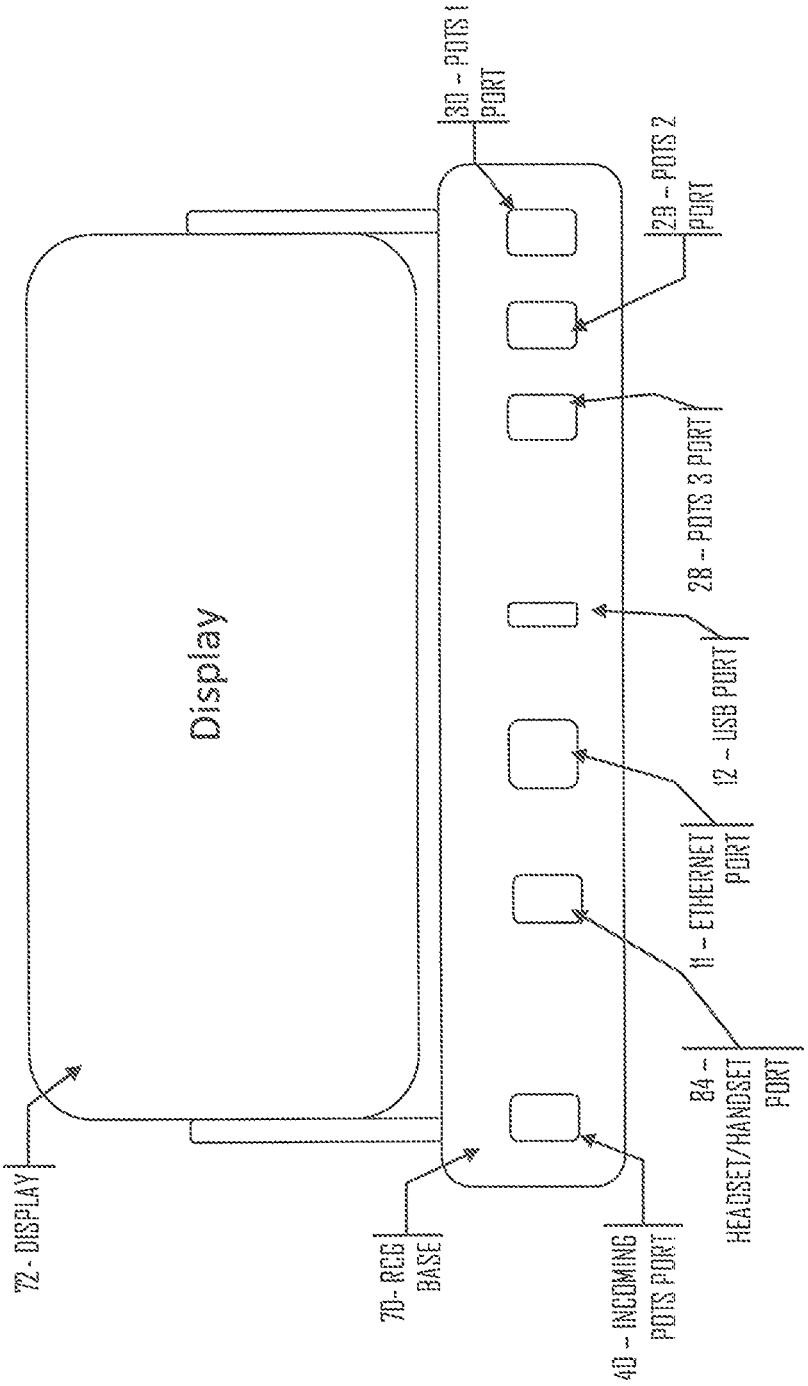

Display
72- DISPLAY
70- REG BASE
40 - INCOMING POTS PORT
84 - HEADSET/HANDSET PORT
11 - ETHERNET PORT
12 - USB PORT
28 - POTS 3 PORT
29 - POTS 2 PORT
30 - POTS 1 PORT

FIG. 5

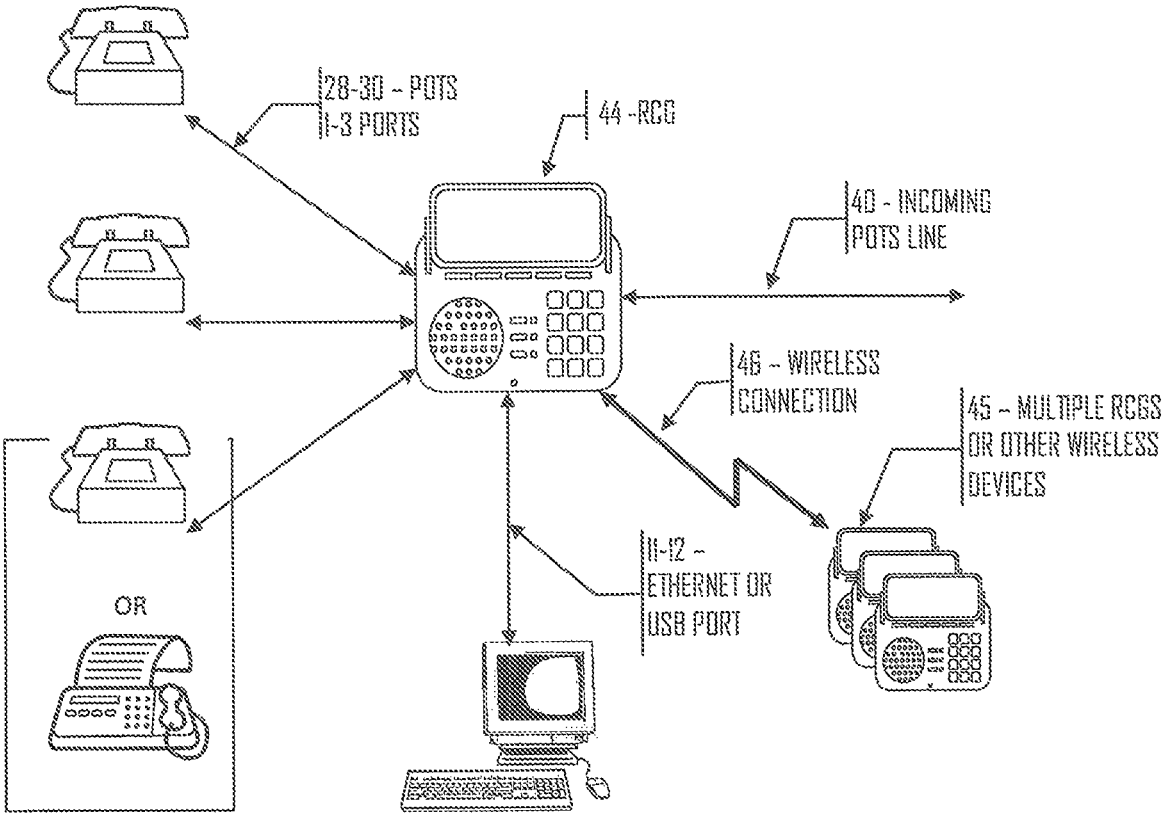

28-30 ~ POTS
1-3 PORTS
44 -RCG
40 - INCOMING
POTS LINE
46 ~ WIRELESS
CONNECTION
45 ~ MULTIPLE RCGS
OR OTHER WIRELESS
DEVICES
11-12 ~
ETHERNET OR
USB PORT
OR

FIG. 6

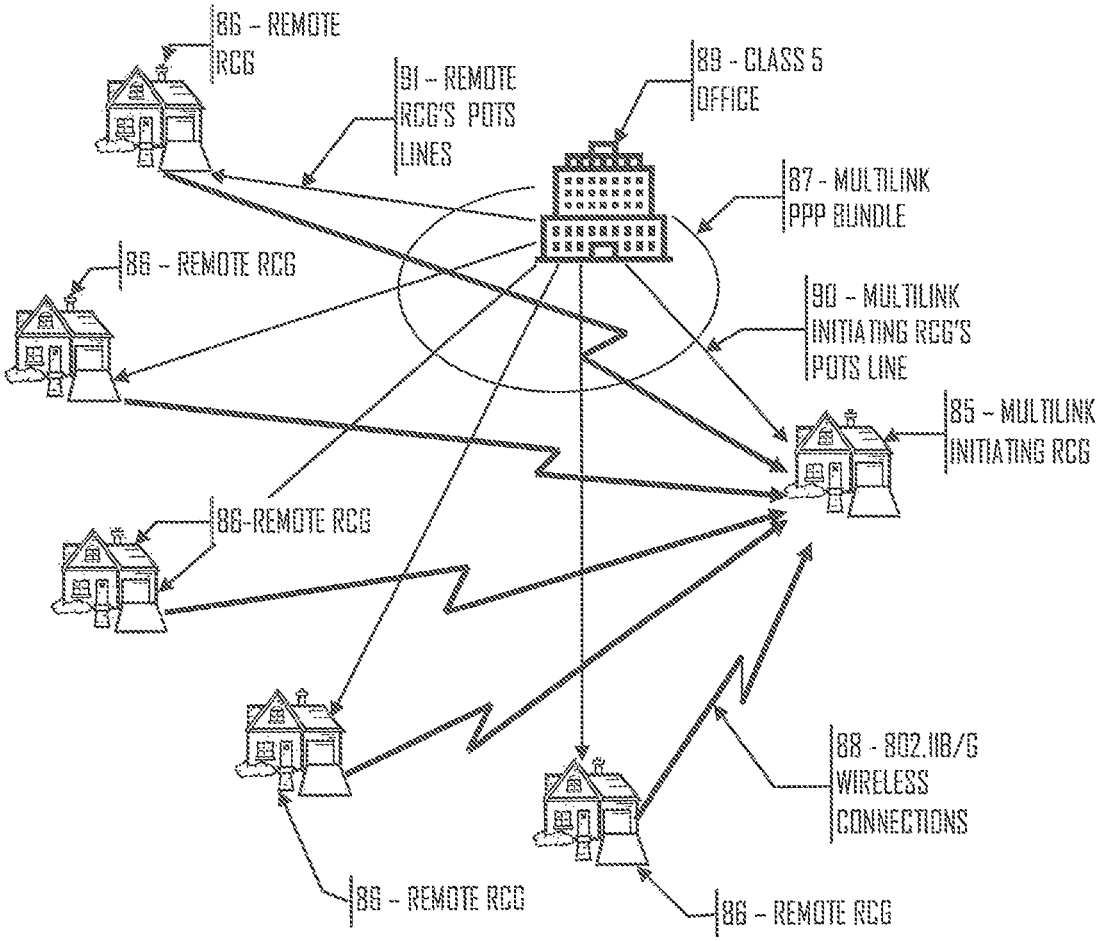

86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
85 – MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG

FIG. 7

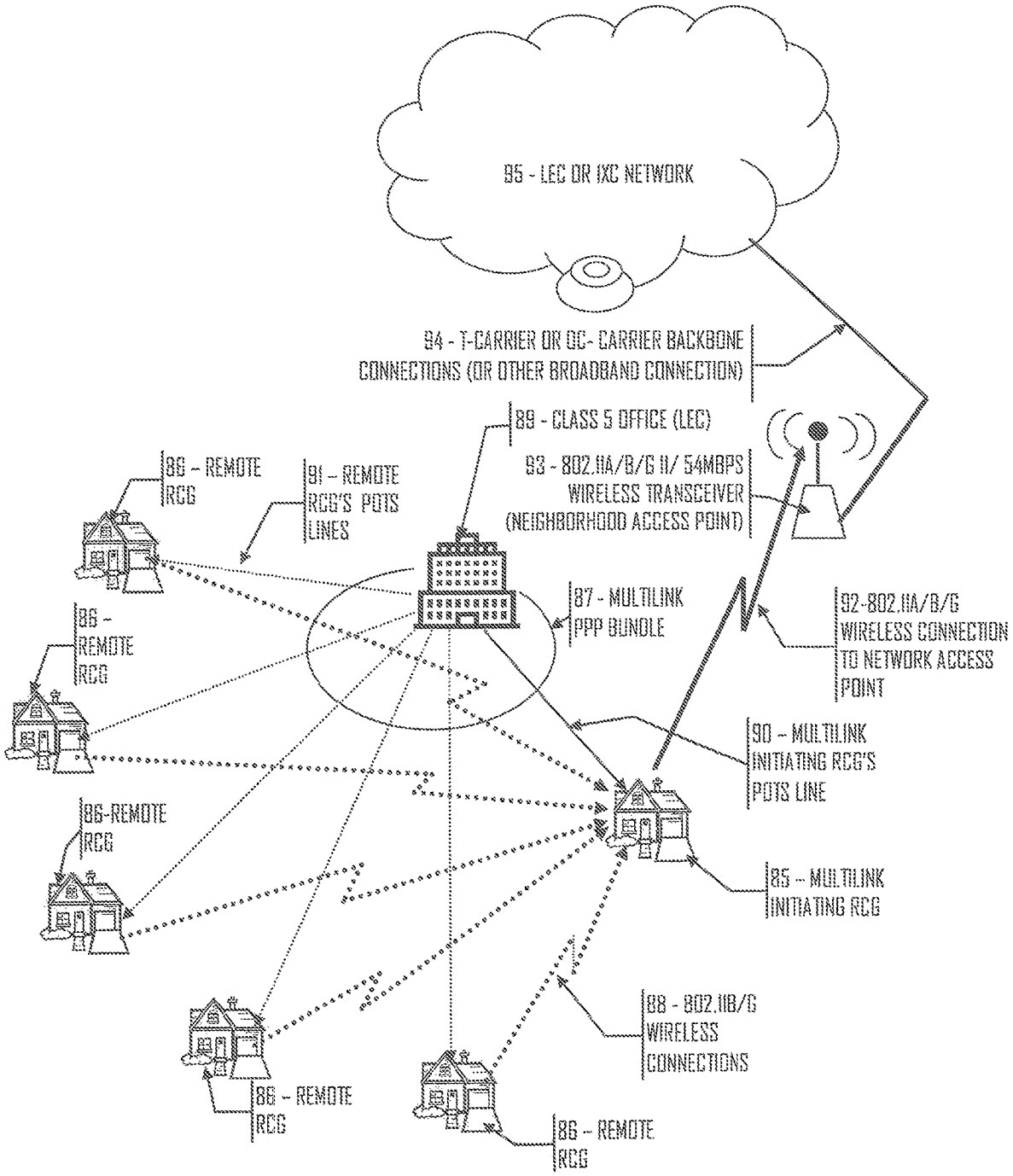

95 - LEC OR IXC NETWORK
94 - T-CARRIER OR OC- CARRIER BACKBONE CONNECTIONS (OR OTHER BROADBAND CONNECTION)
89 - CLASS 5 OFFICE (LEC)
93 - 802.11A/B/G II/ 54MBPS WIRELESS TRANSCEIVER (NEIGHBORHOOD ACCESS POINT)
86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
87 - MULTILINK PPP BUNDLE
92-802.11A/B/G WIRELESS CONNECTION TO NETWORK ACCESS POINT
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
86-REMOTE RCG
85 – MULTILINK INITIATING RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG

FIG. 8

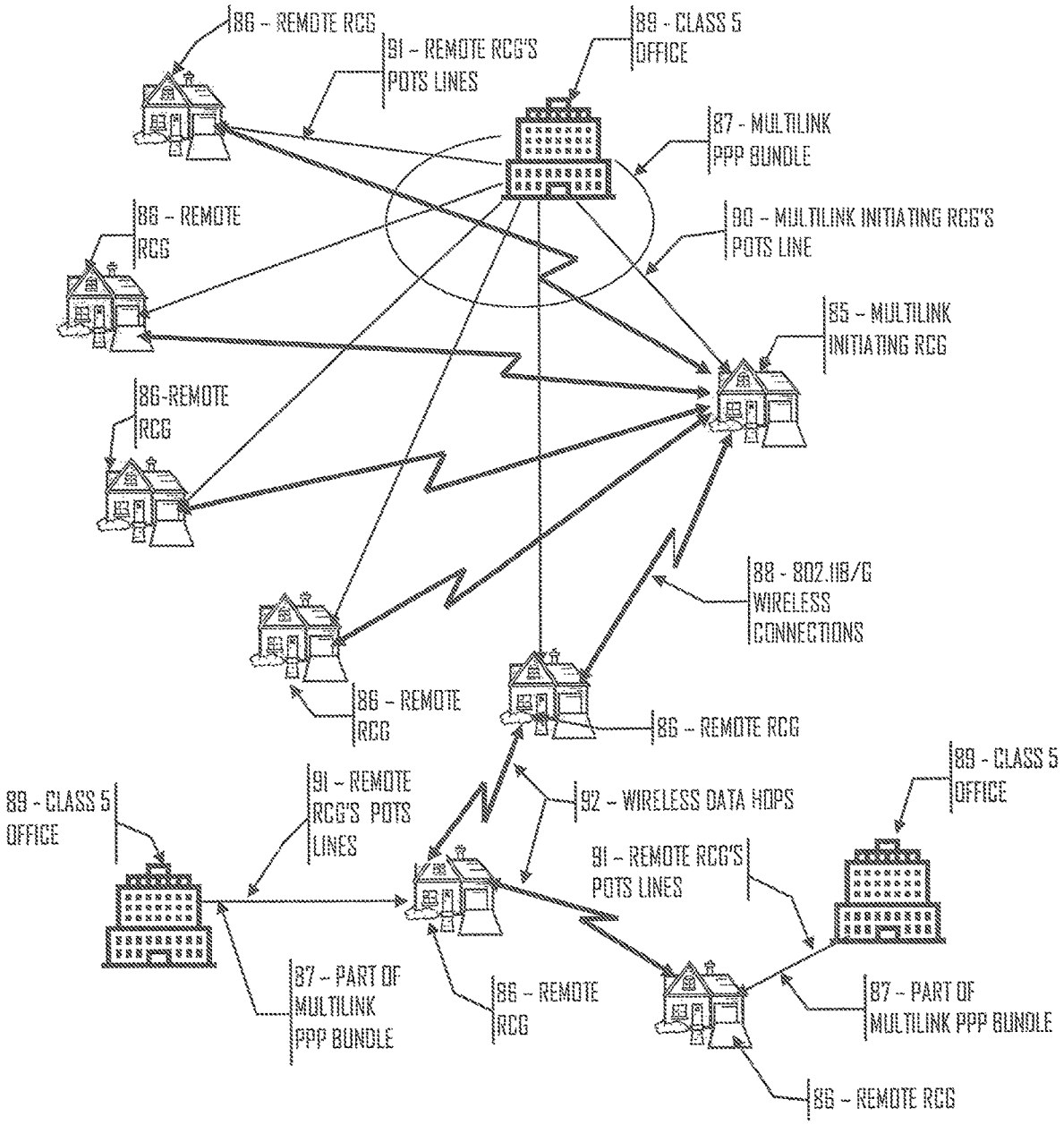

86 – REMOTE RCG
91 – REMOTE RCG'S POTS LINES
89 - CLASS 5 OFFICE
87 - MULTILINK PPP BUNDLE
86 – REMOTE RCG
90 – MULTILINK INITIATING RCG'S POTS LINE
85 – MULTILINK INITIATING RCG
86-REMOTE RCG
88 - 802.11B/G WIRELESS CONNECTIONS
86 – REMOTE RCG
86 – REMOTE RCG
89 - CLASS 5 OFFICE
91 – REMOTE RCG'S POTS LINES
92 – WIRELESS DATA HOPS
89 - CLASS 5 OFFICE
91 – REMOTE RCG'S POTS LINES
87 – PART OF MULTILINK PPP BUNDLE
86 – REMOTE RCG
87 – PART OF MULTILINK PPP BUNDLE
86 – REMOTE RCG

FIG. 9

DEVICES AND METHODS FOR MULTIPATH COMMUNICATIONS

RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 14/512,414 filed Oct. 11, 2014, now patented as U.S. Pat. 9,350,649, which is a continuation of U.S. patent application Ser. No. 13/531,294 filed Jun. 12, 2012, now patented as U.S. Pat. No. 8,861,349, which is a continuation of U.S. patent application Ser. No. 12/581,852 filed Oct. 19, 2009, now patented as U.S. Pat. No. 8,228,801, which is a continuation of U.S. patent application Ser. No. 10/686,375 filed Oct. 14, 2003, now patented as U.S. Pat. No. 7,606,156, which claims priority to U.S. Provisional Application Ser. No. 60/418,521, filed Oct. 15, 2002, all of which are incorporated by reference herein.

BACKGROUND OF INVENTION

The primary function of the RCG is to provide a platform for Competitive Local Exchange Companies (CLECs) to compete with the Local Exchange Companies (LECs) for residential voice and data services. The LECs have a strangle hold on the "last mile" of copper over which almost all residential customers receive their communications services. Today, most CLECs resell the existing services that are offered by the LECs. CLECs make their money by purchasing these services from the LECs at a discount and marking them up to the customer. Since these services are regulated and controlled by the Public Utilities Commission (PUC) the pricing for these services to the CLECs is set. The monthly CLEC discount is approximately $5 to $6 per line per month for basic rate services. This means, in practicality, that a CLEC can only charge an additional $5 or $6 to the residential customer for basic rate services otherwise they would be more expensive than the LEC, and no one would buy the services from them; telephone customers would simply stay with the LEC.

To be competitive then, CLECs try to sell additional services such as call waiting, caller ID, etc. where they have as much as a 50% margin. Some CLECs also bundle long distance services with their packages as additional incentive to get residential customers to buy local telephone service from them. Since long distance fees are as low as pennies per minute to the customer, there is little profit in long distance for the CLECs. As it is, the pricing structure is such that the LECs will stay in control of the residential market, and the CLECs are nothing more than a marketing arm of the LEC. This structure also keeps the CLECs at an equal competitive advantage, or disadvantage, with respect to each other. The only thing that one CLEC could do to gain more customers is to be a better marketer. Since the CLECs are unable to discount their services because their margins are too slim as it is, the net effect is that the consumer looses by not really getting competition in the residential markets, and prices are kept artificially high.

For the CLECs to be truly competitive in the local telecommunications markets, they must be able to do more than simply resell the LECs services. CLECs must be able to offer many more features or services than those that the LEC provides, and they must be able to do this at a lower cost, in order to attract new customers.

So, what new services can the CLECs offer? As things stand today there are none, with the exception of DSL or Cable services which require tremendous infrastructure costs on behalf of the CLEC. However, by deploying an

RCG in a residence, CLECs can offer advanced new calling features and services over the existing POTS line. Their costs for the POTS line from the LEC remains the same, but they can now charge for high bandwidth data services as well as additional calling and messaging features that the LECs cannot offer. This is their competitive advantage.

Competition:

Many companies are currently trying to provide VoIP services to residential customers over high-speed or broadband backbones such as DSL and cable modems, over Internet connections via a computer. The high-speed services require expensive infrastructure enhancements to the local telephone companies' facilities and cable plants, as well as expensive modems at the customer's end. These services are also difficult to deploy and too complicated for the average user. Internet based VoIP services suffer from Internet delays caused by a lack of true Quality of Service (QOS) capabilities across the Internet. Existing VoIP services also require access to a computer and a technical knowledge to be able to make it work. Because of these problems, VoIP services are primarily targeted at the corporate market place where private IP networks that can carry VoIP services with a true guaranteed QOS exist, or can be controlled.

The only available alternatives for the residential user for high speed services are DSL and cable modems. DSL and Cable based communications reach only a small segment of the population, and growth has failed to live up to initial expectations. The recent collapse of the internet boom has led to the failure of many DSL service providers and has effectively eliminated DSL as a potential service for most POTS users for the immediate future.

SUMMARY OF THE INVENTION

The RCG combines the capabilities and features of IP routers, Class 5 circuit switches and wireless LANs in a small stand-alone external modem like device. Additional capabilities for a hands-free speakerphone device with a large touch display are also detailed. The RCG can employ a large display with sufficient resolution to provide a functional user interface to access all of the advanced features offered by the RCG, but also to be able to provide video telephone services.

The device is placed in a residence and connected to the primary POTS line coming from the LEC. Up to three standard telephones or FAX machines (or any combination) are typically connected into the RCG. It also has a Universal Serial Bus (USB) and/or a 10-100 Ethernet interface for connection to a computer or a Local Area Network (LAN). In addition, it has an 802.11b/g wireless interface for wireless home networking as well as broadband-to-the-home services.

The system is installed in a customer's home by simply plugging it into the existing incoming telephone line that provides POTS services from the LEC. One or more standard telephones are then plugged into its three line-output jacks. This is the simplest and most basic usage. In this implementation, the user only is interested in gaining additional telephone lines into the household. No computer connection is required in order to use the system. However, if data communications are desired, then there are three additional interfaces for computer connectivity. Typically either an Ethernet port, USB port or firewire (IEEE 1394) port is used to connect to a PC or LAN. The 802.11b/g interface is for wireless communications between the RCG and PCs, other RCGs as well as any other types of compat-

ible wireless devices. A version of the RCG includes a speakerphone and video camera to provided for video telephone services.

Services provided by the RCG:

The following discussion refers to FIG. **1**. The RCG has a main system processor that is responsible for all house keeping and traffic routing tasks. The Main CPU **19** routes data to and from the Ethernet Port **11**, USB Port **12**, Modem/DAA **41**, DSP Engine **33**, 802.11b/g Module **36** and the Display and Keypad **10**.

The RCG provides a total telecommunications communications services package for residential and small business customers. With the RCG, a CLEC can offer its customers dialtone for up to three separate telephone numbers per residence (the limit of three telephone numbers is an arbitrary number based upon typical residential usage and is not a limit imposed by the system), all local and long distance services, 24/7 always-on Internet access, a host of custom messaging and calling features, as well as Broadband access and lifeline service. All of these services can be offered over a customer's existing POTS line, and it doesn't require any network infrastructure build out like DSL and Cable services. Because there is no expensive network equipment required, it can be readily deployed throughout the country to expand the CLECs customer base quickly.

The RCG is designed to enhance, not replace, the existing telephone line, enabling it to provide new combined packetized voice and data services. Meanwhile, all existing telecommunications infrastructure and equipment will continue to work seamlessly with the RCG. Aside from simply installing the low cost RCG device in the home telephone wiring, no other equipment needs to be purchased by either the home owner or telephone companies. This eliminates the tremendously expensive infrastructure costs for communications companies that are trying to provide voice services using DSL or cable modems.

The RCG VIP Home Gateway Features:

Up to three telephone lines i.e. numbers, over a single POTS line and/or wireless connection.

Ethernet, USB and IEEE 1394 computer interfaces.

Full G1, G2 and G3 FAX support.

Full support for all CLASS services.

Broadband networking for home computers and appliances as well as wide area networking using a combination of a plurality POTS lines connected to a plurality of RCGs and/or a direct wireless connection to a wireless access point. (These interfaces allow smart devices to communicate to other devices within the home, or over the Internet through the RCG.)

Automated, remote upgradability and configuration. (Requires the customer to do nothing.)

Transparent user operation. (User doesn't have to know that any new technology is being employed)

100% compatible with existing public telephone system.

Video Telephone capabilities.

No local or long distance usage charges.

No Internet access fees.

Lower monthly communication costs.

Multiple telephone calls at the same time.

Voice messaging, follow me features, call forwarding, automatic call back, conferencing, custom call routing. Home networking capabilities, all CLASS calling features, high speed broadband networking, continuous 24/7 internet access. and many others.

All of these features are available even while connected to the Internet.

Very low cost of entry into the market, especially as compared to broadband alternatives.

New calling features that are not currently available to home users.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows the RCG functional block diagram with the preferred embodiment of an 802.11 wireless connection.

FIG. **2** shows the network topology for native RCG to RCG communications.

FIG. **3** shows the network topology for an RCG to PSTN call.

FIG. **4** shows the RCG top view with associated functions.

FIG. **5** shows the RCG rear view and associated connections.

FIG. **6** shows a typical application with peripheral equipment connections.

FIG. **7** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity.

FIG. **8** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with connection to a broadband neighborhood access point (Wi-Fi hot spot).

FIG. **9** shows an ad-hoc wireless LAN configuration with ppp multilink data distribution and wireless connectivity with wireless data hopping with POTS connections through numerous different Class 5 offices.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment is detailed herein using the ubiquitous 802.11 wireless protocol. It is by no means insinuated that this is the only wireless scheme that can be used by this device; rather, it is intended that any wireless transmission scheme can be used for wireless communications between this device and other wireless devices as various applications may dictate.

System Initialization

Refer to FIGS. **1**, **2** and **3** for the following discussion. When the RCG is first plugged into an AC power outlet the Main CPU **19**, performs a Power-on Self Test (POST) routine. Once the POST completes and the RCG is connected to an active POTS line, connected to the LEC, by means of the Incoming POTS Port **40**, the RCG automatically initiates a modem connection via the Modem/DAA **41**, to a registration service via a toll free 800 telephone number. The registration service connects directly to the service provider's sales or customer service offices via a VoIP connection. An operator or an automated service answers the call and sets up a new account for the customer. Once the account is set up, the service provider's network automatically sends control information to the device to store the required routing and feature/service information in its non-volatile memory of its Main CPU **19**. As part of this information, a local dialup telephone number is sent to the device that it will use for local network access in the same fashion as a standard ISP connection is made from a home computer. The URL of the Softswitch/SIP Proxy Server and Registrar **51** that will be controlling this particular device is also stored at this time. During the service activation and configuration process, the customer service operator can send test requests to the device, as well as call into it on another telephone number (assuming an additional telephone number is part of the users class of service) or the

speakerphone to verify that it is configured and working properly. The final step of the configuration and initialization process is to register the device with the appropriate Softswitch/SIP Proxy Server and Registrar **51** so that the Softswitch/SIP Proxy Server and Registrar **51** knows that it is the controlling SIP Proxy for this RCG. Also configured at this time is the username/password verification server (this is a standard network device and is not shown) that is used to allow the RCG's modem to make a connection onto the service provider's network. Once the RCG configuration is completed, it disconnects the call by hanging up the Modem/DAA **41**, then dials the new local network access number that had been sent during the configuration process and establishes a constant local network connection. This connection is maintained continuously on a 24/7 basis, and is immediately reestablished whenever it drops. Should the RCG become unable to reestablish this connection after several tries, it will switch over to failsafe mode and inform the user via the Display and Keypad **10**. The RCG will try to reestablish the connection every few minutes until it finally succeeds.

By default, the first telephone port, POTS **1** Port **30**, is assigned as the termination port for the existing POTS service that is connected to Incoming POTS Port **40**. This is the existing telephone service that the user already has as his primary telephone service from his LEC. POTS **1** Port **30**, typically has connected to it a standard telephone set that does not require any power (other than that derived over the POTS interface) to operate properly. POTS **1** Port **30** is the Lifeline telephone port for the user. In the case that all power is lost to the RCG, POTS **1** Port **30** will fail to a direct connection to the Incoming POTS Port **40** telephone line that comes into the RCG from the LEC to provide uninterrupted telephone services to the user. In this state, however, none of the enhanced VoIP services of the RCG are available to the user since the user simply has a stand POTS telephone service to the LEC.

Two additional and unique telephone numbers can be assigned to the other two telephone ports, POTS **2** Port **29** and POTS **3** Port **28**, by the service provider at any time. These numbers are drawn from a pool of available telephone numbers assigned to the service provider. POTS **2** Port **29** and POTS **3** Port **28** must to have standard telephone numbers assigned to them so that the PSTN is able to route calls from its network to these ports. For calls originating from IP based telephones, these numbers are not necessarily needed since POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** are uniquely identifiable to IP networks via their IP addresses assigned through the Dynamic Host Configuration Protocol (DHCP) at the time that the RCG establishes a connection to the service provider's network. Since POTS **2** Port **29** and POTS **3** Port **28** must have a telephone number assigned to them, it is a matter of convenience to use the assigned telephone numbers as part of their SIP address for IP routing of their data. In this way, all three user POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** are all addressed the same manor.

At this point, the user is able to take advantage of all of the RCG's features that have been activated according to his service agreement. The user can at any time connect additional telephones, a computer or a computer network to the RCG. The user will only be able to use those telephone ports (POTS **1** Port **30**, POTS **2** Port **29** or POTS **3** Port **28**) that have been activated, and assigned unique telephone numbers by the service provider. Any type of standard telephone can be connected to the three POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28**. In the event that a cordless telephone or a telephone that derives its power from an AC outlet is connected to POTS **1** Port **30**, the lifeline functionality of this port will be ineffective since the telephone itself will not operate once power is lost.

The speaker phone feature of the RCG, comprised of Speakerphone Drivers **22**, Microphone **24**, Speaker **25** and DSP Engine **33**, can be used on any of the activated telephone numbers and is by default enabled to operate on POTS **1** Port **30**. Once either of the other two telephone ports, POTS **2** Port **29** or POTS **3** Port **28**, is activated, the speakerphone function is activated for those lines as well. To use the speakerphone for any assigned telephone number, the user simply presses either the Line Select Button **79-81** for Line **1**, Line**2** or Line **3** on the face of the RCG, and the speakerphone function is activated on that line. This is convenient for answering any call directly at the RCG. The RCG may or may not have a number keypad for originating calls. This feature may be added or removed based upon the target market price points.

The determination as to which Inter Exchange Carrier (IXC) the RCG will route its data through is determined by any of a number of criteria including, but not limited to, whether the RCG is a private labeled product, or which carrier has the lowest cost routing, or if a specific carrier is specified by the customer, or and number of other considerations. The RCG can be programmed to change its routing path to any IXC at any time by the service provider. Complicated routing algorithms can be programmed into the RCG to control which IXC it will use at any time.

Failsafe Mode

During any time that the RCG is in failsafe mode i.e. Lifeline failsafe logic **39** is activated, the RCG will only be able to receive or initiate telephone calls via the telephone connected to its primary telephone port, POTS **1** Port **30** or through its speakerphone feature. In this condition, all activated telephone numbers are ported via the PSTN to the primary (first) telephone number for delivery to the user's telephone that is connected to POTS **1** Port **30**. While in failsafe mode, the modem is not activated, and the RCG appears to the local Class 5 office as a standard telephone, and the PSTN will route all incoming calls to the RCG as it normally would to any standard telephone.

Call Flow **1**:

Dialed call origination from a telephone connected to an RCG POTS port and terminating at another user's RCG POTS port:

When a user picks up a telephone connected to any of the three POTS ports, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28**, an off hook condition is detected by the SLIC/CODEC Interface **27** that is connected to the DSP Engine **33** by way of the DSP Audio Interface **31**. The DSP Engine **33** responds by sending digitally generated dialtone to the appropriate POTS interface over the DSP Audio Interface **31**. (Note: all BORSCHT telephony functions are performed by the DSP Engine **33** and the SLIC/CODEC Interface **27**.) Upon hearing the dialtone, the user enters the desired telephone number on his telephone keypad. The Dual Tone Multi-Frequency (DTMF) digits that the user dials are decoded within the DSP Engine **33**. The dialed digits are transferred to the Main CPU **19** via the CPU/DSP Communications Path **34**. The Main CPU **19** polls the DSP Engine **33** approximately every two milliseconds looking for data. The Main CPU **19** polling rate varies according to the process that is being performed. The CPU/DSP Communications path **34** also can generate an interrupt to force data transfer between it and the Main CPU **19**.

The Main CPU **19** generates a SIP Invite IP packet using the dialed digits as the called destination address and the URL of its local controlling SIP Proxy Server which was programmed into the RCG during the configuration process. The Main CPU **19** passes this SIP packet off to the Modem/DAA **41** for transmission over the network. The RCG Modem/DAA **41** is connected to and communicating with a modem in a modem bank located in the Inter Exchange Carrier's (IXCs) facility. This facility may actually be located in the LEC's physical plant or it may be physically located at another location.

Referring to FIG. **2**, User A RCG **44** is connected via its modem to the LEC's local Class 5 Office A **47**. In this example, the service provider's connections to the IXC A Modem Bank & Router **48** are through IXC A Inter-Office Trunks **46**. The service provider may or may not be the IXC. If the service provider does not have its own network, then it will purchase capacity from an IXC and route its traffic to that IXC's facilities. The SIP Invite IP Packet that is sent from User A RCG **44** transits the LEC's Class 5 Office A **47** facilities and is routed to the IXC A Modem Bank/Router **48** via the IXC A Inter-Office Trunks **46**. It is the job of the router to take the IP packet and route it on to its intended destination, in this case the appropriate SIP proxy server **51**. The router uses the URL for the Softswitch/SIP Proxy Server and Registrar **51** contained in the SIP Invite to know where to route the packet. (Note: The Softswitch, SIP Proxy Server and Registrar are logical devices that may reside in a single computer system, or may be implemented as completely separate devices. In this example, the Softswitch, SIP Proxy Server and Registrar are all shown as a single physical device running these three separate processes.) The IXC A Modem Bank/Router **48** sends the SIP Invite IP packet on to Softswitch/SIP Proxy Server and Registrar **51** via an IP based network route **52**.

The SIP Proxy Server process running on Softswitch/SIP Proxy Server and Registrar **51** performs a look up to determine the termination destination for the call using the dialed digits passed along in the SIP Invite IP packet. In this example, the terminating device for User B RCG **56** is via IXC B's Modem Bank/Router **49** then through Class 5 Office B **50** and over User B POTS line **55** and finally to User B RCG **56**. Not covered in detail here is the SIP message handling since it is completely covered in IETF RFC2543. This example shows that both the originating and terminating ends of this call are controlled by the same Softswitch/SIP Proxy Server and Registrar **51** device. Where the originating and terminating ends of a call are controlled by different Softswitch/SIP Proxy Server and Registrar devices, an additional level of SIP messaging is used between the two SIP Proxy Server processes of each of the Softswitch/SIP Proxy Server and Registrar devices to locate and control the terminating location of the call. Again, that information is covered in IETF RFC2543 and is repeated here.

After the call routing is setup using SIP, and User B answers the call, the Softswitch/SIP Proxy Server and Registrar **51** device sends IP address of the originating User A RCG **44** to the User B RCG **56** and the IP address of User B RCG **56** to User A RCG **44**. Once both RCG's have the other's IP address, they then communicate directly to each other using Real Time Protocol (RTP), and the Softswitch/SIP Proxy Server and Registrar **51** device is no longer part of the connection. This direct communication is shown as IP based RTP Stream **57** between IXC A Modem Bank/Router **48** and IXC B Modem Bank/Router **49**.

On the receiving end of the call, referring back to FIG. **2**, User B RCG **56** receives the SIP Invite data stream through its Modem/DAA **41** and passes it on to the Main CPU **19**. The Main CPU **19** reassembles the SIP IP packet and interrogates the header information to determine which POTS port, POTS **1** Port **30**, POTS **2** Port **29** and POTS **3** Port **28** the call is destined for based upon the dialed number contained in the SIP Invite message. The Main CPU **19** commands the DSP Engine **33** to control the SLIC/CODEC Interface **27** to apply ringing voltage to the selected POTS port to ring the phone. A corresponding SIP **180** (ringing) message is sent back to User A RCG **44** in the reverse direction. When the phone attached to the selected POTS port is answered, the off hook condition detected by the SLIC/CODEC Interface **27** is sent through the DSP Engine **33** to the Main CPU **19** that sends the SIP **200** OK message back to User A RCG **44** to let the RCG know that the call was answered by User B RCG **56** and to turn off the audible ringing tone for User B. Once the call is established, User A RCG **44** sends and ACK F12 SIP message to User B RCG **56** indicating that User A RCG **44** understands that the call setup has been completed.

The two RCGs now exchange SIP messages that include the type of voice encoding that will be used such as G.729, G.723.1, G.711 etc to configure their RTP streams so that they can reliably transfer the user information between them. At this point the call (voice data) is sent between both RCGs and a normal telephone conversation takes place between the user A and user B.

Call teardown is accomplished by either user hanging up their telephone. The RCG of the terminating end (the end that hangs up the phone first) detects the on-hook condition and sends a SIP Bye message to the other end. The other end upon receiving the SIP Bye message responds with an OK **200** SIP message and disables the appropriate POTS port that the user was using.

The Speakerphone interface can be used for either end of a telephone conversation in exactly the same way as described above except that the corresponding POTS port that the call was intended for is disabled if the call is answered via the speakerphone.

Call Flow **2**:

Calls between an RCG device and a PSTN telephone:

Refer to FIG. **3** for the following discussion.

In the previous call example, the PSTN network had nothing to do since the call was over a previously established modem connection between two RCGs. In the cases where a call originates or terminates to a standard telephone serviced by a Class 5 office, the process is a bit more complicated.

When a call originates from a user via an RCG, such as User A RCG **44**, the call handling practices are exactly the same up to the point that the SIP Proxy Server process in the Softswitch, SIP Proxy Server and Registrar **51** performs a lookup to determine how to route the call. In this case, the SIP Proxy Server process determines that the call terminates at a standard PSTN telephone attached to the Class 5 Office B **50**. Since the call originates as a native VoIP service, it must be converted to a standard switched circuit based service to be able to be delivered to User B's telephone **61**. The conversion is performed by the IXC's Media Gateway **60** device. In this example, the SIP Proxy Server process routes the call via the IXC's Media Gateway **60** device instead of through the IXC B Modem Bank/Router **49** as before. The SIP Proxy Server process sends a SIP Invite to the IXC's Media Gateway **60** device, as well as other control information, to direct the Media Gateway **60** device to

terminate the call and to apply the appropriate voice compression algorithm to the media stream to convert it between switched circuit PCM format and the selected VoIP protocol. At the same time, the Softswitch process of the Softswitch, SIP Proxy Server and Registrar **51** device sends commands to the Media Gateway **60** device to cause it to route the call's PCM data to a specific channel on the IXC B Interoffice Trunk **54**. The Softswitch process then generates an SS7 ISUP message that is sent over the PSTN SS7 signaling network to the Class 5 Office B informing it of the incoming call and on which circuit the call has been placed. It is up to the PSTN at this point to ring the User B telephone **61** and process the call between the IXC's Media Gateway and the User B Telephone **61**. The Softswitch process handles the signaling conversion between the PSTN's SS7 network and the IXC's SIP messaging, as well as any other proprietary signaling schemes utilized by the IXC to control its network. The standard SS7 call control messages, such as ringing, busy, ring back etc., all have a comparable SIP call flow control messages. The Softswitch simply maps the SS7 messages into SIP messages and visa-versa while routing the messages to the appropriate network equipment.

As in the case of a call between two RCGs, the RTP media stream (the actual call data) is routed directly be the IXC A Modem Bank/Router **48** and the IXC's Media Gateway **60** via an IP based RTP Stream **57**.

Again, call teardown is accomplished by either user hanging up their telephone. Depending which end hangs up the phone first, the associated network will generate the appropriate messages which will eventually make it back to the Softswitch process. The Softswitch process will relay the appropriate call control messages between the PSTN and the IXC's SIP based control system.

A telephone call originating from a PSTN telephone is configured and setup in the same fashion as the above description except that the originating messaging begins within the PSTN network instead of the IXC's network.

Personal Computer Based Communications:

Where the RCG is connected to a Personal Computer (PC) through either its USB Port **11** or Ethernet Port **12**, the RCG operates exactly as a cable or DSL type modem device. The RCG is simply a pass through for the computer's data. The RCG receives the IP packets (of whatever type) from the computer and sends the information unchanged to the Modem/DAA **41** interface for transmission over the Internet. Received information from the Internet is processed in the reverse way.

Dynamic Bandwidth Allocation:

When a modem connection is established between the RCG and the "Network", the total available bandwidth of this connection is used in a shared/prioritized fashion. Voice services (calls) take precedence over data services. Therefore, when no calls are in progress all of the available bandwidth is used by data type services such as surfing the Internet or uploading/downloading files. However, when a call is to be passed through the RCG, the required bandwidth for the call is deallocated from the data services and prioritized for the telephone call. This necessary because the Quality Of Service (QOS) is important for effective communications over electronic networks. Since the voice data is carried over a "data centric" network topology (an IP based network), call quality can suffer greatly. Every effort must be taken to eliminate or reduce the packet delay through every network element to be able to provide the best call quality. For data applications such as surfing the Internet or downloading files packet delay is acceptable and expected, and it does not affect the "quality" of the data.

Since all voice and data is transmitted as packets, there are no "time slots" or other type of "channelization" associated with the transmission of this data over either the POTS line or the wireless interface. Channelization of the voice data does occur within the SLIC/Codec Interface—**27** but is converted into IP packets by the DSP engine—**33** and is handled as packets from that point on.

Regardless of whether the call is originating or terminating at the RCG, the bandwidth allocation process is the same. When the SIP call setup messages are processed, the type of voice compression that will be used is defined. The RCG Main CPU **19** handles the IP packet flow between the DSP Engine **33**, USB Port **12**, Ethernet Port **11**, 802.11b/g Module **36** and the Modem/DAA **41** devices giving priority to the voice packets to and from the DSP Engine **33** and the Modem/DAA **41** interfaces. Voice compression algorithms create IP packets at a specified number of packets per second. These packets are handled by a timed process in the RCG. This process is started during call setup so that the packets are handled at the correct rate based upon the compression algorithm's packet generation rate. There is no priority assigned between the voice packets of each of the three different POTS Ports **28-30**. When more than one voice call is in progress, they are handled in a round robin fashion based upon the packet rate for the compression algorithm used. If, for example, two calls are using a compression scheme that generates packets every 2 milliseconds, and the third generates packets every 4 milliseconds, then the calls utilizing the faster packet rate will be polled at twice the rate as the call using a slower packet rate but they are not given priority "over" the other call. Only when there are no voice packets ready for transmission to the Modem/DAA **41**, i.e. during the approximately 2 to 4 millisecond packetization period between packets, will any pending data packets received from the USB Port **12**, Ethernet Port **11** or the 802.11b/g Module **36** be sent to the Modem/DAA **41** for transmission over the network.

Thus, the POTS bandwidth is allocated on a per packet basis, not on a "time slot" or "channelization" or even a "frequency" basis as it the case with T-Carrier, DSL or channelized DSL systems. The same is true for the wireless interface, whether it is carrying pure data or voice.

Security is currently a big concern in today's networks, and especially with wireless 802.11 transmissions. For this reason, the RCG defaults to route voice data over the users POTS connection via Incoming POTS Port **40**. As security concerns regarding wireless communications transmissions are addressed and alleviated, voice call data can, and will, be routed over the wireless interface via the 802.11 b/g Module **36**.

FAX Transmission:

Group I, **2** and **3** fax transmission is completely supported by the RCG. Fax transmission has the same priority as other voice communications. That is to say that FAX transmission is treated the same as a voice call and takes precedence over native IP data traffic.

Broadband Over POTS:

One of the primary functions of the RCG is to be able to transfer large files such as video files over the POTS lines to a residence. The ability to do this is limited by the maximum of 56 Kbps due to the design of the digital Class 5 office linecards and network transmission schemes based upon T carriers. Typical Class 5 linecard design samples the POTS lines at a rate of 8,000 samples per second. Typically, each sample is digitized into 12 to 16 bits by a codec device. The digitized sample is then companded to an 8 bit sample (1 byte) which makes up the PCM data stream that is trans-

ferred over the PSTN. Therefore, each POTS line is sampled at an effective rate of 64 Kbps. Since legacy T1 transmission equipment uses robbed-bit signaling, the maximum guaranteed transmission rate for the PSTN as a whole is 56 Kbps. Because of this limitation, standard POTS lines can only guarantee a maximum of 56 Kbps transfer rate under the best conditions. DSL equipment gets around this problem by installing DSL Access Multiplexing (DSLAM) equipment at the Class 5 office end of the POTS line. By routing around the linecard, as well as routing the data directly over the Internet or other private IP based networks, and therefore the 64 Kbps sampling rate, DSL is not bandwidth limited like PSTN traffic is. DSL, however, suffers from the very high costs associated with the purchase, installation, maintenance, floor lease costs, etc. DSL also suffers from very high deployment costs resulting from the labor intensive process to turn up each line. Each DSL "POTS" line must be inspected, conditioned and all load coils removed.

The RCG gets around the 56 Kbps POTS limitation as well as the DSL problems by using the standard POTS lines as they are, and not requiring any additional equipment to be installed at the Class 5 end of the POTS line. This technique simplifies deployment and drastically cuts costs.

Multilink PPP Connections:

Referring to FIG. **7**, the RCG implements broadband over POTS by employing an 802.11 b/g wireless interface to configure a multilink PPP bundle—**87** (per RFC 1990) comprised of the POTS lines connected to up to 32 RCGs. The limitation of 32 RCGs in a multilink PPP bundle is an arbitrary number and can be scaled up or down as required to support changes in network equipment capabilities. An 802.11b/g interface—**87** is shown as the preferred embodiment, since its 11/54 Mbps interface is considered sufficient bandwidth at this time also, its transmission distances are sufficient for implementation of this device, as opposed to other shorter ranged wireless transmission schemes. However as time goes on, some other wireless interface may be more desirable. There is nothing special or specific to the 802.11 wireless interface that makes it particularly suited to this application. Any wireless interface scheme can be used to implement this device.

The 802.11b/g interface—**88** on an individual RCG is also used to provide a peer-to-peer wireless home networking environment to other 802.11 compatible wireless component within the residence (such as a hand-held computer device) while acting as an always on dialup Internet gateway over the POTS line—**40** for the other wireless devices. An RCG that is transferring a very large file can request the services of 31 (in this embodiment) other RCGs to assist in the file transfer using their respective POTS lines. A single RCG can therefore gain the combined bandwidth of up to 32 POTS lines transferring data at as much as 56 Kbps each to transfer information. This is roughly equivalent to a transfer rate of 1.79 Mpbs in the inbound direction (towards the RCG) and approximately 1.075 Mbps in the outbound direction (towards the PSTN).

The multilink PPP connection—**87** is initiated by an RCG when it determines that the file (or streaming service) that it is to download (receive) is of sufficient size or requires a minimum amount of bandwidth to justify the use of a multilink PPP connection. This determination can be made on many different criteria such as the file size, type of data being transmitted, the type of compression if any, a Quality-of-Service requirement or any other pertinent information. (Since a certain amount of overhead is required to set up a Multilink PPP connection, it doesn't make sense to use it for small or low data rate transfers.)

Multilink PPP Bandwidth Allocation and Initialization:

Referring to FIG. **7**, an RCG—**85** that decides to initiate a multilink PPP session with a remote computer i.e. internet URL, requests a multilink PPP session with that URL resource via Link Control Protocol (LCP) session management. The initiating RCG—**85** and the remote server computer (not shown) will negotiate the pertinent multilink parameters such as compression, packet size, sync/async, link quality monitoring, bit stuffing etc. As part of a successful multilink PPP session setup, the initiating RCG—**85** receives a multilink PPP session ID, or "magic number", which is used to identify this particular multilink PPP session and is also used for adding or removing links from the multilink bundle—**87** . Once the multilink bundle is setup, the initiating RCG—**85** begins data transfer across its POTS interface—**90** with the far end computer system. The initiating RCG—**85** then looks up the addresses of up to 31 (in this embodiment) other RCGs in its router tables to use for the multilink PPP transfer. (If a Neighborhood Access Point is available the RCG could request service through it instead of setting up a Multilink PPP connection—see FIG. **8**.) The initiating RCG—**85** determines the number of remote RCGs—**86** that it wants to use to get the desired bandwidth for the transfer and sends multilink PPP service requests via the 802.11 b/g wireless connections—**88** to the selected remote RCGs—**86**. The selected remote RCGs—**86** respond back to the initiating RCG with either an acceptance or denial of multilink PPP service request. This decision is made based upon the remote RCG's currently available POTS bandwidth and the current local demands for that bandwidth. The remote RCG—**86** makes a decision to participate in a multilink PPP service for an initiating RCG if its POTS line—**91** has a current average bandwidth utilization of less than some arbitrary limit such as 8 Kbps to 16 Kbps. This 8 Kbps to 16 Kbps bandwidth utilization represents about two concurrent voice conversations using standard voice compression techniques, or some small amount of data transmission occurring on the remote RCG's POTS interface—**91** or a combination thereof. Assuming that the remote RCG—**86** has a modem connection speed somewhere between 33 Kbps to 56 Kbps, this would leave approximately 17 Kbps to 40 Kbps of POTS bandwidth that the remote RCG—**86** could offer to the initiating RCG—**85** for use in its multilink PPP bundle—**87**. Of course, if there is no activity on the remote RCG—**86** POTS line, then the entire bandwidth will be used for the multilink transfer. If the remote RCG—**86** accepts the multilink PPP service request from the initiating RCG—**85** it also sends its currently available bandwidth on its POTS line—**91** that the initiating RCG—**85** will have available to it for the multilink PPP transfers. The initiating RCG then selects which of the responding remote RCGs—**86** it will use for the multilink PPP bundle—**87** and sends them a multilink initialization packet containing the URL of the destination as well as the multilink PPP session ID (magic number) and any other pertinent information required for the remote RCG to join in the existing multilink PPP bundle—**87**. Each remote RCG POTS interface—**91** participating in a multilink PPP bundle, represents a logical "link" in the initiating RCG's multilink PPP bundle—**87**. The remote RCGs—**86** then send a multilink PPP packet (over their respective POTS lines—**91**) to the destination URL with the multilink PPP session ID and request to be added to that multilink PPP bundle—**87**. The destination URL accepts the request of each of the remote RCGs—**86** and begins sending data packets to each over their respective POTS lines—**91**. When the remote RCGs—**86** receive data packets sent over their respective POTS

lines—**91**, that are destined for the multilink PPP bundle—**87**, they simply relay the data packets over their 802.11b/g interface—**88** to the initiating RCG—**85**. It is the responsibility of the initiating RCG—**85** to perform all housekeeping tasks associated with the multilink transfer such as detection of lost packets and data packet reassembly, if those functions are required. Typically, lost packet detection and retransmission and reassembly are performed at higher OSI layers by the requesting software such as a browser. The remote RCGs—**86** are simply data transport nodes and do not perform any data processing on data received over a multilink PPP bundle destined for another RCG.

The initiating RCG—**85** of the multilink PPP bundle—**87** continually monitors the bandwidth of each remote RCG's—**86** multilink link which together comprise its multilink bundle—**87**. When the available bandwidth for the multilink PPP link of an individual remote RCG—**86** falls below an arbitrary minimum set by the initiating RCG—**85**, the initiating RCG—**85** instructs the offending remote RCG, via its 802.11b/g wireless interface—**88**, to remove itself from the multilink bundle. The remote RCG—**86** will then notify the remote computer (URL) to be removed as a link in the current multilink bundle on which it is participating. Alternatively, a remote RCG—**86** can inform the initiating RCG—**85** of local demands on its POTS bandwidth, and request that the initiating RCG—**85** remove it (the remote RCG—**86**) from the participation in the initiating RCG's multilink bundle—**87**. The remote RCG—**86** will not unilaterally remove itself from participation in a multilink bundle without prior notification to the Initiating RCG—**85**. The remote RCG—**86** must get authorization from the initiating RCG—**85** to remove itself from the bundle, since the initiating RCG—**85** will have no way of knowing if the loss of data from that remote RCG is due to some sort of failure or from the remote RCG simply removing itself from participation in the multilink bundle—**87**. Also, for services that require a minimum Quality of Service (QOS) such as streaming video, the initiating RCG—**85** needs to control the multilink bundle—**87** bandwidth, and it can not do that if remote RCGs—**86** drop out of the multilink bundle—**87** at will. When a remote RCG—**86** requests to be removed from participation in a multilink bundle—**87**, the initiating RCG—**85** must immediately grant the request. If the initiating RCG—**85** were to not grant the request, then the remote RCG—**86** could, in worst case, delay or drop incoming multilink packets destined for the initiating RCG—**85**. If this were to happen, the initiating RCG—**85** will have missing packets and could over run its reassembly buffer (if reassembly is being performed by the RCG) causing catastrophic data loss and potentially have to restart the entire transmission. In the least case, the initiating RCG—**85** would have to initiate retransmission of potentially many packets which it assumes to be lost, but may simply be delayed by the remote RCG—**86**. Once a remote RCG—**86** has been removed from participating in a multilink bundle—**87**, the initiating RCG—**85** will then look up another remote RCG in its router tables that can be used to participate in the multilink PPP bundle—**87**, and request that the new remote RCG—**86** to join the existing multilink bundle—**87**. This is necessary to maintain a minimum Quality of Service. Since RCGs prioritize their bandwidth requirements based upon their own "local" service requirements, their participation in any multilink PPP service is available only to bandwidth that is not required for its own current local demands. Therefore, a remote RCG's—**86** bandwidth that is available for multilink services can change at any time. The dynamic reassignment of remote RCGs that participate in a multilink bundle is also required to prevent a remote RCG—**86** from receiving packets so slowly that the originating RCG—**85** interprets this delay as lost packets. When the initiating RCG—**85** determines that a packet has been lost, and it is performing packet reassembly, it will, itself, request that the remote computer retransmit the lost packet. The initiating RCG will not ask any remote RCG—**86** to perform retransmissions or any other kind of data computations or manipulations.

Refer to FIG. **8** for the following discussion. In areas where there are existing 802.11 network equipment such as Neighborhood Access Point—**93**, or where there is sufficient bandwidth requirements from an installed base of RCGs to warrant the deployment of a Neighborhood Access Point—**93**, the RCGs will automatically detect the presence of the compatible neighborhood access points and register with that equipment for transport services. In this case, an RCG has an alternative broadband service route in addition to the multilink option. An RCG can communicate directly with a local 802.11 Network Access Point—**93** that is connected to the PSTN or another carrier's network via some sort of high bandwidth backbone such as a T-Carrier or optical carrier connection (T1, T3, OC3, OC12 etc.). The RCGs can communicate directly with neighborhood access points at their full 11/54 Mbps data rates to provide up to that full bandwidth to the user. This functionality is, of course, subject to the Network Access Point—**93** allowing access to its resources to the RCG according to the 802.11 wireless protocol.

This architecture is important since it provides an avenue to relieve the local class 5 offices of congestion that can be caused by a wide spread deployment of RCGs within the class 5 service area. Since each RCG requires a constant 24/7 modem connection, this ties up the class 5 switch in a fashion that it was not designed for. This could lead to wholesale class 5 office expansions which would be extremely expensive, and potentially prohibitive for the Local Exchange Carriers (LECs). By deploying neighborhood access points that operate at 54 Mbps (802.11a/g), in areas where the RCG concentration starts placing too high of a demand on the local class 5 office, the bandwidth from the RCGs can be aggregated by the neighborhood access points into large capacity backbones to relieve the switch congestion. In this case, the RCG POTS interface—**40** can be used solely as a lifeline connection, or when the 802.11 wireless LAN in which the RCG resides is congested. With this implementation, voice calls will be carried over the wireless interface as opposed to the POTS interface on which they would normally be carried. Also, the RCG modem—**41** connected to the POTS interface—**40** would not need to maintain a constant always on connection, it could be a dialed on demand connection and thereby relieving the local class 5 office switch.

Bouncing or Hopping Traffic:

Refer to FIG. **9**. In areas where the density of RCGs is less than the arbitrary number of 32 RCGs within its transmission radius for multilink connections, the RCGs can bounce, or relay, the data traffic between each other to reach other RCGs located farther than the RCGs wireless transmission area. Since the POTS data rate of 56 Kbps is miniscule as compared to the 11/54 Mbps 802.11b/g transfer rate, the overhead associated with bouncing data traffic is not a concern. This will allow for the fastest possible data transfer across POTS lines for every RCG user.

RCGs can also communicate directly with an 802.11a Neighborhood Access Point—**93** device (such as that used in WI-FI networks) that is connected to a data network con-

nection such as a DS3 or OC3 service via a Metro Access Point. Where an RCG has access to a broadband device such as an 802.11a type device, either directly or via a bounced signal across several RCGs, a direct high speed data connection can be used to transfer large files. When an RCG is communicating directly with an 802.11a device, data transfer speeds up to the full 11/54 Mbps can be achieved to speed video transfers for such applications as video on demand.

RCG Router Tables:

The RCG continually monitors its 802.11b/g wireless interface for transmissions from other RCGs or 802.11a Access Points as well as other 802.11b/g wireless devices within the residence. The RCG provides a means to identify and store the addresses of other RCGs and Neighborhood Access Points within its local area. The RCG creates routing tables, much like an IP router device, so that it knows which RCGs are local to itself, and how many hops will be needed to reach the maximum of 32 POTS lines or a Neighborhood Access Point. The RCG can then determine how to route its data transfers to gain the most efficient routing and network efficiencies.

The router tables in each RCG are continually updated by monitoring the 802.11 frames received from other RCGs or Network Access Points. The number of entries in the router tables can be limited to an arbitrary number of other RCGs but contains room for at least 32 entries. For each RCG listed in the router tables, certain information is kept such as signal strength, if the other device is another RCG or some other 802.11 compatible device, if the other RCG is reachable directly, or if it is accessed via another RCGs by hopping. In the case there RCG hopping is used, the address of each RCG that is hopped is stored in the routing table. When an RCG is first powered up, it monitors its 802.11 interface for a period of time to identify other RCGs or Neighborhood Access Point devices, or other Wi-Fi devices within its transmission area. When first deployed, the RCG will not have any entries in its routing tables. This condition can persist for some time, until another RCG or other 802.11 device is deployed within the former RCGs transmission range. In this state, the RCG can be used for wireless networking within the residence, connecting the local computer to the RCGs always on Internet connection as well as to other wireless devices within the home. When an 802.11 frame is received by an RCG that contains the address of an RCG whose address does not exist in the receiving RCG's router table (as is the case when a new RCG is first installed), the receiving RCG polls the transmitting RCG for its router table information. The received router information is reviewed for other RCG's or other 802.11 compatible devices that are not listed in its own router tables. A decision is made to use some, all, or none of the new route information in its router tables. There is no real limitation on the number of RCGs that can be "hopped" in order to build a complete router table or to reach many more RCGs, Neighborhood Access Points or Metro Access Points.

Equipment and Services Priorities:

Just as voice has priority over data transfers within a single RCG, local RCG traffic (both voice and data) has priority over remote transfer requests by other RCGs. If an RCG is currently using all of its available POTS bandwidth for its own purposes, it will deny any remote RCG's request for access to its POTS line. Only when there is available POTS bandwidth available will an RCG allow other RCGs access to its POTS line. It will, however, bounce the traffic to other RCGs within its transmission area if requested by the originating RCG. In this case, available wireless bandwidth of any RCG (that amount of the 11/54 Mbps not currently used for its own traffic) can be used to relay traffic between other RCGs that do have available POTS bandwidth. In the same fashion, excess wireless bandwidth of any RCG can be by other RCGs to access high speed backbones via Neighborhood or Metro Access Points.

RCGs can also access other 802.11 wireless networks (Wi-Fi for example) that happen to be deployed within their service areas. In this case, access agreements between the RCG service provider and the wireless network operator must be put into place. By remaining compatible with the 802.11 standards, the RCGs capabilities will benefit by the growing WI-FI network infrastructure, an the WI-FI network will benefit by the RCG network.

Voice Over POTS and Data Over Wireless:

Normally, all communications from an RCG will be transmitted over the local POTS line, or a multilink bundle made up of many remote RCG POTS lines. By default, all voice calls will be carried over the "local" POTS line—**40** to alleviate security/privacy concerns and only "data" will be transmitted via multilink bundles. Generally, since voice "data" is compressed locally by the RCG, the required bandwidth for a voice call is so small that it does not make for a good choice to route it over a multilink connection. However, it is possible to route voice calls entirely over another RCGs POTS line. It is also possible for an RCG to transmit voice data over POTS lines connected to other RCGs via multilink bundles or directly over its 802.11 wireless interface, and since the 802.11 specification does support the Wired Equivalent Privacy (WEP) specification, a secured connection can be made in this fashion.

Remote Upgradability

The RCG is designed with the capability for unassisted remote upgradability. The remote upgradability feature is not the same as the storing of operational parameters during the configuration process. This feature allows the system operator to add new features as they are developed, or to correct bugs remotely and without the users knowledge or involvement. This feature can also be used to install a complete new operating system (OS).

Key to the successful implementation of the Remote upgradability feature is that a completely fail-safe routine be implemented that can recover from any failure during the upgrade process and to re-initiate and monitor the upgrade process until it has successfully completed. This process is carried out by loading a boot loader program that is stored in non-volatile memory. The boot loader program provides the minimum capabilities to start up the RCG and connect into the system operator's diagnostics network to download fixes or a new OS. The boot loader program is technically part of the OS, but it cannot be over written by any upgrade process. It is responsible for detecting failure of the RCG and initiating a connection to the diagnostics network. Once connected with the diagnostics network, the boot loader will provide diagnostics support to help correct the RCG's operation and reconfigure the OS.

What is claimed is:

1. A client device for multilink data packet communication with a server, the client device comprising:

a first network interface having a first data transfer rate associated with a first path from the server to the first network interface of the client device;

a second network interface having a second data transfer rate associated with a second path from the server to the second network interface of the client device; and

at least one processor configured to:

transmit a first message through the first network interface to the server, wherein the first message includes a multilink request a destination URL;

transmit a second message through the second network interface to the server, wherein the second message includes a multilink session identification the destination URL; and

receive data packets from the server through the first and second network interfaces of the client device during the multilink session wherein the first data transfer rate and the second data transfer rate provide an increased data transfer rate of the first path and the second path from the server to the client device.

2. The client device of claim **1**, wherein the at least one processor further is configured to transmit the first message and the second message to at least one server, wherein the at least one server is a device providing the data packets, or a device that manages the client device and another device that is providing data to the client device.

3. The client device of claim **1**, wherein a server provides the multilink session identification that is unique to the multilink session.

4. The client device of claim **1**, wherein the first information is comprised of at least one of an Internet address associated with the first network interface, and the second information is comprised of at least one of an Internet address associated with the second network interface.

5. The client device of claim **1**, wherein each of the first network interface and the second network interface is one or more of cellular interface, Wi-Fi interface, a wireless interface, a cable interface, a wired interface, an Ethernet interface, a Bluetooth interface, a near-field communication interface, and an optical interface.

6. The client device of claim **1**, wherein the processor is configured to reorder the one or more data packets that are received over the at least two or more network interfaces of the client device during the multilink session.

7. The client device of claim **1**, wherein the client device is one of a cell phone, a tablet, a switch, a server, a network device, a router, a computer, a Wi-Fi device, a Wi-Max device, a wireless device, a mobile communication device, a near-field communications device, and a Bluetooth device.

8. A server for multilink communication with a device, the server comprising:

at least one server network interface; and

one or more processors coupled to the at least one server network interface and configured to:

receive a first multilink packet over the at least one server network interface, the first multilink packet comprised of a request for a multilink communication and first information associated with first network communication interface of the device that is capable of being used by the device to receive data packets;

sending a data packet including the multilink session identification to the first network communication interface of the device;

receive a second multilink packet over the at least one server network interface, the second multilink packet comprised of the multilink session identification and second information associated with a second network communication interface of the device that is capable of being used by the device to receive data packets; and

send different groups of data packets over the at least one server network interface to the first network communication interface of the device and to the second network communication interface of the device, wherein each of the different groups of data packets includes the multilink session identification.

9. The server of claim **8**, wherein the one or more processors is further configured to send the multilink session identification that is unique to the data packets being sent to the first network communication interface and the second network communication interface.

10. The server of claim **8**, wherein the one or more processors is further configured to:

receive a third multilink packet, the third multilink packet is comprised of multilink information associated with a third network communication interface of the device that is capable of being used by the device to receive data packets; and

send different groups of data packets to the first network communication interface of the device, the second network communication interface of the device and the third network communication interface of the device.

11. The server of claim **8**, wherein the one or more processors is further configured to receive a multilink packets comprised of multilink information associated with which one of the first network communication interface of the device, the second network communication interface of the device and the third network communication interface of the device is to be removed from the multilink session.

12. The server of claim **8**, wherein the one or more processors is further configured to receive different multilink packets over the at least one server network interface at different periods of time.

13. A first device comprising:

a network interface; and

at least one processor configured to:

transmit a first message through the network interface to a second device, wherein the first message includes a multilink request and a destination URL, the network interface to the second device having a data transfer rate associated therewith;

transmit a second message through the network interface to a third device, wherein the second message includes a multilink session identification that is unique to the multilink session and the destination URL, the network interface to the third device having a data transfer rate associated therewith; and

receive the different data packets through the at least one network interface from the second device and from the third device during the multilink session, wherein the data transfer rate associated with the network interface to the second device and the network interface to the third device provide an increased data transfer rate for the first device.

14. The first device of claim **13**, wherein the first device and the second device are separate devices or separate parts of the same device.

15. The first device of claim **13**, wherein the first device is one of a cell phone, a tablet, a switch, a server, a network device, a router, a computer, a Wi-Fi device, a Wi-Max device, a mobile communication device, a wireless communications device, a near-field communications device, and a Bluetooth device.

16. A first device for multilink communication, comprising:

at least one network interface; and

one or more processors coupled to the at least one network interface and configured to:

receiving one or more multilink packets where each multilink packet comprises information associated with one or more of a plurality of network communication interfaces of a second device that are capable of being used to receive data packets;

during a multilink session

splitting up data from a data source into different groups of data packets; and

controlling a data server where the data server sends the different groups of data packets from the data server to different network communication interfaces of the second device, wherein each of the different groups of data packets includes the multilink session identification.

17. A client device for multilink communication, the client device comprising:

a first network interface having a first data transfer rate associated therewith;

a second network interface having a second data transfer rate associated therewith; and

at least one processor and configured to:

transmit a first message through the first network interface to at least one server, wherein the first message includes a multilink request and a destination URL;

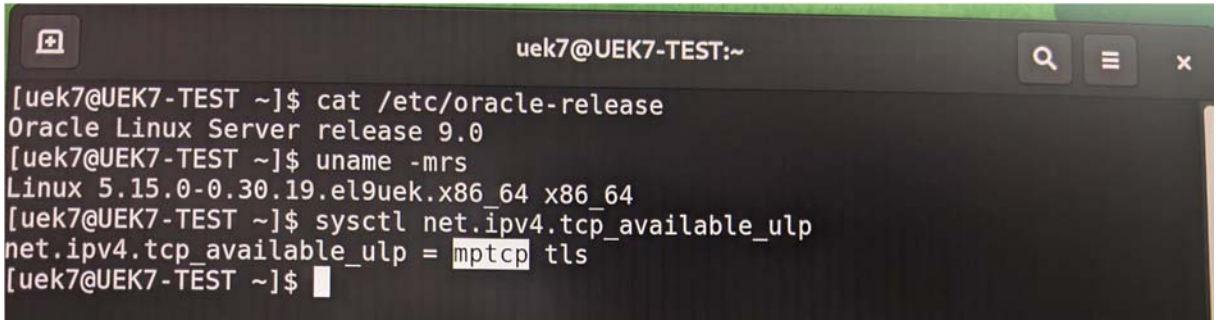
transmit a second message through the second network interface to the at least one server, wherein the second message includes a multilink session identification that is unique to the multilink session and the destination URL; and

receive concurrently the different data packets from the server through the first network interface and the second network interface of the client device during the multilink session, wherein the first data transfer rate and the second data transfer rate provide an increase in the data transfer rate of the client device.

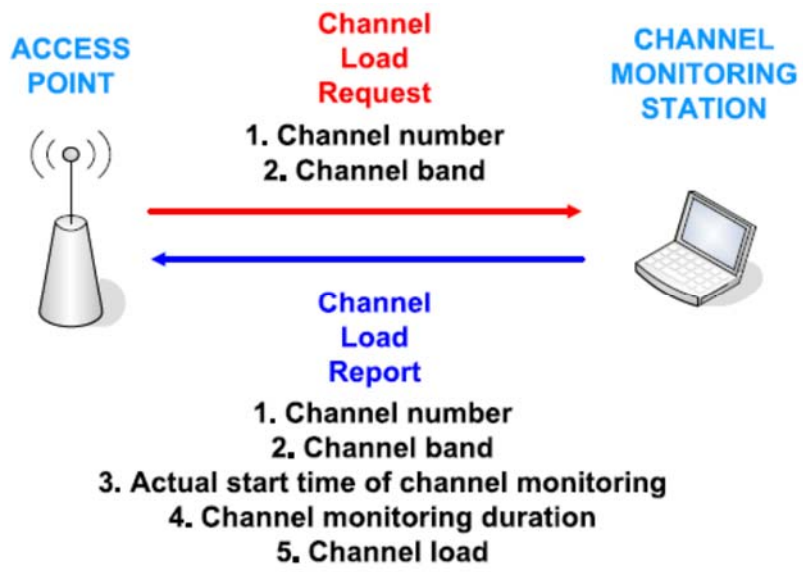
* * * * *

EXHIBIT D

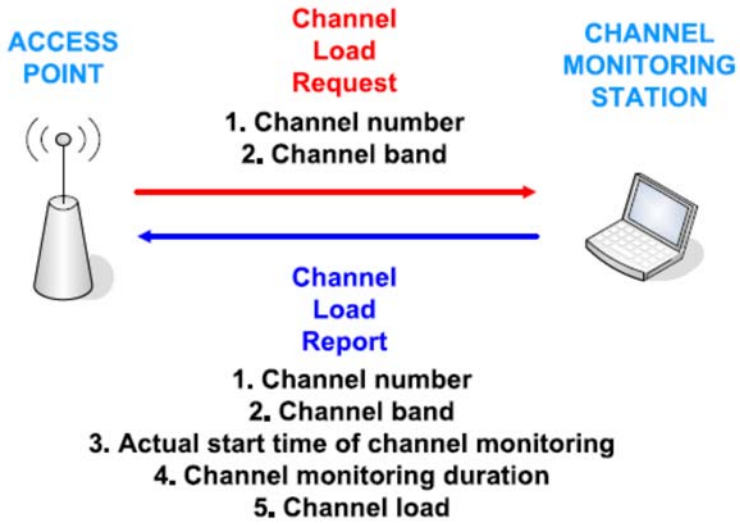
Infringement of U.S. Patent No. 8,228,801 by Oracle MPTCP Products

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
1a	1. A communications device that is capable of providing broadband communications services, comprising:	The Oracle MPTCP Products implement the claimed communication device by, for example, having Oracle Solaris, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6, Oracle Linux 9, and operating systems that operate in a similar manner installed on a device. By way of example, Oracle Linux 9 is charted herein. The Oracle MPTCP Products constitute a communications device that is capable of providing broadband communications services as described below: 
1b	at least one connection for connecting to a communications network;	The Oracle MPTCP Products include at least one connection for connecting to a communications network as described below: Network interfaces are identified by a name that combines a prefix and a suffix. The prefix depends on the type of network interface: Ethernet network interfaces: en; Wireless local area network (LAN) interfaces: wl; Wireless wide area network (WAN) interfaces: ww
1c	at least one wireless interface for connecting wirelessly to at least one remote communications device;	The Oracle MPTCP Products include at least one wireless interface for connecting wirelessly to at least one remote communications device as described below:

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		Network interfaces are identified by a name that combines a prefix and a suffix. The prefix depends on the type of network interface: Ethernet network interfaces: en; Wireless local area network (LAN) interfaces: wl; Wireless wide area network (WAN) interfaces: ww
1d	and a processor that	The Oracle MPTCP Products include a processor as described below: Oracle is pleased to announce Oracle Linux 9 general availability for Intel-64/AMD-64 (x86_64) and Arm (aarch64). This release includes the Unbreakable Enterprise Kernel Release 7 (UEK R7)
1e	requests the at least one remote communications device to assist in transferring data,	The Oracle MPTCP Products request the at least one remote communications device to assist in transferring data as described below: At a high level, an MPTCP implementation will take one input data stream from an application, and split it into one or more subflows, with sufficient control information to allow it to be reassembled and delivered reliably and in order to the recipient application.
1f	sends a request to the at least one remote communications device for requesting use of a portion of unused bandwidth of the at least one remote communications device,	The Oracle MPTCP Products send a request to the at least one remote communications device for requesting use of a portion of unused bandwidth of the at least one remote communications device as described below: The Oracle MPTCP Products provide wpa_supplicant. wpa_supplicant can be used as a roaming daemon to automatically connect to different networks as a device travels between locations. To facilitate roaming, an 11k capable client associated with an AP sends a request for a list of neighbor APs. The request is in the form of an 802.11 management frame known as an action packet…. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		An access point or a WLAN switch can request from a client or another access point data about channel load or how long the channel was used during a given time. A client, or some other access point, called a channel monitoring station, monitors one or more channels and collects load information for a period called channel monitoring duration.  TSPEC allows 802.11 wireless client to signal its traffic requirement to the AP. The client includes the TSPEC in the add traffic stream (ADDTS). TSPEC from client include data rate, packet size, number of stream & more. 802.11e standard specifies TSPEC to provide the management link between higher QoS protocols & the channel access function. Channel Access functions are defined by EDCA (Enhanced Distributed Channel Access) mechanism.

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		101 05:40:46.980979 Cisco_58:e6:1a Cisco_3e:80:bc 802.11 115 Action, SN=199, FN=0, Flags=...P.... Frame 101: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) 802.11 radio information IEEE 802.11 Action, Flags: ...P.... Type/Subtype: Action (0x0d) Frame Control: 0x10D0 (Normal) Duration: 44 Destination address: Cisco_3e:80:bc (54:75:d0:3e:80:bc) Source address: Cisco_58:e6:1a (00:1b:d4:58:e6:1a) BSS Id: Cisco_3e:80:bc (54:75:d0:3e:80:bc) Fragment number: 0 Sequence number: 199 IEEE 802.11 wireless LAN management frame Fixed parameters Action: 0x11 Category code: Management Notification (17) Action code: Setup request (0x0000) Dialog token: 0x04 Status code: Admission accepted (0x0000) Tagged parameters (87 bytes) Tag: Vendor Specific: Microsof: WMM/WME: TSPEC Element Tag Number: Vendor Specific (221) Tag length: 61 OUI: 00-50-f2 (Microsof) Vendor Specific OUI Type: 2 Type: WMM/WME (0x02) WME Subtype: TSPEC Element (2) Tag: Traffic Classification Tag Number: Traffic Classification (14) Tag length: 19 User Priority: 6 Classifier Type: TCP/UDP IP parameters (1) Classifier Mask: 0x55 Tag: TCLAS Processing : Incoming MSDU's higher layer parameters have to match to at least one of the associated TCLAS elements. Tag Number: TCLAS Processing (44) Tag length: 1 Processing: Incoming MSDU's higher layer parameters have to match to at least one of the associated TCLAS elements. (1) *apfMsConnTask_0: Mar 19 19:46:08.897: 00:1b:d4:58:e6:1a sending ADD TS to AP 54:75:D0:3E:80:B0 slotId 1, for client 00:1B:D4:58:E6:1A tid = 6 up = 6, upsd = 1, bw = 1072 *apfMsConnTask 0: Mar 19 19:46:08.897: Not including un-operational rate 6 in TSRS IE
1g	receives a response from the at least one remote communications device, the response containing information about the portion of unused bandwidth,	The Oracle MPTCP Products receive a response from the at least one remote communications device, the response containing information about the portion of unused bandwidth as described below: The Oracle MPTCP Products provide wpa_supplicant. wpa_supplicant can be used as a roaming daemon to automatically connect to different networks as a device travels between locations.

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		To facilitate roaming, an 11k capable client associated with an AP sends a request for a list of neighbor APs. The request is in the form of an 802.11 management frame known as an action packet…. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios. After the channel monitoring process, the results are reported to the requesting entity through a channel load report,…As a result, the station that issued the request is informed about the load of a channel. In other words this parameter gives an idea of how many free slots a new station would have at its disposal."  The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The AP response is also an action packet. From the response frame, the client knows which APs are candidates for the next roam.

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		In 802.11e, after receiving a request to use a portion of unused bandwidth, an AP responds to Tspec containing information about the portion of unused bandwidth. Below is an exemplary image of the response from the AP indicating available bandwidth. 101 05:40:46.980979 Cisco_58:e6:1a Cisco_3e:80:bc 802.11 115 Action, SN=199, FN=0, Flags=...P.... Frame 101: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) 802.11 radio information IEEE 802.11 Action, Flags: ...P.... Type/Subtype: Action (0x0d) Frame Control: 0x10D0 (Normal) Duration: 44 Destination address: Cisco_3e:80:bc (54:75:d0:3e:80:bc) Source address: Cisco_58:e6:1a (00:1b:d4:58:e6:1a) BSS Id: Cisco_3e:80:bc (54:75:d0:3e:80:bc) Fragment number: 0 Sequence number: 199 IEEE 802.11 wireless LAN management frame Fixed parameters Action: 0x11 Category code: Management Notification (17) Action code: Setup request (0x0000) Dialog token: 0x04 Status code: Admission accepted (0x0000) Tagged parameters (87 bytes) Tag: Vendor Specific: Microsof: WMM/WME: TSPEC Element Tag Number: Vendor Specific (221) Tag length: 61 OUI: 00-50-f2 (Microsof) Vendor Specific OUI Type: 2 Type: WMM/WME (0x02) WME Subtype: TSPEC Element (2) Tag: Traffic Classification Tag Number: Traffic Classification (14) Tag length: 19 User Priority: 6 Classifier Type: TCP/UDP IP parameters (1) Classifier Mask: 0x55 Tag: TCLAS Processing : Incoming MSDU's higher layer parameters have to match to at least one of the associated TCLAS elements. Tag Number: TCLAS Processing (44) Tag length: 1 Processing: Incoming MSDU's higher layer parameters have to match to at least one of the associated TCLAS elements. (1) *apfMsConnTask_0: Mar 19 19:46:08.897: 00:1b:d4:58:e6:1a sending ADD TS to AP 54:75:D0:3E:80:B0 slotId 1, for client 00:1B:D4:58:E6:1A tid = 6 up = 6, upsd = 1, bw = 1072 *apfMsConnTask 0: Mar 19 19:46:08.897: Not including un-operational rate 6 in TSRS IE
1h	selects the at least one remote communications device with unused bandwidth,	The Oracle MPTCP Products select the at least one remote communications device with unused bandwidth as described below:

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
		The Oracle MPTCP Products provide wpa_supplicant. wpa_supplicant can be used as a roaming daemon to automatically connect to different networks as a device travels between locations. On informed belief, any of the APs can be selected, including those with unused bandwidth.

1i	sends control information to the at least one remote communications device for participating in a multilink connection,	The Oracle MPTCP Products sends control information to the at least one remote communications device for participating in a multilink connection as described below:
		
		Host A initiates a new subflow between one of its addresses and one of Host B's addresses. The token -- generated from the key -- is used to identify which MPTCP connection it is joining, and the HMAC is used for authentication. The Hash-based Message Authentication Code (HMAC) uses the keys exchanged in the MP_CAPABLE handshake, and the random numbers (nonces) exchanged in these MP_JOIN options. MP_JOIN also contains flags and an Address ID that can be used to refer to the source address without the sender needing to know if it has been changed by a NAT.
		
		`Host A  Host B`
		`------  ------`
		`MP_JOIN  ->`
		`[B's token, A's nonce,`
		`A's Address ID, flags]`
		`<-  MP_JOIN`
		`[B's HMAC, B's nonce,`
		`B's Address ID, flags]`
		`ACK + MP_JOIN  ->`
		`[A's HMAC]`
		`<-  ACK`

1j	receives packets from the at least one remote communications device and	The Oracle MPTCP Products receive packets from the at least one remote communications device and aggregate the data from the at least one remote communications device with data

#	U.S. Patent No. 8,228,801	Oracle MPTCP Products
	aggregates the data from the at least one remote communications device with data transfers from the at least one connection to increase data bandwidth for the communications device.	transfers from the at least one connection to increase data bandwidth for the communications device as described below: At a high level, an MPTCP implementation will take one input data stream from an application, and split it into one or more subflows, with sufficient control information to allow it to be reassembled and delivered reliably and in order to the recipient application. Using recent hardware and 3 dual-port 10Gig NICs, Multipath TCP is able to transmit a single data-stream at the rate of up to 51.8 Gbit/s.

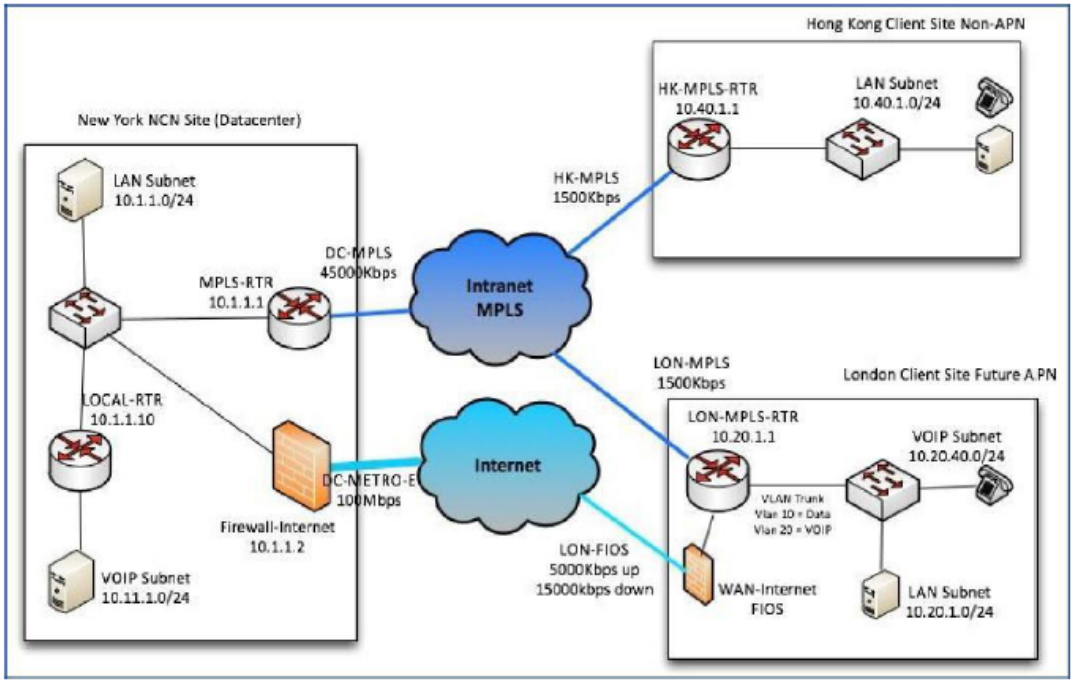
EXHIBIT E

Infringement of U.S. Patent No. 8,228,801 by Oracle SD-WAN Products

#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
10a	10. A communications device that is capable of providing broadband communications services, comprising:	The Oracle SD-WAN Products including Oracle Talari Appliances, including the Talari E50 Appliance, Talari E100 Appliance, Talari D2000 Appliance, Talari D6000 Appliance, Talari T5000 Appliance, and devices that operate in a similar manner, Oracle SD-WAN Virtual Appliances, Oracle SD-WAN Edge, Oracle SD-WAN Aware, Oracle SD-WAN Orchestration Cloud Service, Oracle SD-WAN, and devices that operate in a similar manner, implement the claimed communications device. By way of example, the T5000 Appliance is charted herein. The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. Oracle SD-WAN Release 2.5 incorporates the T5000 seamlessly into the entire family of appliances offered by Oracle.
10b	at least one connection for connecting to a network;	The Oracle SD-WAN Products include at least one connection for connecting to a network as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. A WAN Link provides for the description of individual Internet or Intranet connections of a Site to the WAN or direct connections to other Sites. Individual uses of a WAN Link would be used to describe connections such as: individual Cable, DSL, fiber or other Internet Service Providers; MPLS, IPSec or other site-to-site VPN connections; backup links such as Cellular or Advanced Wireless providers.

#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
10c	at least one wireless interface for connecting wirelessly to remote communications devices; and	The Oracle SD-WAN Products include at least one wireless interface for connecting wirelessly to remote communications devices as described below: The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections. A WAN Link provides for the description of individual Internet or Intranet connections of a Site to the WAN or direct connections to other Sites. Individual uses of a WAN Link would be used to describe connections such as: individual Cable, DSL, fiber or other Internet Service Providers; MPLS, IPSec or other site-to-site VPN connections; backup links such as Cellular or Advanced Wireless providers. Conduit Service (Conduit): A service that is a logical combination of one or more Paths. This is the typical service for enterprise, Site-to-Site Intranet traffic using the full value of the Talari WAN. Depending on the configuration, traffic is managed across multiple WAN Links to create an end-to-end tunnel. Adaptive Bandwidth Detection was introduced in Edge 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Oracle Talari Appliance to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD.
10d	a processor that requests the remote communications devices to transfer portions of data, sends a request to the	The Oracle SD-WAN Products include a processor that requests the remote communications devices to transfer portions of data, sends a request to the remote communications devices for requesting use of a portion of unused bandwidth of each

#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
	remote communications devices for requesting use of a portion of unused bandwidth of each of the remote communications devices, receives a response from each of the remote communications devices, the response containing information about the portion of unused bandwidth for each of the remote communications devices, selects a group of the remote communications devices with a larger, combined, unused bandwidth, sends control information to the selected remote communications devices for participating in a multilink transfer, and receiving packets from the selected remote communications devices and combines and sequences the portions of the data from the remote communications devices with second data transferred from the at least one connection to increase data bandwidth for the communications device.	of the remote communications devices, receives a response from each of the remote communications devices, the response containing information about the portion of unused bandwidth for each of the remote communications devices, selects a group of the remote communications devices with a larger, combined, unused bandwidth, sends control information to the selected remote communications devices for participating in a multilink transfer, and receiving packets from the selected remote communications devices and combines and sequences the portions of the data from the remote communications devices with second data transferred from the at least one connection to increase data bandwidth for the communications device as described below: The Oracle SD-WAN Edge is engineered for maximum business impact in an enterprise network. This is achieved by creating failsafe WANs that offer superior application reliability, while unlocking the benefits of network resiliency and scalable bandwidth. The dynamic conduit is a conduit between two Oracle SD-WAN Edge client sites that is not predefined in the Oracle SD-WAN Edge configuration file, but is created on-demand based on network traffic. From a user perspective, the advantage of a conduit between client sites is that traffic can flow directly from one client Oracle SD-WAN Edge site to a second client site without having to traverse the NCN or two conduits. In addition, the conduit is built and removed dynamically based on user defined traffic thresholds. These thresholds are defined in either packets per second (pps) or bandwidth (kbps).

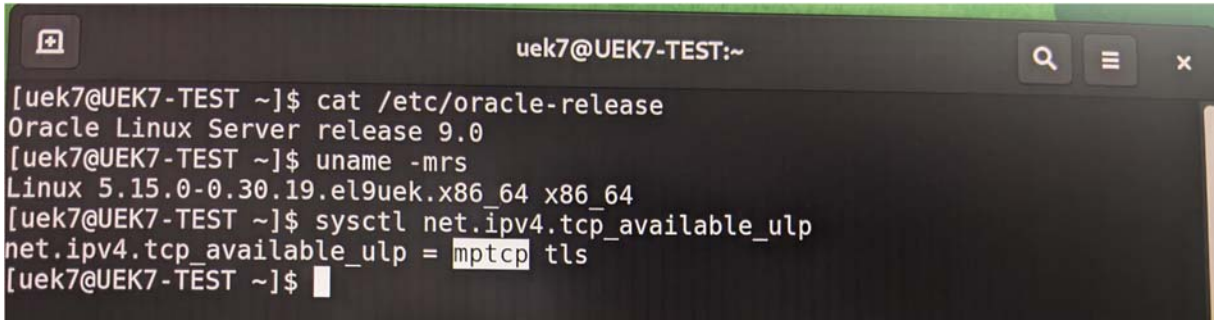
#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
		 SD-WAN Edge Network Settings allows for the configuration of global parameters that impact the operation of the entire SD-WAN Edge network. Global Path Bandwidth Testing Settings allows for the configuration of global parameters that impacts path bandwidth testing operations on individual SD-WAN Edge.. The NCN with the WAN-To-WAN option enabled can forward all routes to all client appliances within a WAN-To-WAN Forwarding Group. By default, all sites reside in the default WAN To-WAN Forwarding Group. The user can also define additional

#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
		WAN-To-WAN Forwarding Groups as required. The groups are defined at the Global configuration level. The intermediate site will monitor the traffic flow between Client Sites to determine if the traffic level reaches the user defined threshold. If the traffic flow reaches the defined threshold, the Intermediate node will instruct the client nodes to establish a Dynamic Conduit. An on-demand standby WAN link is a standby WAN link that may be activated to supplement conduit bandwidth when the bandwidth provided by the primary WAN links in the conduit falls below the bandwidth threshold configured in conduit QoS Policy. In addition, if all primary WAN links are dead or disabled, an on-demand standby WAN link becomes active and user traffic is transmitted on it. Oracle SD-WAN creates a cohesive and efficient collection of all physical links and interfaces, and aggregates them into a single, logical interface to create a virtual WAN conduit. The WAN conduit takes advantage of real-time intelligence encapsulated in the header of every packet the SD-WAN processes. It also supports 128b or 256b advanced encryption standard (AES) across all aggregated WAN paths. All WAN paths are managed unidirectionally so that every packet reliably reaches its destination. Adaptive Bandwidth Detection was introduced in Edge 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Oracle Talari Appliance to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD.

#	U.S. Patent No. 8,228,801	Oracle SD-WAN Products
		The dynamic conduit is a conduit between two Oracle SD-WAN Edge client sites that is not predefined in the Oracle SD-WAN Edge configuration file, but is created on-demand based on network traffic. From a user perspective, the advantage of a conduit between client sites is that traffic can flow directly from one client Oracle SD-WAN Edge site to a second client site without having to traverse the NCN or two conduits. In addition, the conduit is built and removed dynamically based on user defined traffic thresholds. These thresholds are defined in either packets per second (pps) or bandwidth (kbps). "Oracle SD-WAN creates a cohesive and efficient collection of all physical links and interfaces, and aggregates them into a single, logical interface to create a virtual WAN conduit. The WAN conduit takes advantage of real-time intelligence encapsulated in the header of every packet the SD-WAN processes. It also supports 128b or 256b advanced encryption standard (AES) across all aggregated WAN paths. All WAN paths are managed unidirectionally so that every packet reliably reaches its destination." (Five Ways SD-WAN is Transforming Cloud Connectivity White Paper, pp. 3-4).

EXHIBIT F

Infringement of U.S. Patent No. 9,350,649 by Oracle MPTCP Products

#	U.S. Patent No. 9,350,649	Oracle MPTCP Products
7a	7. A method for establishing and sending data during a multipath connection, comprising:	The Oracle MPTCP Products perform the claimed method utilizing, for example, devices having Oracle Solaris, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6, Oracle Linux 9, and devices that operate in a similar manner. By way of example, Oracle Linux 9 is charted herein. The Oracle MPTCP Products perform a method for establishing and sending data during a multipath connection as described below: 
7b	the data-source device receiving multipath connection requests from a plurality of data-requesting devices, each of the multipath connection requests involving a particular multipath connection to a data-requesting device;	The Oracle MPTCP Products include the data-source device receiving multipath connection requests from a plurality of data-requesting devices, each of the multipath connection requests involving a particular multipath connection to a data-requesting device as described below: Network interfaces are identified by a name that combines a prefix and a suffix. The prefix depends on the type of network interface: Ethernet network interfaces: en; Wireless local area network (LAN) interfaces: wl; Wireless wide area network (WAN) interfaces: ww Associating a New Subflow with an Existing MPTCP Connection: The exchange of keys in the MP_CAPABLE handshake provides material that can be used to authenticate the endpoints

#	U.S. Patent No. 9,350,649	Oracle MPTCP Products

		when new subflows will be set up. Additional subflows begin in the same way as initiating a normal TCP connection, but the SYN, SYN/ACK, and ACK packets also carry the MP_JOIN option.
		
		Host A initiates a new subflow between one of its addresses and one of Host B's addresses. The token -- generated from the key -- is used to identify which MPTCP connection it is joining, and the HMAC is used for authentication. The Hash-based Message Authentication Code (HMAC) uses the keys exchanged in the MP_CAPABLE handshake, and the random numbers (nonces) exchanged in these MP_JOIN options. MP_JOIN also contains flags and an Address ID that can be used to refer to the source address without the sender needing to know if it has been changed by a NAT.
		
		`Host A  Host B`
		`------  ------`
		`MP_JOIN  ->`
		`[B's token, A's nonce,`
		`A's Address ID, flags]`
		`<-  MP_JOIN`
		`[B's HMAC, B's nonce,`
		`B's Address ID, flags]`
		`ACK + MP_JOIN  ->`
		`[A's HMAC]`
		`<-  ACK`

7c	the data-source device associating a connection ID to each multipath connection request;	The Oracle MPTCP Products include the data-source device associating a connection ID to each multipath connection request as described below: Token: A locally unique identifier given to a multipath connection by a host. May also be referred to as a "Connection ID".

#	U.S. Patent No. 9,350,649	Oracle MPTCP Products
		Host A initiates a new subflow between one of its addresses and one of Host B's addresses. The token -- generated from the key -- is used to identify which MPTCP connection it is joining, and the HMAC is used for authentication. The Hash-based Message Authentication Code (HMAC) uses the keys exchanged in the MP_CAPABLE handshake, and the random numbers (nonces) exchanged in these MP_JOIN options. MP_JOIN also contains flags and an Address ID that can be used to refer to the source address without the sender needing to know if it has been changed by a NAT.

7d	the data-source device using multipath information about each of a plurality of network-edge devices that is capable of joining in a particular multipath connection to a particular data-requesting device, the particular multipath connection having a particular connection ID;	The Oracle MPTCP Products include the data-source device using multipath information about each of a plurality of network-edge devices that is capable of joining in a particular multipath connection to a particular data-requesting device, the particular multipath connection having a particular connection ID as described below:
		
		The exchange of keys in the MP_CAPABLE handshake provides material that can be used to authenticate the endpoints when new subflows will be set up. Additional subflows begin in the same way as initiating a normal TCP connection, but the SYN, SYN/ACK, and ACK packets also carry the MP_JOIN option.
		
		In the first MP_JOIN on the SYN packet, illustrated in Figure 5, the initiator sends a token, random number, and address ID.
		
		`1 2 3`
		`0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1`
		`+---+---+---+---+---+---+---+---+`
		`| Kind | Length = 12 |Subtype| |B| Address ID |`
		`+---+---+---+---+---+---+---+---+`
		`| Receiver's Token (32 bits) |`
		`+---+---+---+---+---+---+---+---+`
		`| Sender's Random Number (32 bits) |`
		`+---+---+---+---+---+---+---+---+`
		
		Figure 5: Join Connection (MP_JOIN) Option (for Initial SYN)

#	U.S. Patent No. 9,350,649	Oracle MPTCP Products

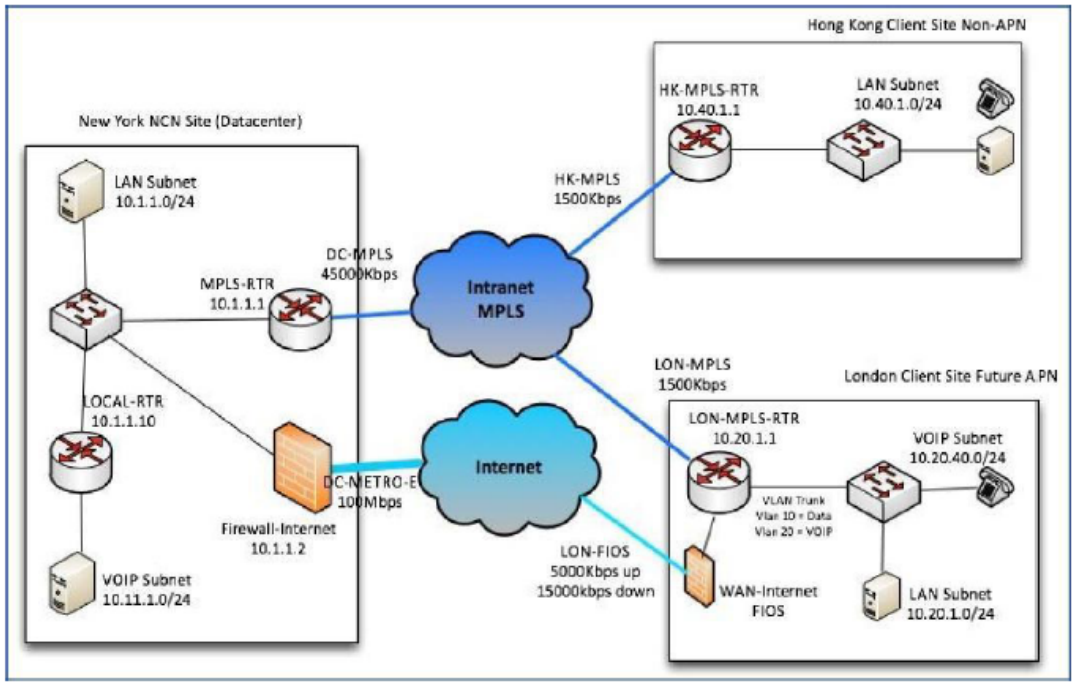
7e	the data-source device notifying each of the network-edge devices that is participating in the particular multipath connection associated with the particular connection ID; and	The Oracle MPTCP Products include the data-source device notifying each of the network-edge devices that is participating in the particular multipath connection associated with the particular connection ID as described below:
		
		HOST B sends an ACK in response to MP_Join for each additional subflow.
		
		`Host A  Host B`
		`------  ------`
		`MP_JOIN  ->`
		`[B's token, A's nonce,`
		`A's Address ID, flags]`
		`<-  MP_JOIN`
		`[B's HMAC, B's nonce,`
		`B's Address ID, flags]`
		`ACK + MP_JOIN  ->`
		`[A's HMAC]`
		`<-  ACK`

7f	the data-source device sending data associated with the particular connection ID to the network-edge devices participating in the particular multipath connection associated with the particular connection ID.	The Oracle MPTCP Products include the data-source device sending data associated with the particular connection ID to the network-edge devices participating in the particular multipath connection associated with the particular connection ID as described below: At a high level, an MPTCP implementation will take one input data stream from an application, and split it into one or more subflows, with sufficient control information to allow it to be reassembled and delivered reliably and in order to the recipient application.

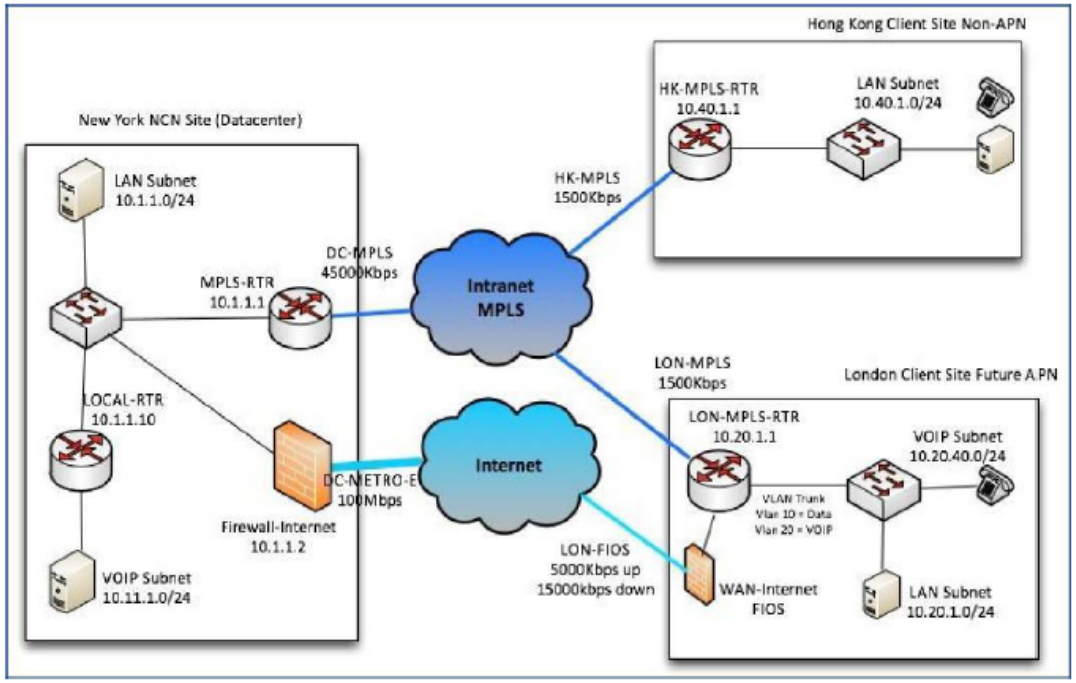
EXHIBIT G

Infringement of U.S. Patent No. 9,350,649 by Oracle SD-WAN Products

#	U.S. Patent No. 9,350,649	Oracle SD-WAN Products
1a	1. A method for establishing and sending data during a multipath connection comprising:	The Oracle SD-WAN Products perform the claimed method utilizing, for example, devices including Oracle Talari Appliances, including the Talari E50 Appliance, Talari E100 Appliance, Talari D2000 Appliance, Talari D6000 Appliance, Talari T5000 Appliance, and devices that operate in a similar manner, Oracle SD-WAN Virtual Appliances, Oracle SD-WAN Edge, Oracle SD-WAN Aware, Oracle SD-WAN Orchestration Cloud Service, Oracle SD-WAN, and devices that operate in a similar manner. By way of example, the T5000 Appliance is charted herein. The Oracle SD-WAN Products perform a method for establishing and sending data during a multipath connection as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. Oracle SD-WAN Release 2.5 incorporates the T5000 seamlessly into the entire family of appliances offered by Oracle.
1b	a data-source device receiving multipath information about each of a plurality of network-edge devices that is capable of joining a multipath connection with a data-requesting device,	The Oracle SD-WAN Products include a data-source device receiving multipath information about each of a plurality of network-edge devices that is capable of joining a multipath connection with a data-requesting device as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private

#	U.S. Patent No. 9,350,649	Oracle SD-WAN Products
		WAN links and public Internet connections and providing support for up to 128 branch connections.  SD-WAN Edge Network Settings allows for the configuration of global parameters that impact the operation of the entire SD-WAN Edge network. Global Path Bandwidth Testing Settings allows for the configuration of global parameters that impacts path bandwidth testing operations on individual SD-WAN Edge. The NCN with the WAN-To-WAN option enabled can forward all routes to all client appliances within a WAN-To-WAN Forwarding Group. By default, all sites reside in the

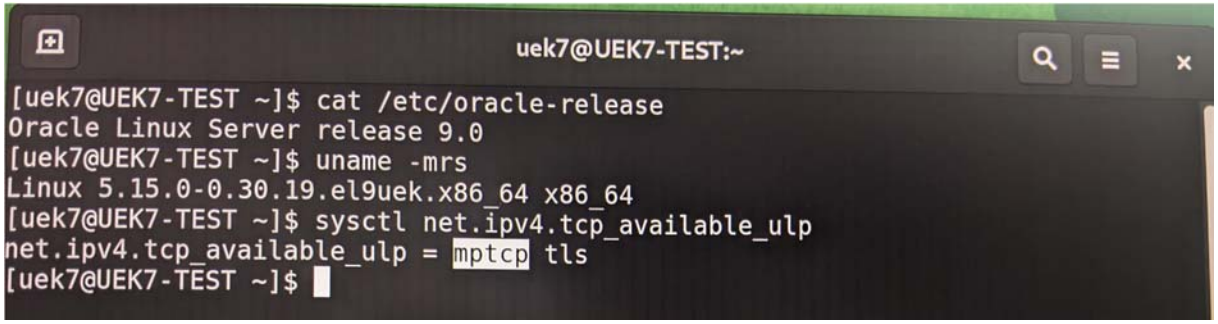
#	U.S. Patent No. 9,350,649	Oracle SD-WAN Products
		default WAN To-WAN Forwarding Group. The user can also define additional WAN-To-WAN Forwarding Groups as required. The groups are defined at the Global configuration level. The intermediate site will monitor the traffic flow between Client Sites to determine if the traffic level reaches the user defined threshold. If the traffic flow reaches the defined threshold, the Intermediate node will instruct the client nodes to establish a Dynamic Conduit. An on-demand standby WAN link is a standby WAN link that may be activated to supplement conduit bandwidth when the bandwidth provided by the primary WAN links in the conduit falls below the bandwidth threshold configured in conduit QoS Policy. In addition, if all primary WAN links are dead or disabled, an on-demand standby WAN link becomes active and user traffic is transmitted on it. Adaptive Bandwidth Detection, introduced in Edge 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Oracle Talari Appliance to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD.
1c	each of the network-edge devices being connected to one or more networks, and	The Oracle SD-WAN Products include each of the network-edge devices being connected to one or more networks as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections.

#	U.S. Patent No. 9,350,649	Oracle SD-WAN Products
		
1d	the data-source device performing at least one of (i) sending different groups of data packets to different network-edge devices that are participating in the multipath connection, (ii) sending different streams of data to one or more of the network-edge devices that are participating in the multipath connection, and	The Oracle SD-WAN Products include the data-source device performing at least one of (i) sending different groups of data packets to different network-edge devices that are participating in the multipath connection, (ii) sending different streams of data to one or more of the network-edge devices that are participating in the multipath connection, and (iii) sending combinations of different streams and different groups of data packets to one or more of the network-edge devices that are participating in the multipath connection as described below: Oracle SD-WAN creates a cohesive and efficient collection of all physical links and interfaces, and aggregates them into a single, logical interface to create a virtual WAN conduit. The WAN conduit takes advantage of real-time intelligence encapsulated in the header of every packet the SD-WAN processes. It also supports 128b or 256b advanced encryption standard (AES)

#	U.S. Patent No. 9,350,649	Oracle SD-WAN Products
	(iii) sending combinations of different streams and different groups of data packets to one or more of the network-edge devices that are participating in the multipath connection.	across all aggregated WAN paths. All WAN paths are managed unidirectionally so that every packet reliably reaches its destination.

EXHIBIT H

Infringement of U.S. Patent No. 10,868,908 by Oracle MPTCP Products

#	U.S. Patent No. 10,868,908	Oracle MPTCP Products
1a	1. A client device for multilink data packet communication with a server, the client device comprising:	The Oracle MPTCP Products implemented the claimed client device utilizing, for example, devices having Oracle Solaris, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6, Oracle Linux 9, and devices that operate in a similar manner. By way of example, Oracle Linux 9 is charted herein. The Oracle MPTCP Products constitute a communications device that is capable of providing broadband communications services as described below: 
1b	a first network interface having a first data transfer rate associated with a first path from the server to the first network interface of the client device;	The Oracle MPTCP Products include a first network interface having a first data transfer rate associated with a first path from the server to the first network interface of the client device as described below: Network interfaces are identified by a name that combines a prefix and a suffix. The prefix depends on the type of network interface: Ethernet network interfaces: en; Wireless local area network (LAN) interfaces: wl; Wireless wide area network (WAN) interfaces: ww. Each network interface has its own data transfer rate and path from the server to the first network interface.

#	U.S. Patent No. 10,868,908	Oracle MPTCP Products
1c	a second network interface having a second data transfer rate associated with a second path from the server to the second network interface of the client device; and	The Oracle MPTCP Products include a second network interface having a second data transfer rate associated with a second path from the server to the second network interface of the client device as described below: Network interfaces are identified by a name that combines a prefix and a suffix. The prefix depends on the type of network interface: Ethernet network interfaces: en; Wireless local area network (LAN) interfaces: wl; Wireless wide area network (WAN) interfaces: ww. Each network interface has its own data transfer rate and path from the server to the second network interface.
1d	at least one processor configured to:	The Oracle MPTCP Products include at least one processor as described below: Oracle is pleased to announce Oracle Linux 9 general availability for Intel-64/AMD-64 (x86_64) and Arm (aarch64). This release includes the Unbreakable Enterprise Kernel Release 7 (UEK R7)
1e	transmit a first message through the first network interface to the server, wherein the first message includes a multilink request a destination URL;	The Oracle MPTCP Products transmit a first message through the first network interface to the server, wherein the first message includes a multilink request a destination URL as described below: In the first MP_JOIN on the SYN packet, illustrated in Figure 5, the initiator sends a token, random number, and address ID.

#	U.S. Patent No. 10,868,908	Oracle MPTCP Products

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+-------+-----+-+---------------+
|     Kind      |  Length = 12  |Subtype|     |B|   Address ID  |
+---------------+---------------+-------+-----+-+---------------+
|                  Receiver's Token (32 bits)                   |
+---------------------------------------------------------------+
|                Sender's Random Number (32 bits)               |
+---------------------------------------------------------------+
```

Figure 5: Join Connection (MP_JOIN) Option (for Initial SYN)

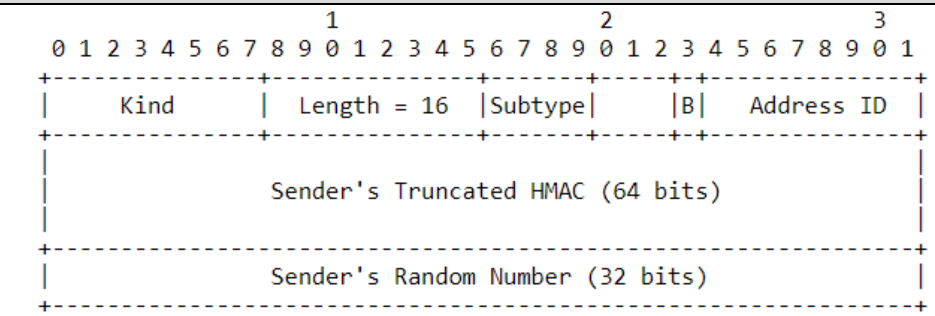
The MP_JOIN SYN sends not only the token (which is static for a connection) but also random numbers (nonces) that are used to prevent replay attacks on the authentication method.

The MP_JOIN option includes an "Address ID". This is an identifier that only has significance within a single connection, where it identifies the source address of this packet, even if the IP header has been changed in transit by a middlebox. The Address ID allows address removal (Section 3.4.2) without needing to know what the source address at the receiver is, thus allowing address removal through NATs. The Address ID also allows correlation between new subflow setup attempts and address signaling (Section 3.4.1), to prevent setting up duplicate subflows on the same path, if an MP_JOIN and ADD_ADDR are sent at the same time.

The exchange of keys in the MP_CAPABLE handshake provides material that can be used to authenticate the endpoints when new subflows will be set up. Additional subflows begin in the same way as initiating a normal TCP connection, but the SYN, SYN/ACK, and ACK packets also carry the MP_JOIN option.

Host A initiates a new subflow between one of its addresses and one of Host B's addresses. The token -- generated from the key -- is used to identify which MPTCP connection it is joining, and the HMAC is used for authentication. The Hash-based Message Authentication Code (HMAC) uses the keys exchanged in the MP_CAPABLE handshake, and the random numbers

#	U.S. Patent No. 10,868,908	Oracle MPTCP Products
		(nonces) exchanged in these MP_JOIN options. MP_JOIN also contains flags and an Address ID that can be used to refer to the source address without the sender needing to know if it has been changed by a NAT. Host A Host B ------ ------ MP_JOIN -> [B's token, A's nonce, A's Address ID, flags] <- MP_JOIN [B's HMAC, B's nonce, B's Address ID, flags] ACK + MP_JOIN -> [A's HMAC] <- ACK
1f	transmit a second message through the second network interface to the server, wherein the second message includes a multilink session identification the destination URL; and	The Oracle MPTCP Products transmit a second message through the second network interface to the server, wherein the second message includes a multilink session identification the destination URL as described below: The second message transmitted in multilink data packet communication is MP_JOIN that includes an MP_JOIN option containing a random number and a truncated (leftmost 64 bits) Hash-based Message Authentication Code (HMAC) as well as references to the source address.

#	U.S. Patent No. 10,868,908	Oracle MPTCP Products
		 Figure 6: Join Connection (MP_JOIN) Option (for Responding SYN/ACK) The exchange of keys in the MP_CAPABLE handshake provides material that can be used to authenticate the endpoints when new subflows will be set up. Additional subflows begin in the same way as initiating a normal TCP connection, but the SYN, SYN/ACK, and ACK packets also carry the MP_JOIN option. Host A initiates a new subflow between one of its addresses and one of Host B's addresses. The token -- generated from the key -- is used to identify which MPTCP connection it is joining, and the HMAC is used for authentication. The Hash-based Message Authentication Code (HMAC) uses the keys exchanged in the MP_CAPABLE handshake, and the random numbers (nonces) exchanged in these MP_JOIN options. MP_JOIN also contains flags and an Address ID that can be used to refer to the source address without the sender needing to know if it has been changed by a NAT.
1g	receive data packets from the server through the first and second network interfaces of the client device during the multilink session wherein the first data transfer rate and the	The Oracle MPTCP Products receive data packets from the server through the first and second network interfaces of the client device during the multilink session wherein the first data transfer rate and the second data transfer rate provide an increased data transfer rate of the first path and the second path from the server to the client device as described below:

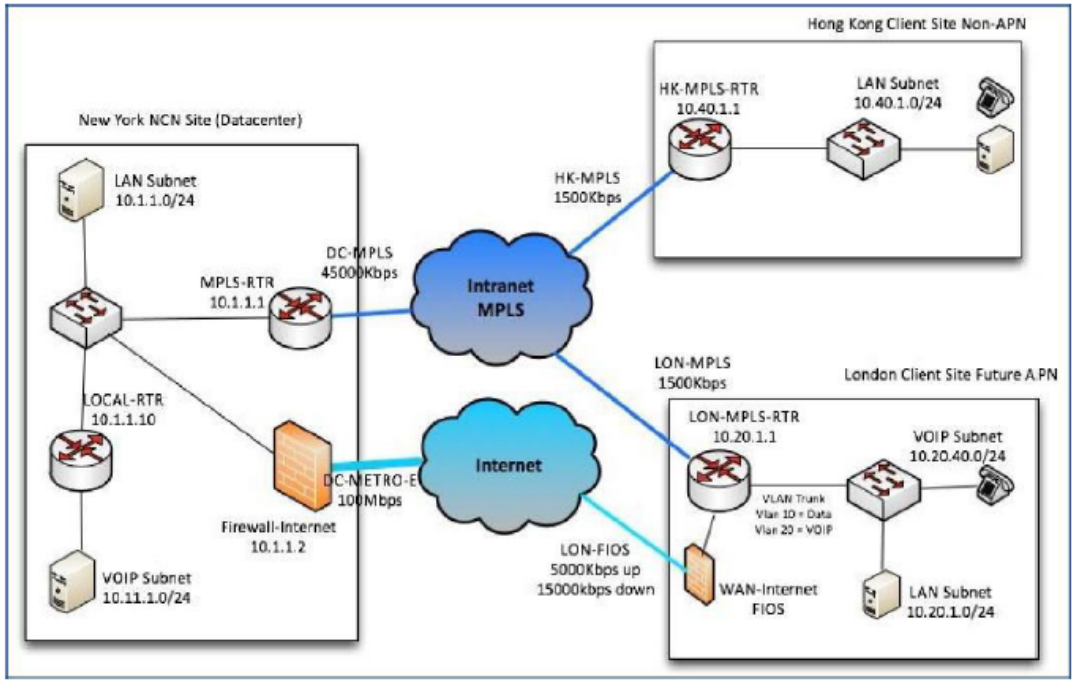
#	U.S. Patent No. 10,868,908	Oracle MPTCP Products
	second data transfer rate provide an increased data transfer rate of the first path and the second path from the server to the client device.	Once an MPTCP connection has begun with the MP_CAPABLE exchange, further subflows can be added to the connection. Hosts have knowledge of their own address(es), and can become aware of the other host's addresses through signaling exchanges as described in Section 3.4. Using this knowledge, a host can initiate a new subflow over a currently unused pair of addresses. It is permitted for either host in a connection to initiate the creation of a new subflow MPTCP can be used to increase the data transfer rate for data communications. For example, using recent hardware and 3 dual-port 10Gig NICs, Multipath TCP is able to transmit a single data-stream at the rate of up to 51.8 Gbit/s.

EXHIBIT I

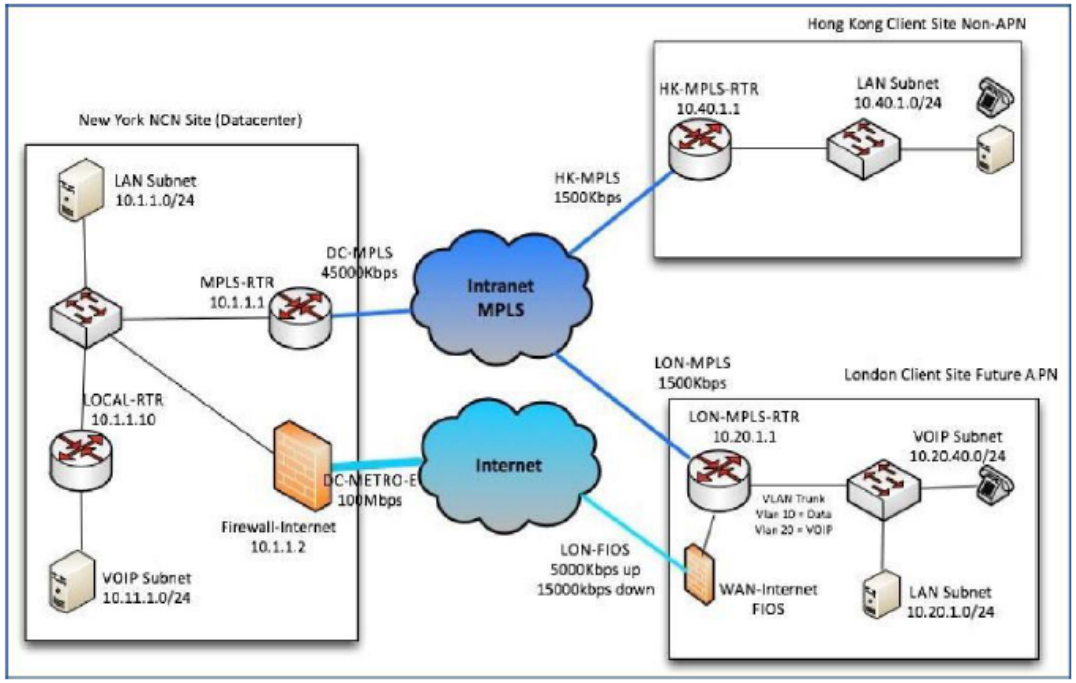
Infringement of U.S. Patent No. 10,868,908 by Oracle SD-WAN Products

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
13a	13. A first device comprising:	The Oracle SD-WAN Products, including Oracle Talari Appliances, including the Talari E50 Appliance, Talari E100 Appliance, Talari D2000 Appliance, Talari D6000 Appliance, Talari T5000 Appliance, and devices that operate in a similar manner, Oracle SD-WAN Virtual Appliances, Oracle SD-WAN Edge, Oracle SD-WAN Aware, Oracle SD-WAN Orchestration Cloud Service, Oracle SD-WAN, and devices that operate in a similar manner, implement the claimed device. By way of example, the T5000 Appliance is charted herein. The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. Oracle SD-WAN Release 2.5 incorporates the T5000 seamlessly into the entire family of appliances offered by Oracle.
13b	a network interface; and	The Oracle SD-WAN Products include a network interface as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. A WAN Link provides for the description of individual Internet or Intranet connections of a Site to the WAN or direct connections to other Sites. Individual uses of a WAN Link would be used to describe connections such as: individual Cable, DSL, fiber or other Internet Service Providers; MPLS, IPSec or other site-to-site VPN connections; backup links such as Cellular or Advanced Wireless providers.
13c	at least one processor configured to:	The Oracle SD-WAN Products include at least one processor as described below:

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
		The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections.
13d	transmit a first message through the network interface to a second device, wherein the first message includes a multilink request and a destination URL, the network interface to the second device having a data transfer rate associated therewith;	The Oracle SD-WAN Products transmit a first message through the network interface to a second device, wherein the first message includes a multilink request and a destination URL, the network interface to the second device having a data transfer rate associated therewith as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections." (Oracle SD-WAN Edge Features Guide, p. 3-1). The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections.

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
		 SD-WAN Edge Network Settings allows for the configuration of global parameters that impact the operation of the entire SD-WAN Edge network. Global Path Bandwidth Testing Settings allows for the configuration of global parameters that impacts path bandwidth testing operations on individual SD-WAN Edge. Adaptive Bandwidth Detection was introduced in Edge 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Oracle Talari Appliance to adjust the bandwidth rate on the WAN Link dynamically

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
		based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD.
13e	transmit a second message through the network interface to a third device, wherein the second message includes a multilink session identification that is unique to the multilink session and the destination URL, the network interface to the third device having a data transfer rate associated therewith; and	The Oracle SD-WAN Products transmit a second message through the network interface to a third device, wherein the second message includes a multilink session identification that is unique to the multilink session and the destination URL, the network interface to the third device having a data transfer rate associated therewith as described below: The Oracle SD-WAN includes the T5000 Appliance, which delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. The T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections.

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
		 SD-WAN Edge Network Settings allows for the configuration of global parameters that impact the operation of the entire SD-WAN Edge network. Global Path Bandwidth Testing Settings allows for the configuration of global parameters that impacts path bandwidth testing operations on individual SD-WAN Edge. Adaptive Bandwidth Detection was introduced in Edge 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Oracle Talari Appliance to adjust the bandwidth rate on the WAN Link dynamically

#	U.S. Patent No. 10,868,908	Oracle SD-WAN Products
		based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD. The Internet Service is for traffic between an enterprise user and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, Oracle SD-WAN Edge does actively manage bandwidth by rate-limiting Internet traffic relative to the conduit and intranet traffic as per the configuration established by the administrator.
13f	receive the different data packets through the at least one network interface from the second device and from the third device during the multilink session, wherein the data transfer rate associated with the network interface to the second device and the network interface to the third device provide an increased data transfer rate for the first device.	The Oracle SD-WAN Products receive the different data packets through the at least one network interface from the second device and from the third device during the multilink session, wherein the data transfer rate associated with the network interface to the second device and the network interface to the third device provide an increased data transfer rate for the first device as described below: Oracle SD-WAN creates a cohesive and efficient collection of all physical links and interfaces, and aggregates them into a single, logical interface to create a virtual WAN conduit. The WAN conduit takes advantage of real-time intelligence encapsulated in the header of every packet the SD-WAN processes. It also supports 128b or 256b advanced encryption standard (AES) across all aggregated WAN paths. All WAN paths are managed unidirectionally so that every packet reliably reaches its destination.