Obviously, those skilled in the art may make various modifications of the present invention and modifications without departing from the spirit and scope of the invention. Thus, if such modifications and variations of the present invention and the claims of the invention belongs to the technical scope of equivalents, the present invention is also intended to include these changes and modifications included.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100450130C	21 Dec 2005	7 Jan 2009	中兴通讯股份有限公司	System and method for realizing intermediately informing user telephone fee
CN101286858B	12 Apr 2007	8 Dec 2010	中兴通讯股份有限公司	Method and system for charging of WAP gateway for mobile terminal
CN101287161B	14 May 2008	20 Apr 2011	华为软件技术有限公司	Service request forwarding method, gateway for wireless application protocol and communication system
CN101583095B	3 Jun 2009	8 May 2013	中兴通讯股份有限公司	Telephone charge prewarning method and prewarning system
CN101674561B	15 Jan 2009	4 Jul 2012	华为技术有限公司	Subscriber arrearage treatment method, device and system
WO2010028556A1 *	10 Jul 2009	18 Mar 2010	Huawei Technologies Co., Ltd.	Method for processing user debt, mobile management entity and network system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04Q7/22, H04L12/14, H04M17/00

LEGAL EVENTS

Date	Code	Event	Description
6 Oct 2010	C14	Granted	
17 Jan 2007	C10	Request of examination as to substance	
22 Nov 2006	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101815275 A
(43)申请公布日 2010.08.25

(21)申请号 201010143134.0

(22)申请日 2010.04.09

(71)申请人 刘泱
地址 100190 北京市海淀区知春路63号卫星大厦6层604单元

(72)发明人 梁秋实 袁彬

(74)专利代理机构 北京联创佳为专利事务所（普通合伙） 11362
代理人 郭防

(51)Int.Cl.
H04W 4/24(2009.01)
H04W 88/02(2009.01)

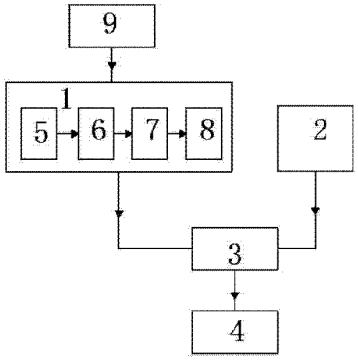
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种手机话费计算装置

(57)摘要

本发明公开了一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的同步用户的话费计费规则到手机的网络同步模块(1)，记录用户通话详情的监控模块(2)，使用网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价的批价模块(3)和将批价后的账单存储在手机上的存储模块(4)。本发明计算话费时的实时性和准确性高，并且可直接在手机上查询，话费详单数据量小，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。



CN 101815275 A

1. 一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的

网络同步模块(1)，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器(9)相连；

监控模块(2)，用于记录用户通话详情；

批价模块(3)，用于将网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价；

存储模块(4)，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块(2)和网络同步模块(1)与批价模块(3)相连，批价模块(3)与存储模块(4)相连。

2. 根据权利要求1所述的手机话费计算装置，其特征在于：所述网络同步模块(1)包括获取手机的运营商、归属地和品牌信息的用户信息模块(5)，根据获取的用户信息从业务支撑服务器(9)下载运营商该品牌下所有的套餐列表的列表下载模块(6)、用于用户选择所用套餐的选择模块(7)和根据用户所选套餐从业务支撑服务器(9)获取该套餐计费规则的规则下载模块(8)。

3. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

4. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

5. 根据权利要求4所述的手机话费计算装置，其特征在于：所述短信中心号与运营商、省份的对应关系从业务支撑服务器(9)下载，或预先存储在手机上。

6. 根据权利要求2所述的手机话费计算装置，其特征在于：所述规则下载模块(8)下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS上网费用计费规则、月租费、套餐费和手机号段。

7. 根据权利要求1所述的手机话费计算装置，其特征在于：所述监控模块(2)在手机端监控用户的通话、发送短信、通过GPRS联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

8. 根据权利要求7所述的手机话费计算装置，其特征在于：所述通话详情包括用户的通话、发送短信和通过GPRS联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

9. 根据权利要求1、2或5所述的手机话费计算装置，其特征在于：所述业务支撑服务器(9)是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

一种手机话费计算装置

技术领域

[0001] 本发明涉及一种手机话费计算装置，特别是一种手机上使用的手机话费计算装置。

背景技术

[0002] 一个典型的电信运营商所使用的计费系统中，业务网元是电信运营商提供基础服务的系统，电信的核心服务包括通话、短信、GPRS(GeneralPacketRadioService) 等，每个服务对应一组业务网元。CDR(calldetailrecord) 是业务详情记录，记录业务网元向用户提供的每次服务的详情。CDR40 不仅仅指通话详情记录，也包括短信或 GPRS 的使用详情记录。每条 CDR 中包含发话时间、结束时间、主叫、被叫、发话地点等信息。系统向业务网元查询 CDR40，然后对 CDR40 批价，得到账单详情，并将账单详情存入账单数据库。

[0003] 而现有的话费计算系统存在下述问题：

首先，现有的话费计算系统是在各电信运营商内部运作，且因为一些技术原因容易出现话费错算、误算的情况，手机用户很难清楚的了解自己每笔话费的产生原因，进而无法确定自己话费的准确性、正确性。

[0004] 其次，因为话单的数量巨大，一些电信运营商并不对全部用户提供话费详单查询服务。即便某些电信运营商对于部分用户开放了详单查询的业务，也存在使用不便(比如要输入服务密码、或者到移动营业厅现场办理)、实时性不强(比如只能查上月的话费详单、或几天前的话费详单) 等问题。

[0005] 再次，即便用户拿到了话费详单，也会因为各运营商、各种套餐的计算规则各异，如存在优惠时段、赠送通话分钟数等特殊规则，导致用户对话费的核对非常困难。

发明内容

[0006] 本发明的目的在于，提供一种手机话费计算装置。它是一种便于用户查看和理解，具有高实时性、准确性的手机话费计算装置。

[0007] 本发明的技术方案：一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器和手机；还包括设置在手机上的

网络同步模块，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器相连；

监控模块，用于记录用户通话详情；

批价模块，用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价；

存储模块，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块和网络同步模块与批价模块相连，批价模块与存储模块相连。

[0008] 上述的手机话费计算装置中，所述网络同步模块包括获取手机的运营商、归属地

和品牌信息的用户信息模块，根据获取的用户信息从业务支撑服务器下载运营商该品牌下所有的套餐列表的列表下载模块、用于用户选择所用套餐的选择模块和根据用户所选套餐从业务支撑服务器获取该套餐计费规则的规则下载模块。

[0009] 前述的手机话费计算装置中，所述用户信息模块为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0010] 前述的手机话费计算装置中，所述用户信息模块为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0011] 前述的手机话费计算装置中，所述短信中心号与运营商、省份的对应关系从业务支撑服务器下载，或预先存储在手机上。

[0012] 前述的手机话费计算装置中，所述规则下载模块下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0013] 前述的手机话费计算装置中，所述监控模块在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0014] 前述的手机话费计算装置中，所述通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0015] 前述的手机话费计算装置中，所述业务支撑服务器是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0016] 与现有技术相比，本发明由于使用了无线网络、业务支撑服务器和手机组成的基本构架，并在手机上结合了用于同步用户的话费计费规则到手机上的网络同步模块、用于记录用户通话详情的监控模块和用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价的批价模块。这种结合方式可以使计算话费时的实时性和准确性高，并且可直接在手机上查询，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。本发明所提供的手机话费计算装置，针对特定用户计算他自身的手机话费，话费详单数据量小，使用户可以很方便、快捷的查看、汇总自己以往的话费使用情况，并且可以在通话结束后立刻看到通话费用的变化。同时利用了电信运营商的话费计算规则，保证了话费计算的准确性，透明性。又因为计费规则存储在手机上，所以无需等待一次通话、联网结束即可实时计算当前通话、联网所产生的费用，更可以在拨出、接听一个电话之前预估本次通话每分钟的费用。现有的计费装置是在电信端计算，这套装置要对一个地市或一省的所有用户提供计费服务，其计算、存储的数据量相当庞大，因此也造成了计算的实时性较差，准确度不高，查询不便的问题。而本装置只针对特定用户计算，数据量、运算量只有电信计费装置的数百万至数千万分之一。对于正常使用的用户，每个月的数据存储只消耗数百 K，每天需要计费的电话、短信、上网等次数也只有数百次以内，完全可以做到实时准确的计算。

附图说明

[0017] 图 1 是本发明的结构示意图；

图 2 是本发明实施例的工作流程图；

EX1060 - Page 519

图 3 是图 2 中步骤 S10 的工作流程图。

[0018] 附图中的标记：1- 网络同步模块，2- 监控模块，3- 批价模块，4- 存储模块，5- 用户信息模块，6- 列表下载模块，7- 选择模块，8- 规则下载模块，9- 业务支撑服务器。

具体实施方式

[0019] 下面结合附图和实施例对本发明作进一步的说明，但并不作为对本发明限制的依据。

实施例

[0020] 一种手机话费计算装置，结构如图 1 所示，包括无线网络、业务支撑服务器 3 和手机；还包括设置在手机上的

网络同步模块 1，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器 9 相连；

监控模块 2，用于记录用户通话详情；

批价模块 3，用于将网络同步模块 1 上的话费计费规则对监控模块 2 记录的用户通话详情进行批价；

存储模块 4，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块 2 和网络同步模块 1 与批价模块 3 相连，批价模块 3 与存储模块 4 相连。

[0021] 网络同步模块 1 包括获取手机的运营商、归属地和品牌信息的用户信息模块 5，根据获取的用户信息从业务支撑服务器 9 下载运营商该品牌下所有的套餐列表的列表下载模块 6、用于用户选择所用套餐的选择模块 7 和根据用户所选套餐从业务支撑服务器 9 获取该套餐计费规则的规则下载模块 8。

[0022] 用户信息模块 5 为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0023] 用户信息模块 5 也为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0024] 短信中心号与运营商、省份的对应关系从业务支撑服务器 9 下载，或预先存储在手机上。

[0025] 规则下载模块 8 下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0026] 监控模块 2 在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0027] 通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0028] 业务支撑服务器 9 是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0029] 本发明的工作流程(如图 2)：

步骤 S10，通过网络同步模块 1 同步该用户的话费计费规则到手机；

步骤 S20，在手机端通过监控模块 2 监控用户的通话、发送短信、通过 GPRS 联网的行为，

并将此行为存为详细日志；

步骤 S30，在批价模块 3 上，使用该用户的话费计费规则对详细日志进行批价；

步骤 S50，用存储模块 4 将批价后的账单存储在手机上。并通过手机显示设备（可为手机显示屏）展现给用户。

[0030] 其中步骤 S10 还包括以下步骤（如图 3）：

步骤 S101，通过用户信息模块 5，用户选择所用手机的运营商、归属地和品牌；

步骤 S102，通过列表下载模块 6，手机从支撑服务器获取该运营商该品牌下所有的套餐列表；

步骤 S103，通过选择模块 7，用户从列表中选择自己采用的套餐；

步骤 S104，通过规则下载模块 8，手机从支撑服务器获取该套餐的计费规则。

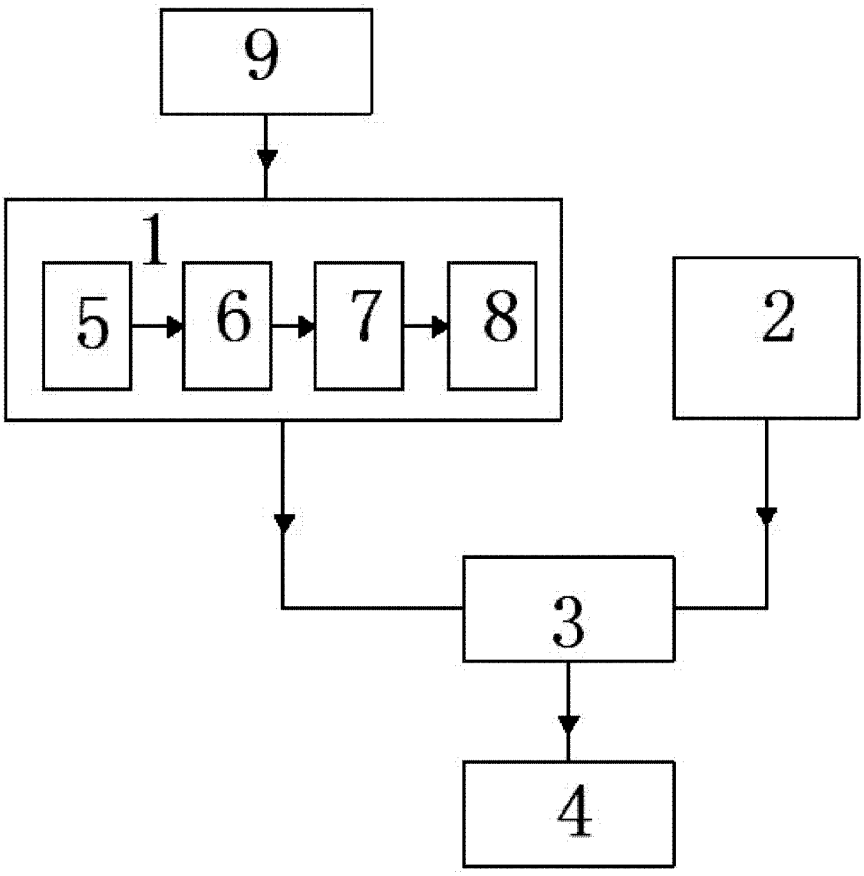


图 1

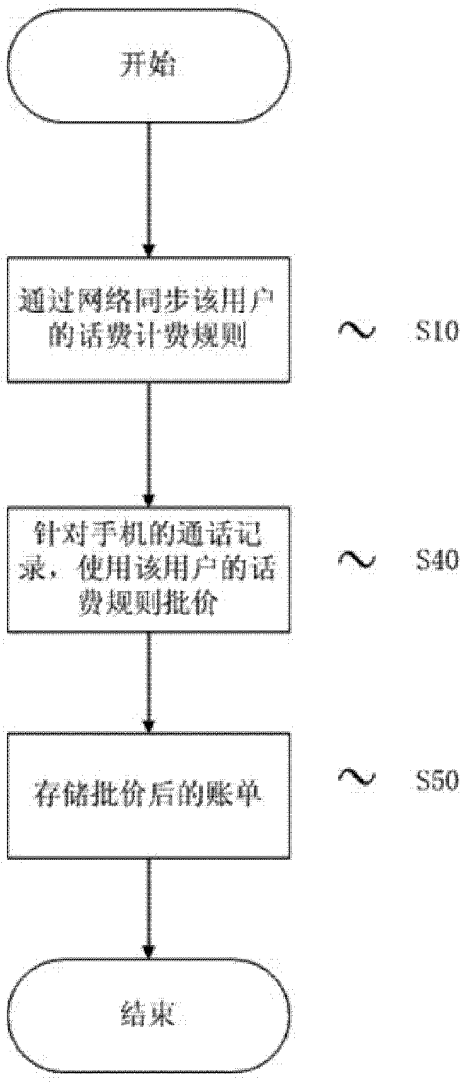

开始
通过网络同步该用户的话费计费规则
S10
针对手机的通话记录，使用该用户的话费规则批价
S40
存储批价后的账单
S50
结束

图 2

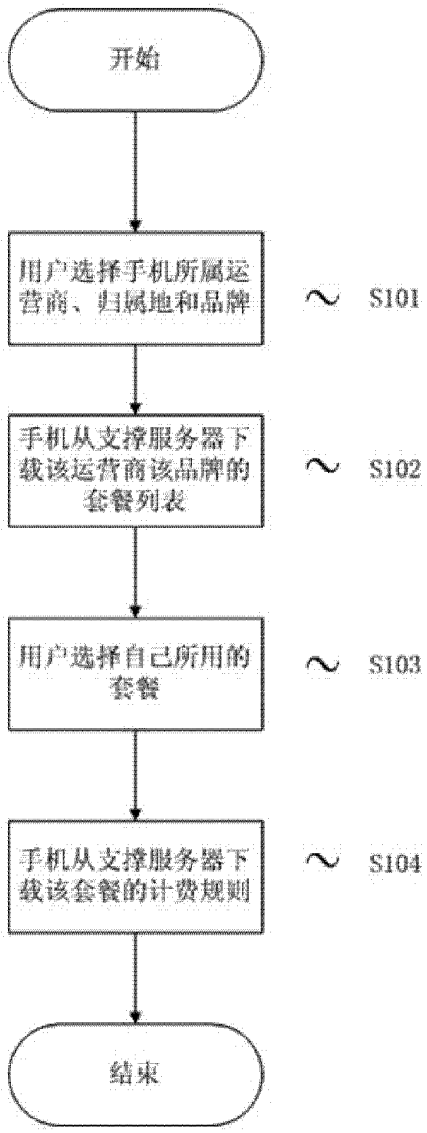

开始
用户选择手机所属运营商、归属地和品牌
S101
手机从支撑服务器下载该运营商该品牌的套餐列表
S102
用户选择自己所用的套餐
S103
手机从支撑服务器下载该套餐的计费规则
S104
结束

图 3

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Mobile phone charge calculating device

CN 101815275 A

Publication number	CN101815275 A
Publication type	Application
Application number	CN 201010143134
Publication date	Aug 25, 2010
Filing date	Apr 9, 2010
Priority date	Apr 9, 2010
Inventors	梁秋实, 袁彬
Applicant	刘涉
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (2), Classifications (2), Legal Events (5)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a mobile phone charge calculating device, which is characterized by comprising a wireless network, a service support server (9), a mobile phone, a network synchronization module (1), a monitoring module (2), a pricing module (3) and a storage module (4), wherein the network synchronization module (1) is arranged on the mobile phone and is used for synchronizing a charge billing rule of a user to the mobile phone; the monitoring module (2) is used for recording user conversation details; the pricing module (3) is used for pricing the user conversation details recorded by the monitoring module (2) by using the charge billing rule on the network synchronization module (1); and the storage module (4) is used for storing a bill after pricing in the mobile phone. The calculating device has high real-time performance and accuracy during charge calculation, can query the charge on the mobile phone directly, has a small charge detail record data volume, needs no password and is more convenient and efficient, and simultaneously the stored bill is convenient for a user to check the charge.

DESCRIPTION translated from Chinese

One kind of phone calls computing device

Art

[0001] The present invention relates to a phone bill computing devices, especially cell phone calls on a computing device to use the phone.

BACKGROUND

[0002] A typical billing system used by telecom operators, the business NE telecommunications operators to provide basic services systems, telecommunications core services include calls, SMS, GPRS (GeneralPacketRadioService), etc., each service corresponds to a Group business NE. (3)R (calldetailrecord) is the business details of the recording, the details of each service provided to the user NE business records. CDR40 not only refers to the call detail records, including SMS or GPRS usage detail records. Each CDR contains the utterance time, end time, caller, callee, caller location and other information. Systems to business NE query CDR40, then CDR40 grant price, get bill details and billing details stored in the billing database.

[0003] and the existing computing system calls the following problems:

First, the existing computing system calls in the inner workings of the telecom operators, and prone to technical reasons because some calls wrong calculation, miscalculation of the situation, the mobile phone user is difficult to clearly understand the causes of their own each bill, and thus can not be determine their own phone bill accuracy, correctness.

[0004] Second, because of the huge number of single words, some carriers do not bill for all users with details of a single query service. Even some telecom operators for some users open the details of a single query of business, there are also inconvenient to use (for example, to enter the service password, or to apply for Business Hall site), real-time is not strong (such as last month's bill can only check single detail, or details of a single bill a few days ago) and other

CLAIMS (9) translated from Chinese

1. A phone bill computing device, comprising: a wireless network, business support server (9) and mobile phones; also includes network settings on the phone synchronization module (1), is used to synchronize the user's calls to a cell phone charging rules connected through a wireless network and business support server (9); monitoring module (2) for recording call details of the user; grant price module (3) for network synchronization module calls accounting rules (1), for monitoring Module User Call Details (2) batch record price; memory module (4) for the phone, and connected storage bills after the grant price and the phone's display equipment; monitoring module (2) and network synchronization module (1) the approved price module (3) is connected, (4) is connected to the grant price module (3) and memory modules.

2. The phone calls computing device of claim 1, wherein, wherein: said network synchronization module (1) including access to mobile phone operators, attribution and brand information subscriber information module (5), according to the obtained user information from the business support server (9) Downloads operators under the brand list download module lists all the packages (6) for the user to select the choice with our subscription module (7) and based on user selected business support package from the server (9) to get the package charging rules rules download module (8).

3. 3. Phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

4. The phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) through the phone's SMS center number to determine the user's operators and the home provinces, through the mobile phone base station information to the current assist in determining the

issues.

[0005] Once again, even if the user got the details of a single bill, also because the calculation rules for each operator, a variety of different packages, such as the existence of preferential period, giving the number of calls and other special rules minute, causing the user to check the phone bill is very difficult .

SUMMARY

The purpose of [0006] The present invention is to provide a phone bill computing device. It is a user-friendly viewing and understanding, with a high real-time accuracy of phone calls computing device.

[0007] aspect of the present invention: a phone bill computing device, comprising: a wireless network, business support servers and mobile phones; also includes setting on the phone

Network synchronization module for synchronizing user charging rules to the phone calls connected through a wireless network and business support server;

Monitoring module for recording user call details;

Grant price module for network synchronization module calls on the accounting rules for the monitoring module records the user calls the details were approved price;

Storage module for on the phone, and connected storage bills after the grant price and the phone's display device; connected monitoring module and network synchronization module and the grant price of the module, the module is connected to the grant price and the storage module.

[0008] The computing device of phone calls, the network synchronization module includes access to mobile phone operators, attribution and subscriber information module brand of information, access to information based on user downloads carriers under the brand all the support from the business server Package list List Download module for the user to select the package selection module and access rules of the charging rules package downloaded from the service module supporting server based on user-selected packages.

[0009] The aforementioned phone bill computing device, wherein the user information module for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0010] The foregoing phone calls computing device, the mobile phone subscriber information module for SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0011] The foregoing phone calls computing device, the message center number correspondence between operators, provinces and downloaded from the service support server or stored on the phone.

[0012] The foregoing phone calls computing device, the rules of the download module download package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, Package fee and phone number section.

[0013] The aforementioned phone bill computing device, wherein the monitoring module to monitor the end user in the mobile phone calls, send text messages through GPRS network acts as the call details, and this behavior is saved as a detailed log, or directly call phone call records As the call details.

[0014] The foregoing calculation means phone calls, the call details including the user's calls, send text messages and through the GPRS network behavior utterance time, end time, the called party, the caller, the caller location and traffic.

[0015] The foregoing phone calls computing device, the storage server is a business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0016] Compared with the prior art, the basic framework of the present invention is the use of a wireless network, composed of business support servers and mobile phones, combined with a bill charging rules for synchronizing user on the phone to the network synchronization module on your phone record the call details of the user for the monitoring module and charging rules calls for network synchronization module for monitoring module records the user's call details were awarded the grant price price module. This combination can make calls when calculating real-time and high

location of the user module.

5. 5. phone calls computing device according to claim 4, wherein, characterized in that: the SMS center number correspondence between operators, provinces and from business support server (9) download, or stored on the phone.

6. 6. phone calls computing device according to claim 2, wherein, wherein: said rules download module (8) Download the package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, GRPS Charging Rules Internet access charges, monthly fees, course fees and phone number section.

7. 7. The phone calls computing device according to claim 1, characterized in that: the monitoring module (2) monitor the user's end of the phone call, send SMS, via GPRS network acts as the call details, and keep this behavior for detailed logging, or directly call phone call records as a call for more information.

8. 8. phone calls computing device according to claim 7, wherein, wherein: said call details including the user's calls, send SMS and GPRS network behavior by utterance time, ending time, the called party, the caller, the caller Location and traffic.

9. 9. phone calls, 2 or computing device according to claim 5, characterized in that: the business support server (9) is a storage package list, the corresponding charging rule packages and SMS center number and operators, provinces server relationship.

accuracy, and can query directly on the phone without a password, faster and more convenient, but also easy for users to store bills for calls reconciliation. Phone calls computing device of the present invention provides, calculated for a particular user's phone bill of his own, a small amount of data calls single detail, so that users can easily and quickly view, summarizing his past calls usage, and can end in a call After seeing changes in the cost of calls immediately. While taking advantage of the service provider's bill calculation rules to ensure that the bill calculation accuracy, transparency. And because the accounting rules are stored on the phone, so no need to wait for a call, the networking end the current call to real-time computing, networking costs arising, more can be set aside, before answering a phone call estimate this cost per minute . Existing billing system is to calculate the telecommunications side, this device is to provide billing services for all users by one city or a province, which is calculated, the amount of data storage is quite large, and therefore resulted in the more real-time computing poor accuracy is not high, the query inconvenient questions. And this is only for a specific user computing device, the amount of data, computation device only telecommunications billing millions to thousands of parts per million. For normal use, the monthly data storage consumes only several hundred K, daily need billing telephone, text messaging, Internet and other times only within hundreds of times, can be done in real-time and accurate count Da Bian.

Brief Description

[0017] Figure 1 is a schematic structural view of the present invention; FIG. 2 is a flowchart of an embodiment of the present invention; FIG. 3 is a flowchart of step SIO of Figure 2.

[0018] The drawings mark: 1- network synchronization module, 2-monitoring module, 3 grant price module, 4 storage modules, user information module 5-, 6- List Download module, 7-selection module, 8 Rules download module, 9-business support server.

Specific embodiments

[0019] accompanying drawings and the following embodiment of the present invention will be further illustrated by, but not as a basis for limiting the present invention.

Example

[0020] A computing device phone calls, the structure shown in Figure 1, including Wi-Fi, business support server 3 and mobile phones; also includes setting on the phone

Network synchronization module 1, calls for synchronizing user charging rules to the phone, connected through a wireless network and business support server 9;

Monitoring Module 2, is used to record the call details of the user;

Module 3 approved price for network synchronization module Call Details user charging rule calls for a monitoring module 2 on the batch record price;

Storage Module 4 for the bill after the grant price of storage on the phone, and the phone is connected to a display device; monitoring module 2 and network synchronization module 1 module 3 is connected with the grant price, grant price of module 3 is connected with the storage module 4.

[0021] network synchronization module 1 includes access to mobile phone operators, attribution and brand information user information module 5, download carriers under the brand list all the packages to download the module from the list of six business support server 9 based on user access to information for the user to select the package selection module download module with 7 and rules based on user-selected packages to get the package from the service support server charging rules 9 8.

[0022] The user information module 5 for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0023] The user information module 5 also via mobile phone SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0024] SMS center number corresponds to the relationship operators, provinces and downloaded from the service support server 9, or stored on the phone.

[0025] Rule 8 download download module packages billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, package costs and phone number section.

[0026] 2 at the end of the phone monitoring module to monitor the user's call, send SMS, via GPRS network acts as the call details, and keep a detailed log of this behavior, or directly call phone call records as a call for more information.

[0027] Call details include the user's calls, send text messages and through the GPRS network behavior utterance time,

end time, the called party, the caller, the caller location and traffic.

[0028] 9 is a storage server business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0029] The workflow of the invention (Figure 2):

Step S10, the synchronous network synchronization module 1 through the user's calls to the phone charging rules; step S20, the mobile terminal 2 through the monitoring module to monitor users' calls, send text messages through GPRS network behavior, and this behavior is saved for details logs;

Step S30, the grant price Module 3, using the user's calls for a detailed log accounting rules grant price; step S50, with a storage module 4 will grant price after the bill is stored on the phone. And through mobile display devices (for mobile phone display) presented to the user.

[0030] wherein step further comprises the step SIO (Figure 3):

Step S101, the user information module 5, the user selects the mobile phone operators, attribution and brand; step S102, 6, cell phones get packages list of all under the carrier of the brand from the supporting server list download module; step S103, 7, users choose their own package by selecting the modules used from the list; step S104, the adoption of the rules download module 8, cell phone charging rules to get the package from the support server.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN102711076B *	May 24, 2012	Feb 11, 2015	武汉诚迈科技有限公司	一种实时预测手机通话余额的方法
WO2012171369A1 *	Mar 15, 2012	Dec 20, 2012	Zte Corporation	Method and system for calculating call charge of terminal

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04W88/02

LEGAL EVENTS

Date	Code	Event	Description
Oct 30, 2013	C12	Rejection of an application for a patent	
Jun 1, 2011	C41	Transfer of the right of patent application or the patent right	
Jun 1, 2011	ASS	Succession or assignment of patent right	**Effective date:** 20110421 **Free format text:** FORMER OWNER: LIU YANG **Owner name:** BEIJING WALI NETWORK TECHNOLOGY CO., LTD.
Jun 1, 2011	COR	Bibliographic change or correction in the description	**Free format text:** CORRECT: ADDRESS; FROM: 100190 UNIT 604, 6/F, SATELLITE BUILDING, NO. 63, ZHICHUN ROAD, HAIDIAN DISTRICT, BEIJING TO: 100114 ROOM 2533, BUILDING 3, NO. 3, XIJING ROAD, BADACHU HIGH-TECH. PARK, SHIJINGSHAN DISTRICT, BEIJING
Aug 25, 2010	C06	Publication	

Electronic Acknowledgement Receipt

EFS ID:	22208784
Application Number:	14667353
International Application Number:	
Confirmation Number:	8845
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3
Receipt Date:	29-APR-2015
Filing Date:	24-MAR-2015
Time Stamp:	17:21:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	P007C11C3_Statement.pdf	118425 f0dc2d6d2b2317220d2d5ef81e35f96ecc932aec	no	3

Warnings:	
Information:	

2	Transmittal Letter	P007C11C3_IDSTransLtr.pdf	58126 ca10918170b2fed7117b6ecfe42399762878 75b1	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	IDS1.pdf	622625 4ea8ca498c7a8ab2ccf4aa4a18d722a2e6f0 5aa4	no	36
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	IDS2.pdf	619448 c7cadde46bc619bf235274fcc6bcb71fbe50 2bcf	no	27
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	IDS3.pdf	619067 18b25ccf3adafba49d3f7c57af58cf4319b1c 59c	no	31
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	IDS4.pdf	613707 fb5b4c16bad9742f9934b1947091cb64828 02985	no	8
Warnings:					
Information:					
7	Foreign Reference	2060.pdf	1082588 d731de97188a46d46fa00f136f87db05a28 d9044	no	10
Warnings:					
Information:					
8	Foreign Reference	2061.pdf	2061940 86232d632925d26176ca285a7928e3c5a3f 21baa	no	21
Warnings:					
Information:					
9	Foreign Reference	2062.pdf	907410 8e1e1537e7aa0c658cd339f06c2b1b63ab4 48ad0	no	12
Warnings:					
Information:					
10	Non Patent Literature	3039.pdf	1271520 5ff7631e8a8dfa2c00f75e44b77d86a2e971 9407	no	12
Warnings:					
Information:					

Total Files Size (in bytes):	7974856

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Gregory G. Raleigh

Application No./Patent No.: 14/667,353 Filed/Issue Date: March 24, 2015

Titled: Mobile Device With Common Secure Wireless Message Service Serving Multiple Applications

Headwater Partners I LLC, a Limited Liability Company

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 035246, Frame 0173, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe completed application form to the USPTO.Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/James E. Harris/	April 29, 2015
Signature	Date
James E. Harris	40013
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that yoube given certain informationin connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, pleasebe advised that: (1) the general authority forthe collection of thisinformation is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and(3) the principal purpose forwhich the information isused by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent applicationor patent. If you do not furnish the requested information,the U.S. Patent and Trademark Office may not be able to process and/or examineyour submission,which may result in termination of proceedings or abandonment of the applicationor expiration of the patent.

The informationprovided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the informationin order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an InternationalApplication filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, arecord may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from thissystem of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	not yet assigned
Serial No.:	14/667,353	Art Unit:	2431
Filed:	March 24, 2015	Conf. No.:	8845
Title:	Mobile Device With Common Secure Wireless Message Service Serving Multiple Applications		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 14/263,604 filed April 28, 2014, of which the instant application is a continuation. Any foreign or non-patent references not submitted in that parent application are transmitted herewith.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **50-5876**.

Respectfully submitted,

Date: April 29, 2015

By: /James E. Harris/
James E. Harris
Reg. No. 40,013
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood City, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Apr. 29, 2015 By: /Ann Taylor/
Ann Taylor

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
JUN 05 2015
OFFICE OF PETITIONS

HEADWATER PARTNERS I LLC
555 TWIN DOLPHIN DRIVE, SUITE 310
REDWOOD SHORES CA 94065

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 14/667,353

1. THE REQUEST FILED 3/24/15 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an 1application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Cheryl Gibson-Baylor at (571)272-3213, Office of Petitions. In his/her absence, calls may be directed to Brian W. Brown, (571)272-5338.

Cheryl Gibson-Baylor
/Cheryl Gibson-Baylor/
[*Signature*]

Petitions Paralegal Specialist
(Title)

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6578076	B1	2003-06-10	Putzolu, David Matthew	
	2	7084775	B1	2006-08-01	Smith, Michael R.	
	3	7133695	B2	2006-11-07	Beyda, William J.	
	4	7260382	B1	2007-08-21	Lamb et al.	
	5	7271765	B2	2007-09-18	Stilp et al.	
	6	7627872	B2	2009-12-01	Hebeler et al.	
	7	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	8	7685530	B2	2010-03-23	Sherrard et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	7760137	B2	2010-07-20	Martucci et al.	
	10	7843843	B1	2010-11-30	Albert L. Papp et al.	
	11	7925778	B1	2011-04-12	Wijnands et al.	
	12	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	13	7937450	B2	2011-05-03	Janik, Craig M.	
	14	8010082	B2	2011-08-30	Sutaria et al.	
	15	8019846	B2	2011-09-13	ROELENS et al.	
	16	8050705	B2	2011-11-01	Sicher et al.	
	17	8086791	B2	2011-12-27	Caulkins, Jason	
	18	8103285	B2	2012-01-24	Kalhan, Amit	
	19	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	20	8233433	B2	2012-07-31	Kalhan, Amit	
	21	8259692	B2	2012-09-04	Bajko, Gabor	
	22	8406736	B2	2013-03-26	Das et al.	
	23	8489110	B2	2013-07-16	Frank et al.	
	24	8495181	B2	2013-07-23	Venkatraman et al.	
	25	8532610	B2	2013-09-10	Manning Cassett et al.	
	26	8571598	B2	2013-10-29	Valavi, John J.	
	27	8634425	B2	2014-01-21	Gorti et al.	
	28	8739035	B2	2014-05-27	Trethewey, Jim	
	29	8825109	B2	2014-09-02	Montemurro et al.	
	30	8831561	B2	2014-09-09	Sutaria et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	31	8880047	B2	2014-11-04	Konicek et al.	
	32	8930238	B2	2015-01-06	Coffman et al.	
	33	8977284	B2	2015-03-10	Reed, Mark J.	
	34	9014973	B2	2015-04-21	Ruckart, John	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070293191	A1	2007-12-20	Mir et al.	
	5	20070294410	A1	2007-12-20	Pandya et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	6	20080050715	A1	2008-02-28	Golczewski et al.	
	7	20080282319	A1	2008-11-13	Fontijn et al.	
	8	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	9	20100151866	A1	2010-06-17	Karpov et al.	
	10	20110145920	A1	2011-06-16	Mahaffey et al.	
	11	20130326356	A9	2013-12-05	Zheng et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	3	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	4	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-06-26
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710123501.9

[43] 公开日 2008 年 12 月 31 日

[11] 公开号 CN 101335666A

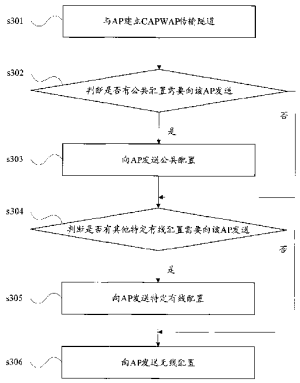
[22] 申请日 2007.6.29
[21] 申请号 200710123501.9
[71] 申请人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地
[72] 发明人 史 扬 张志飞
[74] 专利代理机构 北京挺立专利事务所
代理人 龚家骅
权利要求书 3 页 说明书 13 页 附图 4 页

[54] 发明名称

一种配置发送的方法、接入控制设备和接入点

[57] 摘要

本发明公开了一种配置发送方法，包括如下步骤：接入点接入时，获取需要向所述接入点发送的至少一个配置文件，该配置文件中包括供接入点进行接入的配置信息；向接入点发送该配置文件。 本发明还提供了一种接入控制设备和接入点。 通过使用本发明，实现了 CAPWAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。



1、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

2、如权利要求 1 所述配置发送方法，其特征在于，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

3、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

4、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

5、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

6、一种配置发送方法，其特征在于，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

7、如权利要求 6 所述配置发送方法，其特征在于，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

8、如权利要求 6 所述配置发送方法，其特征在于，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

9、如权利要求 6 所述配置发送方法，其特征在于，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤：

接收所述接入控制设备发送的包括无线配置信息的协议消息；

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

10、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

11、如权利要求 10 所述配置发送方法，其特征在于，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

12、一种接入控制设备，其特征在于，包括：

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件；

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

13、如权利要求 12 所述接入控制设备，其特征在于，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

14、如权利要求 12 所述接入控制设备，其特征在于，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

15、一种接入点，其特征在于，包括:

终端获取模块，用于获取接入控制设备发送的至少一个配置文件;

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

16、如权利要求 15 所述接入点，其特征在于，所述终端配置模块进一步包括:

解析子模块，用于解析所述配置文件并获得可执行的配置命令;

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

17、如权利要求 15 所述接入点，其特征在于，还包括:

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

一种配置发送的方法、接入控制设备和接入点

技术领域

本发明涉及通信技术领域，尤其涉及一种配置发送的方法、接入控制设备和接入点。

背景技术

802.11 WLAN（Wireless Local Area Network，无线局域网）网络提供了一种局域网的无线连接服务。AP（Access Point，接入点）是无线局域网的一个重要组成设备，是一个无线收发设备，用于将从有线网络（例如 Internet）接收到的数据转换成无线信号发送，将接收到的无线信号转换成数据并转发到有线网络。

802.11 WLAN 网络目前已经广泛地应用于企业等用户。这些用户的 AP 设备数量多、安全敏感、对 Qos（Quality of Service，服务质量）有严格要求，需要有效地管理手段来保证网络可管理性，降低用户的操作管理成本。

针对企业用户的需求，IETF 组织成立了专门的 WG（Work Group，工作组）制定 CAPWAP（Configuration and Provisioning for Wireless Access Points，无效接入点控制与配置）协议草案，预计在很快将成为正式的标准。传统意义的 AP 如目前家庭普遍使用的 AP 设备，用于完成 802.11 协议定义的完整功能。CAPWAP WG 提出了 Fit AP 的概念，Fit AP 主要完成实时性功能如消息确认、发送 Beacon 帧等，而对 AP 的管理、用户认证等功能需要通过 AC（Access Controller，接入控制设备）协同完成。

CAPWAP 协议定义了 AP 和 AC 之间将建立控制和数据隧道来完成网络的控制和转发。在向无线用户提供接入之前，AC 必须完成对 AP 的参数配置以完成控制平面的建立。现有技术中 AC 向 AP 发送配置的流程如图 1 所示，包括:

步骤 s101、AP 向网络中广播 Discover Request（发现请求）消息，寻找

网络中存在的 AC。

此步骤为 AP 寻找 AC 的阶段。AP 以广播方式发送 Discover Request 消息，寻找网络中可以使用的 AC。

步骤 s102、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response（发现响应）消息。

AC 接收到 AP 的 Discover Request 消息后，向该 AP 发送 Discover Response 消息作为响应。

步骤 s103、AP 向 AC 发送 Join Request（加入请求）消息。

AP 接收到 AC 发送的 Discover Response 消息后，与该 AC 建立 DLTS（Datagram Transport Layer Security，数据报传输层安全性）连接，并向 AC 发送向 AC 发送 Join Request 消息。

步骤 s104、AC 向 AP 发送 Join Response（加入响应）消息。

AC 接收到 AP 的 Join Request 消息后，向该 AP 发送 Join Response 消息作为响应，通知 AP 可以开始对其提供服务。

步骤 s105、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s106～s107、AP 与 AC 之间通过 Configuration status request（配置状态请求）和 Configuration status Response（配置状态响应）消息进行交互，实现 AC 对 AP 的配置下发。

步骤 s108～s109、AP 与 AC 之间通过 Configuration Update Request（配置更新请求）和 Configuration Update Response（配置更新响应）消息进行交互，实现 AC 对 AP 的配置更新。

上述步骤 s106～s109 中，Configuration status request、Configuration status Response、Configuration Update Request 和 Configuration Update Response 消息中通过携带 TLV（Type Length Value，类项长度值）来实现对 Radio，WLAN service，Qos 等配置。CAPWAP 协议中定义的 TLV 格式如图 2 所示，其中 Type 项（16bit）和 Length 项（16bit）分别标识了 Value 一项中携带的内容和长度。

现有技术中这个配置方法主要是面向无线属性的配置，没有对有线相关属性的配置。而 WLAN 网络并不是一个独立于有线网络的另一个网络，特别

是当 AP 也进行本地数据转发，如即 CAWPAP 定义的 Local Bridge（本地桥接）模式），AP 需要知道整个网络中的 ACL（Access Control List，访问控制列表）、Qos 等策略。

如果对于有线相关的配置下发仍然通过扩展新的 TLV 方式来实现，必然增加很大工作量，而且 CAPWAP 要进行大量的 TLV 扩展。有线和无线配置紧密耦合的方式必然影响 CAPWAP 协议的扩展性。另外，在 TLV 的扩展上，特定的 TLV 扩展对应了特定的软件版本。而在配置时要求 AC 和 AP 同时支持相同版本的 TLV，如果 AC 和 AP 版本不配套将影响 TLV 配置的下发。因此在对 TLV 的扩展不是进行有线配置下发的有效方法。

发明内容

本发明要解决的问题是提供一种配置发送方法、接入控制设备和接入点，以实现 CAPWAP 协议下 AC 根据不同 AP 的需求向 AP 发送不同的有线和无线配置。

为达到上述目的，本发明实施例的技术方案提供一种配置发送方法，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

其中，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

其中，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

本发明实施例的技术方案还提供一种在接入控制设备上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入控制设备上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

其中，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

其中，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

其中，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤:

接收所述接入控制设备发送的包括无线配置信息的协议消息;

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

本发明实施例的技术方案还提供一种在接入点上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入点上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤:

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息;

向所述接入点发送所述配置文件。

其中，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

本发明实施例的技术方案还提供一种接入控制设备，包括:

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件;

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

其中，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

其中，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置

文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

本发明实施例的技术方案还提供一种接入点，包括：

终端获取模块，用于获取接入控制设备发送的至少一个配置文件；

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

其中，所述终端配置模块进一步包括：

解析子模块，用于解析所述配置文件并获得可执行的配置命令；

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

其中，还包括：

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

本发明实施例的技术方案还提供一种网络，包括前述的接入控制设备以及前述的接入点。

与现有技术相比，本发明具有以下优点：

实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

附图说明

图 1 是现有技术中 AC 向 AP 发送配置的流程图；

图 2 是现有技术中 CAPWAP 协议中定义的 TLV 格式示意图；

图 3 是本发明的实施例中配置发送方法的流程图；

图 4 是本发明的实施例中 CAPWAP 协议控制消息的格式示意图；

图 5 是本发明的实施例中 AC 与 AP 间配置发送的信令流程图；

图 6 是本发明的实施例中接入控制设备的结构示意图；

EX1060 - Page 554

图 7 是本发明的实施例中接入点的结构示意图。

具体实施方式

以下结合附图和实施例，对本发明的实施方式做进一步说明。

本发明中的实施例中，将AC向AP发送配置的过程分为了三个部分:

第一部分为向AP发送公共配置。该公共配置为所有的AP在配置时都会使用的相同配置，主要包括有线配置，也可能包括部分无线配置。对于这部分配置可以存储在一个公共配置文件中。

第二部分为向AP发送有线配置。

对于特定的AP，除了公共配置外，可能还存在其他特别的有线配置。该有线配置可以根据AC对不同AP的控制策略在配置内容上有所不同，因此需要保存为不同的配置文件。或因不同厂商的AP支持的配置命令格式不同，而需要保存为不同的配置文件。AC可以将使用同一配置格式及配置策略的配置保存在独立的配置文件中，并在需要时独立下发，从而管理支持不同配置方式的AP。

第三部分为向AP发送无线配置。

该部分即当前的CAPWAP协议过程，具体的，AC可以通过与AP的消息交互，如通过在Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response中携带相关的无线配置的TLV，实现无线配置的发送。

以上三个配置发送过程对于特定的AP不一定全部存在，如对于某些AP可能不需要进行公共配置的发送，对于另外的某些AP可能不需要进行特定有线配置的发送。

本发明的实施例中一种配置发送的方法以AC对AP依次进行公共配置、有线配置、无线配置的发送为例，其中公共配置和有线配置的发送位于AC与AP的Join过程后、通过Configuration Status Request/Configuration Status Response消息交互进行无线配置下发前。如图3所示，该配置发送包括以下步骤:

步骤s301、AC与AP建立CAPWAP隧道。

EX1060 - Page 555

步骤s302、AC判断是否有公共配置需要向AP发送，需要发送时进行步骤s303，否则进行步骤s304。

对于被管理的AP，像ACL，Qos等策略配置（一般称为全局配置），与该AC相连接的所有AP一般会共用相同的配置。这些配置，可以保存在一个公共配置文件中，如appublic.cfg，并在AP与AC建立CAPWAP隧道后，作为第一个配置下发给AP。

在该公共配置文件的格式上，可以采用文本文件txt的格式。在该文件中包括对不同的项的具体设置。例如在文件中，对于每一需要进行配置的公共配置中的内容，通过Type和Value项进行表示。其中Type项表示Value一项中所携带的内容的标识，Value项表示具体的配置内容。例如，假设在预先设置的公共配置编制规则中ACL的标识为4096，则需要在公共配置中进行ACL的设置时，将Type项设置为4096，并在Value项中携带需要向AP发送的ACL内容。AP在接收到该公共配置文件后，可以根据Type项的值得知该配置是对ACL的配置，并根据Value项的值对ACL进行配置。当然也可直接通过字符串对不同的配置内容进行标识，并通过Value项的值携带具体的配置。

步骤s303、AC向AP发送该公共配置。

在该公共配置的发送方式上，可以采取以下方式:

方式一: AC可以将appublic.cfg通过多个CFG Data request（配置数据请求）消息发送给AP。

每次AP收到消息后，向AC发送CFG Data response（配置数据响应）消息确认收到了配置。完成配置文件传输后，AP执行配置文件更新本地配置。

该CFG Data request消息和CFG Data response消息的格式可以参考现有CAPWAP协议中的控制消息的格式。现有CAPWAP协议中的控制消息的格式如图4所示，包括Message Type（消息类型）项、Sequence Number（顺序号）项、Message Element Length（消息信元长度）项、Flags（标识）项以及Message Element（消息信元）项。其中，通过Message Type项标识了控制消息的类型与功能，Sequence Number项用于对接收到的Request消息和返回的Response消息进行对应，Message Element Length项为Message Element项的长度，Flags项

EX1060 - Page 556

为0，Message Element项为控制消息的相关具体内容。对于Message Type项，现有的CAPWAP协议中已经对一些控制消息进行了定义，如1代表Discovery Request消息，2代表Discovery Response消息等，因此通过扩展该Message Type项并使用新的标识，可以对CFG Data Request和CFG Data Response消息进行定义。

进行消息类型的定义后，AC可以根据和AP预先约定的发送方式，将公共配置向AP发送，例如AC约定每次向AP发送1000bit的内容，则AC将公共配置文件中前1000bit的内容添加在CFG Data Request消息中向AP发送，并在消息的末尾设置标识位。AP接收该CFG Data Request消息完毕后，向AC发送CFG Data Response消息作为响应。接收到该消息后，AC继续向通过CFG Data Request消息向AP发送公共配置，直至所有的公共配置发送完成。

方式二：AC可以通知AP通过其他协议，如tftp（Trivial File Transfer Protocol，普通文件传输协议）协议或ftp（File Transfer Protocol，文件传输协议）协议来获得公共配置。具体的，AC可以通知AP存储有该公共配置文件的tftp或ftp服务器的地址，以及可能需要的登录密码，由AP登录该tftp或ftp服务器，下载配置文件后，执行该配置文件更新本地配置。

步骤s304、AC判断是否有其他特定有线配置需要向该AP发送，需要发送时进行步骤s305，否则进行步骤s306。

除了公共配置外，对于特定的AP还可能还有其他特定有线配置。这些配置并不属于公共配置，可以保存在一个独立的配置文件，该配置文件名称可以对应AP的标示，如AP + AP序列号.cfg。

这些独立的配置文件可以保证系统的兼容性，例如当网络中出现不同厂商的AP，而这些AP支持不同的配置方式（配置文件格式）。系统可以把这些AP的配置保存在各自独立的配置文件中。通过这些不同AP配置的独立下发，可以实现AC同时管理来不同厂商的AP。

步骤s305、AC向AP发送该有线配置。

在该有线配置的发送方式上，可以参考步骤s303中AC在发送公共配置时所采取的不同发送方式。AP在接收到该有线配置文件后，执行该配置文件更

新本地配置。至此，AP完成了公共配置和有线配置的流程。

步骤s306、AC向AP发送无线配置。

该步骤中，通过当前CAPWAP协议中已经定义的与无线相关配置对应的TLV，AC与AP交互Configuration status request、Configuration status Response、Configuration Update Request或Configuration Update Response等消息实现对Radio、WLAN service、Qos等与无线相关的配置。AP收到配置后，更新本地无线配置。至此，AC向AP发送配置的流程结束。

上述实施例中AC对AP依次进行公共配置、有线配置、无线配置的信令流程图如图5所示，

步骤 s501、AP 向网络中广播 Discover Request 消息，寻找网络中存在的 AC。

步骤 s502、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response 消息。

步骤 s503、AP 向 AC 发送 Join Request 消息。

步骤 s504、AC 向 AP 发送 Join Response 消息。

步骤 s505、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s506～s507、AC 与 AP 之间通过 CFG Data Request 和 CFG Data Response 消息进行交互，实现公共配置和特定有线配置的下发。

步骤 s508～s509、AP 与 AC 之间通过 Configuration status request 和 Configuration status Response 消息进行交互，实现 AC 对 AP 的无线配置下发。

步骤 s510～s511、AP 与 AC 之间通过 Configuration Update Request 和 Configuration Update Response 消息进行交互，实现 AC 对 AP 的无线配置更新。

在上述实施例中，以AC对AP依次进行公共配置、有线配置、无线配置的下发为例，描述了本发明中一种发送配置的方法。该配置发送的顺序主要是基于一般情况下发送配置的顺序，即先公共配置后特定配置、先有线配置后无线配置。但是，在发送配置时所采用的顺序不限于以上顺序。另外，在不同的配置发送步骤，还需要考虑不同配置间的关系。以上述实施例为例，AC需要考虑对于某些AP只发送其特定的有线配置即可，而不需要下公共配置。

另外，在公共配置与特定的有线配置存在冲突时，应该通过设定优先级关系或修改配置文件以达到避免配置冲突的问题。

通过使用上述实施例中提供的配置发送方法，实现了CAWPAP能够灵活支持新的配置下发需求，特别是ACL，Qos等有线相关的配置需求，保证CAPWAP协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展TLV带来的繁琐的工作。

本发明的另一实施例中，提供了一种接入控制设备，如图6所示，包括:

配置存储模块10，用于存储需要向AP发送的配置文件。该配置文件具体为：包括公共配置信息的公共配置文件，以及包括特定有线配置的有线配置文件。其中，公共配置文件一般只有一个，其中主要包括有线配置，也可能同时包括无线设置。而有线配置文件可能很多，其文件个数由所需要的不特定有线配置的数量而定，不同的特定有线配置存储在不同的有线配置文件中。在具体的实现中，该存储模块10可能为AC上的存储实体，也可能为AC之外的tftp或ftp服务器等存储实体。

配置获取模块20，用于对不同的AP的状态，获取需要向该AP发送的公共配置和/或有线配置。并将需要向该AP发送的公共配置和/或特定有线配置通知配置发送模块30。

配置发送模块30，用于在接收到配置获取模块20发送的需要向AP发送的公共配置或特定的有线配置时，向AP发送该公共配置或特定的有线配置。发送方式从配置存储模块10中获取需要发送的内容并通过CFG Data Request消息发送；或在配置存储模块10为外部tftp或ftp服务器等存储实体时，通知AP该存储该公共配置或特定有线配置的服务器的地址。

接收模块 40，用于当配置发送模块 30 通过 CFG Data Request 消息发送有线配置时，接收接入点响应的 CFG Data Response 消息。并通知配置发送模块30，以继续公共配置或特定有线配置的发送直至完成。

本发明的另一实施例中，还提供了一种接入点，如图7所示，包括:

终端获取模块 50，用于接收接入控制设备发送的配置文件。获取方法可以为接收接入控制设备发送的 CFG Data Request 消息，或从接收接入控制设

EX1060 - Page 559

备通知的网络设备通过 tftp 或 ftp 协议获取。

终端配置模块 60，用于根据终端获取模块 50 接收到的配置文件，更新本地的配置。该模块进一步包括解析子模块 61，用于解析配置文件并获得可执行的配置命令；以及处理子模块 62，用于根据解析子模块 61 获得的配置命令更新本地的配置。

终端发送模块 70，用于终端获取模块 50 完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向接收接入控制设备响应 CFG Data Response 消息。

通过使用以上实施例所提供的接入控制设备和接入点，实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

以上方式中，仍然是通过在 Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response 中携带相关的无线配置的 TLV，实现无线配置的发送。这样做可以和现有的 CAPWAP 协议相兼容，然而，无线配置部分同样可以纳入到公共配置和特定配置中来，无线配置不再特殊化处理，可以统一到一个公共配置及各个特有配置中，而各个特有配置也不在局限为特定有线配置。本发明通过将各种配置纳入到一个或者多个配置文件中然后下发给 AP，AP 接收以后解析这些文件获取其中的配置命令完成配置工作。其通过一次开发就可以解决以后所有新增配置的问题，因为无论新增什么配置，只需要把它纳入到配置文件中即可，AP 就可以通过解析文件获得配置。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实

EX1060 - Page 560

施例所述的方法。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

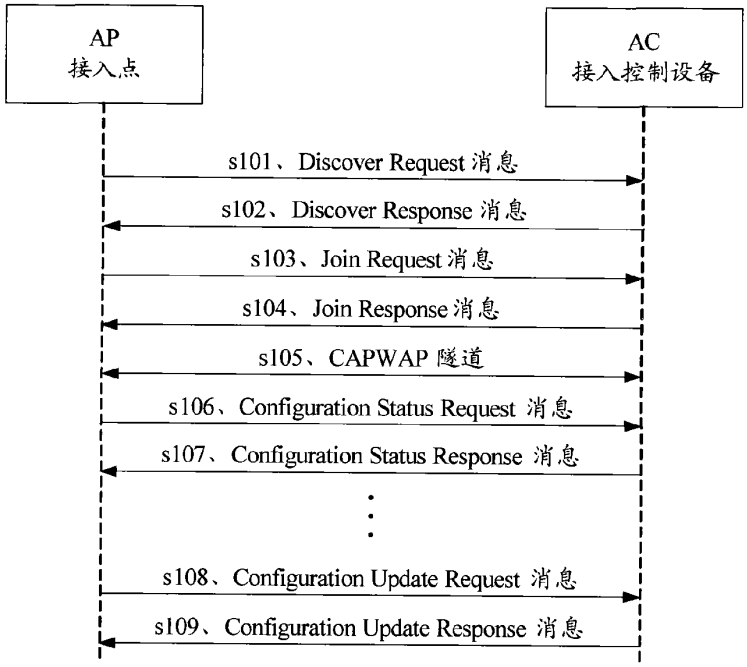

AP
接入点
AC
接入控制设备
s101、Discover Request 消息
s102、Discover Response 消息
s103、Join Request 消息
s104、Join Response 消息
s105、CAPWAP 隧道
s106、Configuration Status Request 消息
s107、Configuration Status Response 消息
s108、Configuration Update Request 消息
s109、Configuration Update Response 消息

图 1

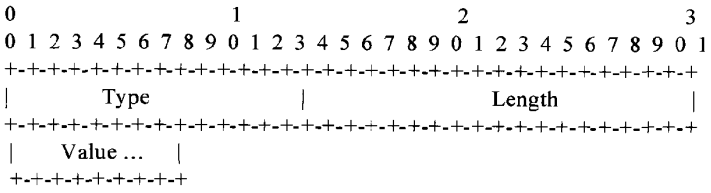

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Value ...

图 2

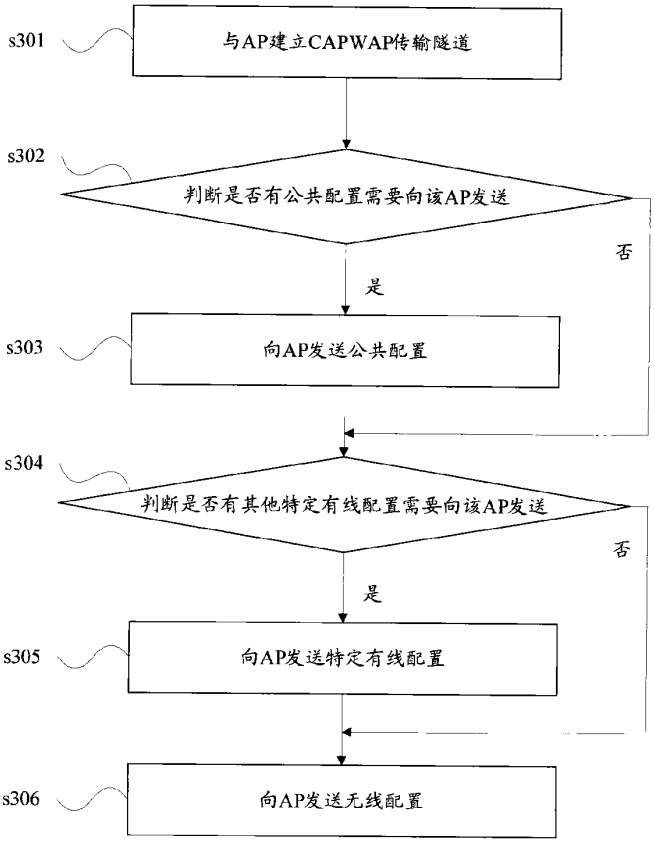


图 3

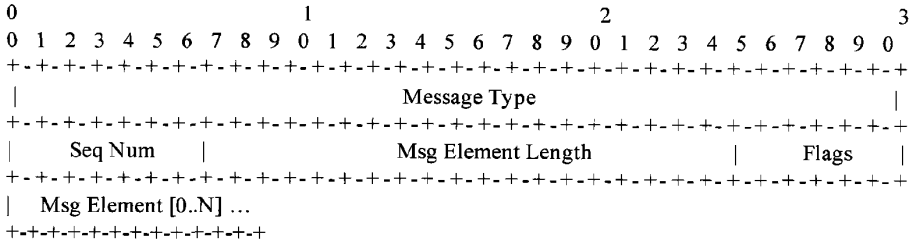


图 4

EX1060 - Page 563

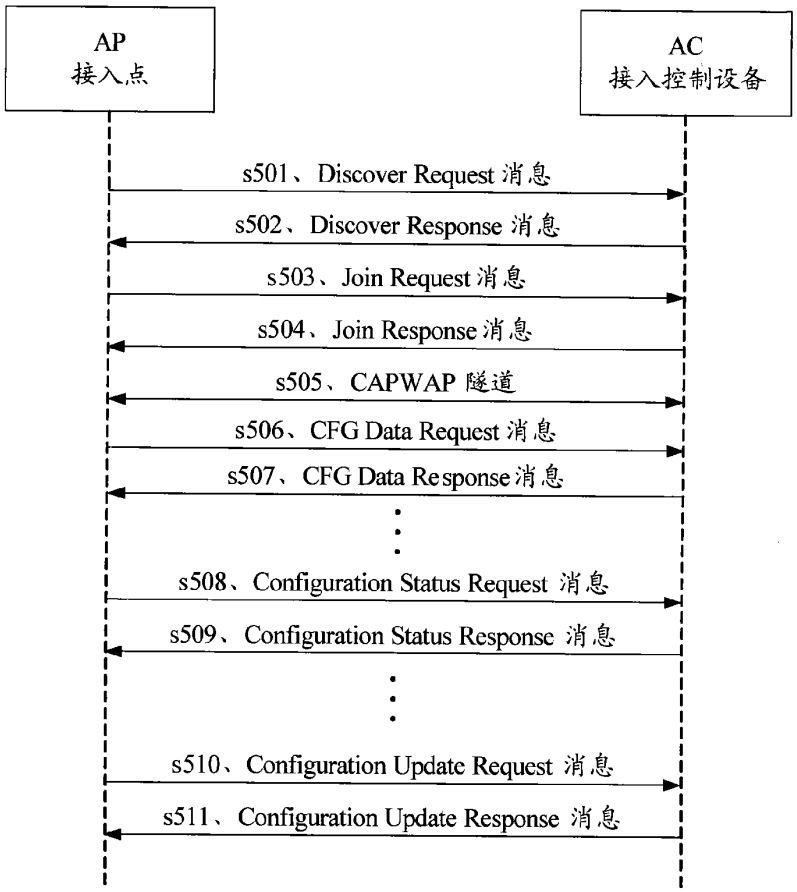

AP
接入点
AC
接入控制设备
s501、Discover Request 消息
s502、Discover Response 消息
s503、Join Request 消息
s504、Join Response 消息
s505、CAPWAP 隧道
s506、CFG Data Request 消息
s507、CFG Data Response 消息
s508、Configuration Status Request 消息
s509、Configuration Status Response 消息
s510、Configuration Update Request 消息
s511、Configuration Update Response 消息

图 5

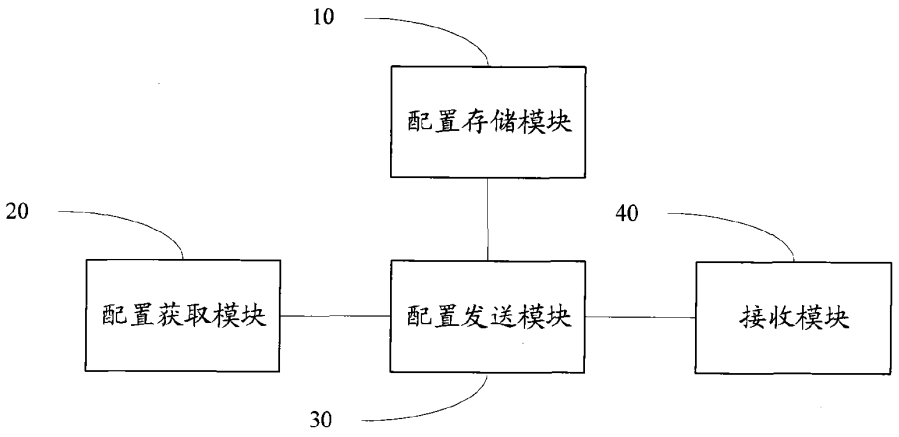


图 6

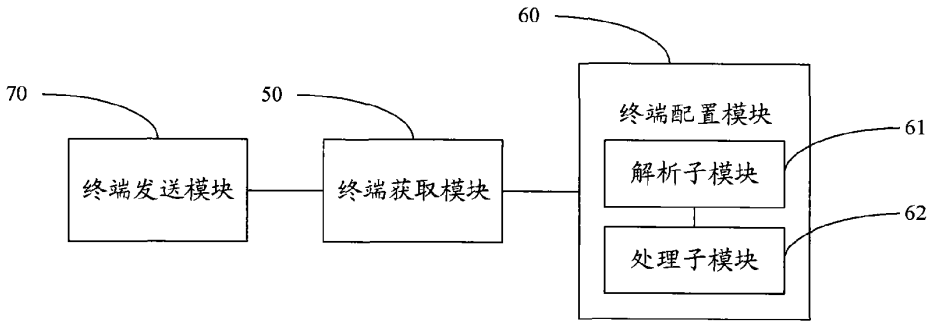


图 7

EX1060 - Page 565

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04M 1/247 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610157819.4

[43] 公开日 2007 年 11 月 28 日

[11] 公开号 CN 101080055A

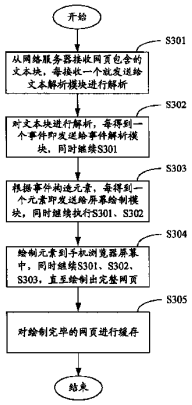
[22] 申请日 2006.12.21
[21] 申请号 200610157819.4
[71] 申请人 腾讯科技（深圳）有限公司
地址 518057 广东省深圳市高新科技园南区高新南一道飞亚达高科技大厦 5－10 层
[72] 发明人 纪 宇
[74] 专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 郭伟刚 蔡晓红
权利要求书 4 页 说明书 12 页 附图 3 页

[54] 发明名称

一种基于手机浏览器快速浏览网页的方法、系统及设备

[57] 摘要

本发明涉及移动通信领域，提供了一种基于手机浏览器快速浏览网页的方法、系统及设备。 所述方法包括以下步骤：A. 所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给文本解析模块；B. 对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块，同时继续执行步骤 A；C. 根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤 A 和 B；D. 每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤 A、B、C，直至绘制出完整网页。 本发明提高了手机浏览器浏览网页时的显示效率。



1、一种基于手机浏览器快速浏览网页的系统，包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

2、根据权利要求1所述的基于手机浏览器快速浏览网页的系统，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

3、一种手机浏览器，包括网络收发模块、文本解析模块、事件处理模块

和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

4、根据权利要求3所述的手机浏览器，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

5、根据权利要求3或4所述的手机浏览器，其特征在于，所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

6、一种基于手机浏览器快速浏览网页的方法，其特征在于，所述方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A；

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B；

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

7、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤B中对文本块进行解析并得到对应事件的过程包括：

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件；

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件；

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件；

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

8、根据权利要求7所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤C中根据事件构造元素的过程包括：

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点；

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前

游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

9、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

10、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

一种基于手机浏览器快速浏览网页的方法、系统及设备

技术领域

本发明涉及移动通信领域，更具体地说，涉及一种基于手机浏览器快速浏览网页的方法、系统及设备。

背景技术

随着因特网和移动通信技术的发展和融合，利用手机浏览器浏览网页已日益普及。

现有技术实现手机浏览器浏览网页所采取的方式是，首先下载完显示网页所需的全部文本及图片信息，然后在浏览器中统一显示。由于该现有技术的下载方式受限于网络速度，往往会导致网页显示得非常慢。

另一现有技术则采取将文本图片分步下载并显示的方式，也即：首先下载完文本文件，显示文本文件，然后下载图片，最后再显示完整的网页。该现有技术相对于前一技术，在网页显示效率方面有所提高，但仍不乐观。

因此需要一种新的方法，能够通过手机浏览器快速浏览网页。

发明内容

本发明的目的在于提供一种基于手机浏览器快速浏览网页的系统，旨在解决现有技术在利用手机浏览器浏览网页时显示效率低下的问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的设备，以更好地解决现有技术中存在的上述问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的方法，以更好地解决现有技术中存在的上述问题。

为了实现发明目的，所述基于手机浏览器快速浏览网页的系统包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括：

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块；

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

为了更好地实现发明目的，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事

件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

为了更好地实现发明目的，所述基于手机浏览器快速浏览网页的方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A;

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B;

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

所述步骤B中对文本块进行解析并得到对应事件的过程包括:

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件;

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件;

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件;

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

所述步骤C中根据事件构造元素的过程包括:

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点;

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

本发明通过将文本流转换成事件流，并利用手机浏览器中的各个模块以并行的方式对各事件进行解析、处理和绘制，从而提高了手机浏览器浏览网页时的显示效率；另外将所绘制的网页以对象树的形式进行缓存，进一步提高了网页的显示效率；此外还通过检查内存和进行流量控制，保证了浏览的安全性。

附图说明

图1是本发明中基于手机浏览器快速浏览网页的系统结构图;

图2是本发明中基于手机浏览器快速浏览网页的实现示意图;

图3是本发明中基于手机浏览器快速浏览网页的方法流程图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

在本发明中，手机浏览器利用其网络收发模块从网络服务器接收网页包含的文本块，且每接收到一个文本块就将其发送给手机浏览器中的文本解析模块；文本解析模块对所接收到的文本块进行解析，得到与文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收

文本块；事件处理模块根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素，直至绘制出完整网页。这种并行处理的方式极大地提高了手机浏览器浏览网页时的显示效率。

图1示出了本发明中基于手机浏览器快速浏览网页的系统结构，包括手机浏览器100和网络服务器200。

其中网络服务器200用于存储网络数据，并当用户通过手机浏览器100发送网页访问请求时，将该网页所包含的网络数据以文本块的形式返回给手机浏览器100。

手机浏览器100包括网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104和缓存管理模块105，其中：

（1）网络收发模块101与网络服务器200之间进行通信，当用户期望浏览一个网页时，其根据用户的操作发送网页访问请求给网络服务器200，并接收返回的文本块形式的网页数据，然后将网页数据的这些文本块转发至文本解析模块102中进行处理。

（2）文本解析模块102与网络收发模块101和事件处理模块103相连，用于对网络收发模块101转发的文本块进行解析，得到相应的事件。本发明中并不是在网络收发模块101接收完网页的所有数据之后才将其发送到文本解析模块102中进行解析，而是在网络收发模块101接受完第一文本块之后就将其发送给

文本解析模块102，文本解析模块102立刻解析该第一文本块，得到与其对应的第一事件。在文本解析模块102对第一文本块进行解析的同时，网络收发模块101继续接收其他文本块。

（3）事件处理模块103与文本解析模块102、屏幕绘制模块104相连，用于对文本解析模块102解析得到的事件进行进一步处理，构造出与事件对应的元素。本发明中也并不是在文本解析模块102解析完所有的文本块之后才开始进行事件处理，而是在文本解析模块102解析得到第一事件之后就将该第一事件发送给事件处理模块103，事件处理模块103立刻处理该第一事件，构造其对应的第一元素。在事件处理模块103构造第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析。

（4）屏幕绘制模块104与事件处理模块103和缓存管理模块105相连，用于将事件处理模块103构造得到的元素绘制到手机浏览器100的屏幕上，直至最终绘制出完整的网页。本发明中也并不是在事件处理模块103构造出所有元素之后才开始进行绘制，而是在事件处理模块103构造出第一元素之后就将该第一元素发送给屏幕绘制模块104，屏幕绘制模块104立刻对该第一元素进行判断，若该第一元素的Rect值与屏幕Rect存在交集，则将该第一元素绘制到手机浏览器100的屏幕上。在屏幕绘制模块104绘制第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析，以及事件处理模块103继续构造其他元素。按照以上的并行处理方式，最终可快速地绘制出完整网页。

关于网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104相互协作并行处理的具体过程，可参考附图2。

（5）缓存管理模块105与屏幕绘制模块104相连，用于缓存屏幕绘制模块

104所绘制出的网页的对象树，当用户再次访问该网页时则可根据该缓存管理模块105中的网页的对象树进行显示，进一步加快了网页显示的效率。

图2是本发明中基于手机浏览器100快速浏览网页的实现示意图。由该图可知，本发明中接收、解析、构造元素、绘制这四个步骤并不是单纯的串行处理：

各个模块内部所执行的操作是串行的，例如，网络收发模块101按时间顺序以串行方式接收各个文本块，文本解析模块102按时间顺序以串行方式对各个文本块进行解析并得到相应的事件，事件处理模块103按时间顺序以串行方式根据各个事件构造对应的元素，屏幕绘制模块104按时间顺序以串行方式将各元素绘制到手机浏览器100屏幕中的相应位置。

但是在整体上，各个模块对不同文本块的处理过程却是并行的，在本发明的其中一个实施例中，以图2进行说明如下：网络收发模块101接收到第一文本块并发送给文本解析模块102；当文本解析模块102对该第一文本块进行解析以得到第一事件的同时，网络收发模块101在接收第二文本块；当事件处理模块103根据第一事件构造第一元素的同时，网络收发模块101有可能正在接收第三文本块，且文本解析模块102则在对第二文本块进行解析；当屏幕绘制模块104将第一元素绘制到屏幕上的同时，网络收发模块101有可能正在接收第四文本块，且文本解析模块102则在对第三文本块进行解析，以及事件处理模块103正在根据第二事件构造第二元素。

利用以上的并行处理方式，可极大地提高网页显示的速度。例如，现有技术中显示一张网页时，需10秒钟读取完该网页包含的全部网络数据，3秒钟进行解析，3秒钟根据解析得到的事件构造出所有元素，5秒钟完成显示，则显示出来需要21秒。而在本发明中，若手机屏幕是128*128像素，用户访问的网页

经过排版后128像素宽、1024像素高，网络收发模块101只需要2秒钟左右可以读取128像素宽、128像素高的内容，其将此内容传递给文本解析模块102，文本解析模块102利用1秒钟完成解析，事件处理模块103用1秒钟构造元素，屏幕绘制模块104只需2秒钟完成绘制并显示，这样便只需要6秒钟就可以显示完占满用户手机屏幕的内容，在用户阅读内容的同时，继续作后续内容的收取、解析、构造和绘制显示。

图3示出了本发明中基于手机浏览器100快速浏览网页的方法流程。

在执行所有步骤之前，当用户期望浏览一个网页时，则通过手机浏览器100发送网页访问请求，该网页访问请求通过手机浏览器100中的网络收发模块101发送至网络服务器200。

在步骤S301中，网络收发模块101接收网络服务器200返回的上述网页包含的HTTP数据，这些数据以文本块的形式传送给网络收发模块101，网络收发模块101再将所接收到的文本块转发至文本解析模块102中。本发明中网络收发模块101并不是接收完网页的全部数据之后才将其发送，而是每接收到一个文本块则将其发送给文本解析模块102进行处理，同时网络收发模块101继续接收该网页的其他文本块。步骤S301的具体过程包括：若网络收发模块101收取到一个新的网页文档，则产生一个新文档（new Document）事件，自身继续收取文档。本发明中，网络收发模块101收取到一个文本块，则产生一个新文本块（new Document Block）事件，并将其立即发送给文本解析模块102进行解析。收取完所有文本块，则产生一个结束文档（end Document）事件，结束自己的线程。

在步骤S302中，文本解析模块102每次接收到网络收发模块101发送过来的文本块之后，则立刻对其进行解析，得到与该文本块对应的事件，且每解析得

到一个事件即发送至事件处理模块103中，同时继续执行步骤S301接收其他文本块。步骤S302中解析的具体过程包括：（1）对所接收到的文本块进行检测，当检测到一个文档开始标记（如<html>）时，则产生一个开始文档树事件；（2）继续检测到一个Tag开始标记（如<body>）时，则产生一个开始元素事件；（3）继续检测到一个Tag结束标记（如</body>）时，则产生一个结束元素事件；（4）当检测到一个文档结束标记（如</html>）时，则产生一个结束文档树事件。完成上述解析，则得到文本块对应的事件，并将该事件发送给手机浏览器100的事件处理模块103进行处理。在本发明的一个实施例中，若由于网络传输等因素造成网络收发模块101所接到到的是非完整性文档，如一个文档有5K字节，网络中断导致网络收发模块101仅收取了3K，则当文本解析模块102在对其进行解析时也将产生结束文档树事件，并通知事件处理模块103解析结束。

在步骤S303中，事件处理模块103根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块104中，同时继续执行步骤S301接收其他文本块，以及继续执行步骤S302对所接收到的文本块进行解析。步骤S303中根据事件构造元素的具体过程包括：（1）当事件处理模块103收到文本解析模块102发送的开始文档树事件，则新建一个文档树，并设置当前游标为该文档树的根节点；（2）当事件处理模块103继续接收到文本解析模块102发送的开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点；（3）当事件处理模块103继续接收到文本解析模块102发送的结束元素事件，则对游标元素进行排版，计算出游标元素的Rect，并同时更新此结点的父结点、爷爷结点直至根节点的Rect，如该游标元素的Rect与屏幕Rect（SR）存在交集，则产生一个绘制元素事件，同时调整游标，将游标节点的父结点设置为当前游标节点；（4）当事件处理模块103继续接收到文本解析模块102发送的结束文

档树事件，则结束当前线程，并将所生成的元素发送到手机浏览器100的屏幕绘制模块104中进行绘制。

在步骤S304中，屏幕绘制模块104每接收到事件处理模块103发送的一个绘制元素事件及相应的元素，就将该元素绘制到手机浏览器100屏幕上的对应位置，同时继续执行步骤S301、S302、S303，直至绘制出完整网页。关于对每一个元素进行绘制的具体过程，可参考现有技术。

如上所述，以上步骤S301、S302、S303、S304的执行过程，并不是一个简单的串行过程，在整体上是一个并行处理的过程，在一个步骤执行的同时其他步骤对应的线程也在运行，这样可在最短的时间内绘制出网页并显示给用户。

此外，在步骤S305中，当屏幕绘制模块104绘制出完整网页后，则将该网页的对象树存入缓存管理模块105中，这样当用户再次访问该网页时，则可直接提取该对象树显示出网页，进一步提高了效率。

本发明在实现快速浏览网页的同时，还考虑到安全浏览问题。由于手机在访问内容较多的互联网网页时，很可能会因为网页太大或者手机内存资源受限而造成手机浏览器100程序死机。为了解决这个问题，本发明提供了两种方法：

（1）引入内存检测（Check Memory）机制：在每个需要花费大量内存空间的函数入口都执行该内存检测机制，且在每一次申请内存时，都检查是否申请成功。如果内存检测的返回结果是“出错”（false），说明手机空余内存不足，或者申请内存失败，此种情况下应首先释放缓存，设置已经释放的标志，再回调到失败的函数本身。如果已经释放缓存仍然在内存检测时返回false，则产生内存不足错误，并且提示用户。

（2）在手机浏览器100中引入流量控制，典型的例如，可允许用户在手机浏览器100中设置三种流量控制模式：系统控制，限定单张网页最大流量，以及不下载图片。当用户选择“系统控制”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与系统预设的允许大小值，如果大于系统预设的允许大小值，则不下载；当用户选择“限制单张网页最大流量”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与用户设定的单张网页最大流量，大于用户设定值，则不下载；当用户选择“不下载图片”时，则不下载所有图片。

应当作出说明的是，本发明典型的应用但是并不限于在手机浏览器中浏览网页的情形，基于其他相关或类似的电子设备浏览网页时，也可以采用本发明的上述方法。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

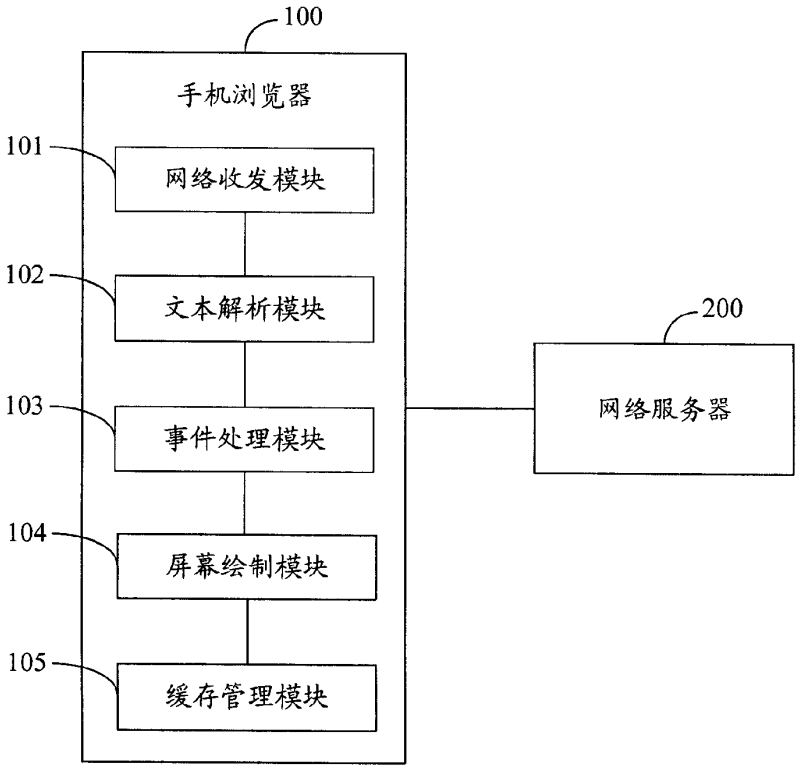

100
手机浏览器
101
网络收发模块
102
文本解析模块
103
事件处理模块
104
屏幕绘制模块
105
缓存管理模块
200
网络服务器

图 1

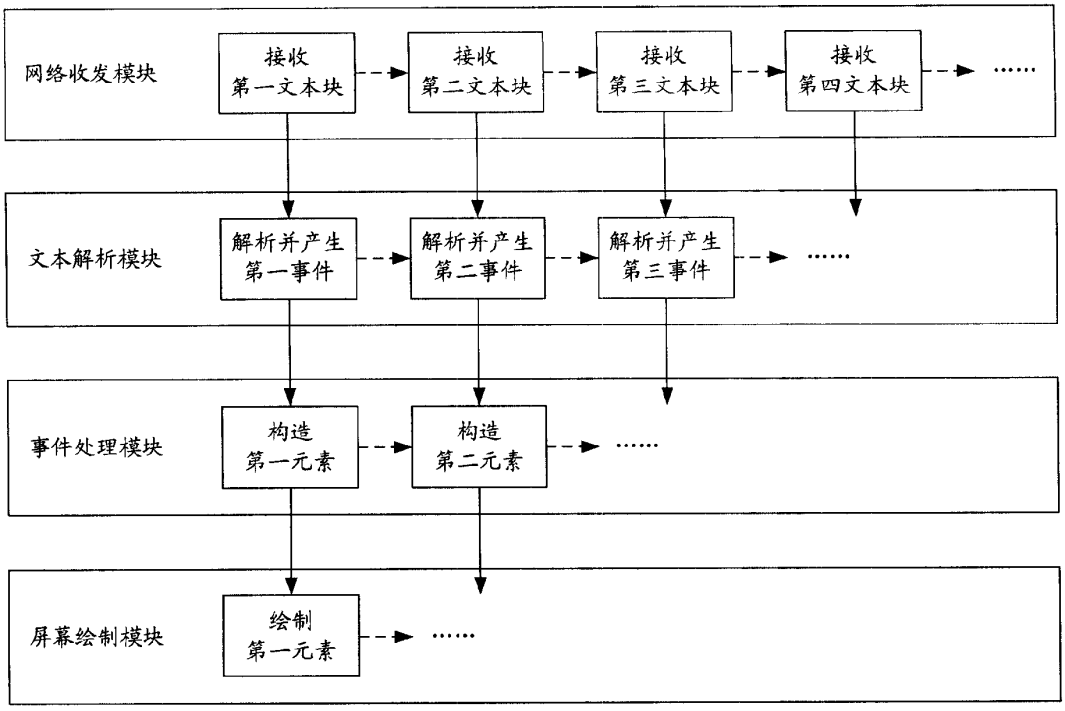

网络收发模块
接收
第一文本块
接收
第二文本块
接收
第三文本块
接收
第四文本块
……
文本解析模块
解析并产生
第一事件
解析并产生
第二事件
解析并产生
第三事件
……
事件处理模块
构造
第一元素
构造
第二元素
……
屏幕绘制模块
绘制
第一元素
……

图 2

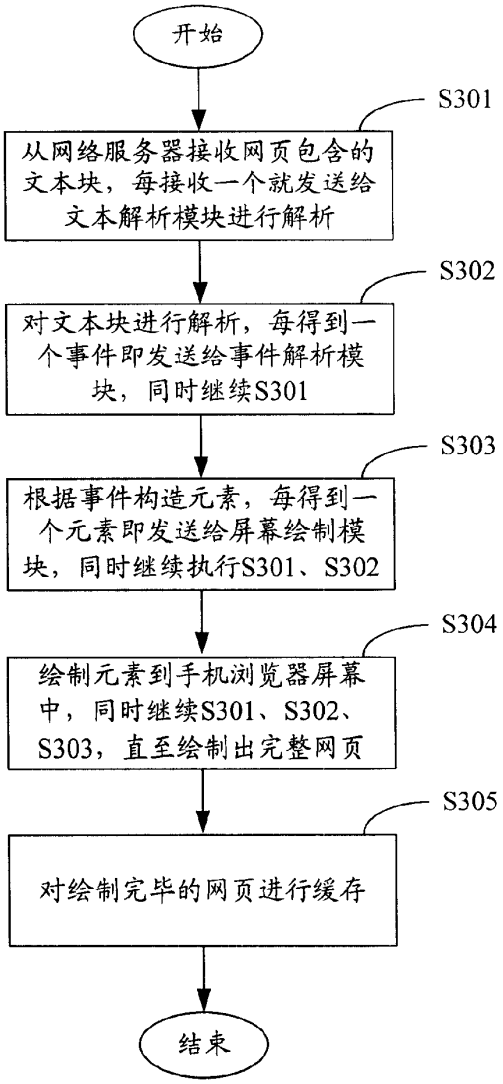

开始
S301
从网络服务器接收网页包含的文本块，每接收一个就发送给文本解析模块进行解析
S302
对文本块进行解析，每得到一个事件即发送给事件解析模块，同时继续S301
S303
根据事件构造元素，每得到一个元素即发送给屏幕绘制模块，同时继续执行S301、S302
S304
绘制元素到手机浏览器屏幕中，同时继续S301、S302、S303，直至绘制出完整网页
S305
对绘制完毕的网页进行缓存
结束

图 3

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/14
H04M 17/00

[12] 发明专利申请公开说明书

[21] 申请号 03137490.5

[43] 公开日 2005 年 1 月 19 日

[11] 公开号 CN 1567818A

[22] 申请日 2003.6.25 [21] 申请号 03137490.5

[71] 申请人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 张 庆 于 泽 严雪松

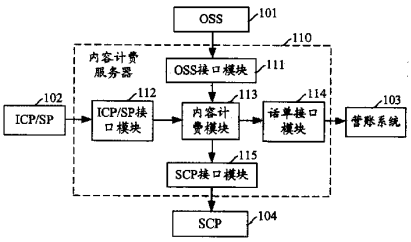
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 宋志强 王 琦

权利要求书 3 页 说明书 13 页 附图 1 页

[54] 发明名称 一种数据业务的内容计费方法及其计费系统

[57] 摘要

本发明公开了一种数据业务的内容计费方法，该方法将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/业务提供商(ICP/SP)获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。本发明同时公开了一种业务的内容计费系统，该系统由专用的内容计费服务器来实现，其包含运营支撑系统(OSS)接口模块、ICP/SP 接口模块、内容计费模块、付费接口模块。本发明的这种内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。



ISSN1008-4274

1、一种数据业务的内容计费方法，其特征在于，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

2、如权利要求1所述的内容计费方法，其特征在于，所述的步骤1）进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

3、如权利要求1所述的内容计费方法，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

4、如权利要求3所述的内容计费方法，其特征在于，所述的步骤3）包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

5、如权利要求4所述的内容计费方法，其特征在于：当对移动数据业务进行计费时，所述的预付费处理设备为业务控制节点（SCP）。

6、如权利要求4所述的内容计费方法，其特征在于：该方法进一步包括，

步骤3）获得的计费结果由营帐系统根据用户需要生成用户帐单。

7、一种数据业务的内容计费系统，其特征在于，该系统包含内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将ICP/SP与内容计费模块相连， ICP/SP将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。

8、如权利要求7所述的内容计费系统，其特征在于，所述的付费接口模块包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

9、如权利要求8所述的内容计费系统，其特征在于，所述的预付费接口模块为：业务控制节点（SCP）接口模块，将SCP与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给SCP。

10、如权利要求7所述的内容计费系统，其特征在于，所述的内容计费模块至少包含：

计费引擎，与OSS和ICP/SP分别相连，从OSS中获取签约数据业务用户的用户信息，接收ICP/SP发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据

EX1060 - Page 588

业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

11、如权利要求 7 所述的内容计费系统，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

12、如权利要求 8 所述的内容计费系统，其特征在于，所述的话单接口模块为话单接口机，其与内容计费模块通过以文件格式传输信息。

13、如权利要求 9 所述的内容计费系统，其特征在于：所述的内容计费服务器与 OSS 为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均按照运营商接口规范进行连接。

14、如权利要求 13 所述的内容计费系统，其特征在于，所述内容计费服务器与 ICP/SP 采用消息或文件方式进行交互；内容计费服务器与 SCP 之间采用扩展移动点到点协议（EMPP）协议消息进行交互。

15、如权利要求 8 所述的内容计费系统，其特征在于：话单接口模块与营帐系统以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

16、如权利要求 7 所述的内容计费系统，其特征在于，所述的内容计费服务器包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

一种数据业务的内容计费方法及其计费系统

技术领域

本发明涉及数据业务的计费技术，特别涉及一种数据业务的内容计费方法及其计费系统。

背景技术

目前，根据通用移动通信系统（UMTS）论坛报告9的分析，3G数据业务分成内容连接类和移动性类两大类，内容连接类可以划分成：移动Internet接入和企业Intranet/Extranet接入；移动性类可以划分成：客户化信息、娱乐；多媒体消息业务；基于位置的业务；另外还有增强话音共6类业务。

这6类业务代表了3G业务的主要需求。今天以话音为主宰的移动通信领域，将来一定会是一个以数据业务为中心的环境。在任何时间任何地点能够接入Internet的内容将明确成为3G的重要任务。

3G 计费是 3G 解决方案的一个重要组成部分。虽然 3G 业务是多种多样的，前景是诱人的，但如果没有相应的计费解决方案，不建立相应的价值链体系，即运行商无法运营，那么一切都是空谈。

目前传统的计费系统都是针对语音业务来设计的，一般根据呼叫持续的时间、主被叫的距离等因素进行计费。即传统计费与呼叫时长及主被叫位置相关，而与消费的业务内容无关。

目前的3G计费系统，仍然以语音业务的计费为主，其计费策略普遍采用硬编码的方式，即计费公式在代码中写死，一旦计费费率表确定，其计费算法也就相应固定。

硬编码方式的主要缺点在于代码重用性、灵活性差，如果增加新的需求则需要更改大量代码，代码间耦合性大，修改涉及面广，不易维护，也不利于计

费系统的稳定性。针对3G业务对计费灵活性的要求，此种实现方式显然不能满足。

另外一种方法是使用脚本的方式固化计费策略，使用脚本语言实现计费公式。使用脚本语言虽然可以非常灵活的增加新的计费策略，修改计费公式时也不必修改代码，但由于计费公式一般比较复杂，使用脚本实现有很大的困难、可读性很差。除此之外，对脚本语言的解释对系统性能也会产生一定的影响。

现有 3G 计费系统是由移动通信系统原有的设备整合来实现的，即计费功能融合在 SSP 或 SCP 中，由 SSP/SCP 完成对用户的计费功能。

传统的话音业务计费是和用户消费的内容无关的，只与时长（用户的通话时间）、距离（本地通话或长途）有关，因此不必上报业务信息或内容属性等，同时不关心用户消费业务的流量、次数，只需要在 SSP/SCP 侧统计用户的通话时间，由 SSP/SCP 完成对用户的计费功能后，由营帐系统根据计费结果，生成用户帐单，在用户需要时提交给用户。

3G 最吸引人的地方在于“永远在线”的服务，即只要打开手机就可以享受到丰富多采的业务内容，因此仅限于语音业务的传统计费系统明显不能满足多样化业务所带来的多样化内容计费的需求。因此传统的话音计费不能满足内容计费的需要。

且由于现有技术的计费系统通过移动通信系统原有的设备整合来实现，占用了移动通信系统的资源，计费过程繁琐，灵活性差，不能适应日益发展的丰富多采的数据业务的计费需要。

发明内容

有鉴于此，本发明的目的在于提供一种数据业务的内容计费方法，实现根据业务内容进行计费，满足数据业务中灵活多样的计费要求。

本发明的另一个目的在于提供一种数据业务的内容计费系统，节省移动通信系统资源，实现根据业务内容进行计费，满足数据业务中灵活多样的计

EX1060 - Page 591

费要求。

根据上述目的的一个方面，本发明提供了一种数据业务的内容计费方法，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

其中，所述的步骤 1）可以进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的步骤3）可以包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

当对移动数据业务进行计费时，所述的预付费处理设备可以为业务控制节点（SCP）。

根据上述目的的另一个方面，本发明提供了一种内容计费系统，该系统包含专用的内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中

获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将 ICP/SP 与内容计费模块相连， ICP/SP 将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。该付费接口模块可以包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

其中，所述的预付费接口模块可以为：业务控制节点（SCP）接口模块，将 SCP 与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给 SCP。

所述的内容计费模块至少可以包含：

计费引擎，与 OSS 和 ICP/SP 分别相连，从 OSS 中获取签约数据业务用户的用户信息，接收 ICP/SP 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的话单接口模块可以为话单接口机，其与内容计费模块通过以文件格

式传输信息。

所述的内容计费服务器与 OSS 可以为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均可以按照运营商接口规范进行连接。

所述内容计费服务器与 ICP/SP 可以采用消息或文件方式进行交互；内容计费服务器与 SCP 之间可以采用扩展移动点到点协议（EMPP）协议消息进行交互。

话单接口模块与营帐系统可以以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

所述的内容计费服务器可以包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

由本发明的技术方案可见，本发明的这种内容计费系统及其计费方法，将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

附图说明

图 1 为本发明一个较佳实施例的内容计费实现框图；

图 2 为图 1 所示实施例中内容计费模块的实现框图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明的这种数据业务的内容计费方法，是为了满足 3G 业务的特点，采用根据业务内容进行计费的方式。并根据计费需求的灵活多变，定制不同

的计费规则。也就是说，本发明能够根据计费规则定制不同的计费公式，对计费策略、折扣策略等实现灵活组合、易于扩充。

本发明的这种数据业务的内容计费方法，首先按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；同时预先保存签约数据业务用户的用户信息，该用户信息可以包括：用户开户信息、付费类型、用户属性、欠费记录等。

其中，在定制计费规则部件时，参考了下列因素：

A、不同 ICP/SP 可能有不同的计费策略；

B、不同业务可能有不同的资费策略，如游戏，不同游戏可能的收费不同；

C、支持按时长计费，如游戏，时间长短收费不同；

D、支持基于内容的流量计费，如下载图片，按照流量计费，但是费率根据不同的图片有所区别；

E、支持按使用次数计费（包括按条、按页面、按次计费），如下载图片、MP3、铃声等；

F、支持按时间段或日期采用不同的计费策略；如某些日期免费促销、每天的某些时间段访问给予一定折扣等；

G、支持平价计费、支持签约费（月租）+按使用次数或时长或流量等计费策略；

H、支持用户个性化的计费，不同用户可以根据自身情况选择不同的资费或计费策略；

I、支持随使用量不同（时长、流量、次数）采用不同的计费策略，其类似于跳档；

J、广告业务，支持用户访问ICP的广告送费服务，又可以分为赠送使用费和赠送使用量两种；

K、支持接入不同的数据网络采用不同的计费策略，考虑QoS等因素；

L、支持在不同区域或地区运用不同的计费策略，有可能在各“热点地区”

EX1060 - Page 595

向用户收费不同。比如，可以相对于“办公区”的概念，对“生活区”收取更低的费用；

M、支持封顶费用。

除此之外，折扣是SP和网络运营商吸引用户的非常重要的手段，无论是传统的语音业务，还是面向3G的移动数据业务，折扣的地位都是举足轻重的。折扣方式多种多样，目前普遍使用的折扣方式主要有以下几种：

a、时间段折扣——保留现有的日常、星期、节假日折扣方式。这种方式也可以扩展到按流量计费的计费模式中。

b、累计折扣——包括时长累计折扣、流量累计折扣、条目累计折扣、金额累计折扣等4种折扣方式。

c、一次累计折扣——按照一次使用总量、一次使用总金额折扣

d、用户折扣——对某种集团用户进行统一的折扣。可在所有折扣基础上累乘。

e、业务折扣——对某种业务进行统一折扣。

本发明在具体实施中根据上述因素，定制了多个计费规则部件。一种业务的计费可以通过批价部件和一个或多个计费规则部件来实现。计费规则部件可以进行组合计费，同时为一种组合设置一个计费因子，在实际计费过程中用批价部件中的基本费率和计费因子实现多种附加计费规则的组合计费。

在实际应用中，数据业务的计费策略可以用批价部件中保存的基本费率信息+附加计费规则部件的计费因子信息”来描述。

例如：对应于互联网内容提供商的短信业务，那么其基本费率信息可以如表一所示，表一为一种短信业务简单的费率表。

费率 ID	计费模式	计费单位	费率值
1	1（按次计费）	1（次）	10（分）

表一

表一的含义就是对按次计费的业务，每次收 10 分钱。

EX1060 - Page 596

不同的用户附加的计费因子可能不同，如果要求用户同时享受累积折扣、时间折扣，计费因子信息可以如表二所示，表二为一种短信业务计费因子表。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3（代表累积折扣）	0	累积折扣
0	5（代表时间折扣）	1	时间折扣

表二

表二对应了两种折扣，相当于将两种折扣组合成了一个计费因子。

上述两个表都是基本信息，实际应用中的表结构不仅限于此。

对应于累积折扣，如表三所示，表三为累积折扣表。

折扣 ID	折扣下限	折扣类型	折扣值
0（对应于计费因子表中的“折扣索引”字段）	30	0（表示百分比折扣）	80

表三

表三的含义就是当用户累积使用业务达到 30 次后，可以享受 8 折优惠

同样的，如表四所示，表四为时间折扣表。

折扣索引	起始时间	结束时间	折扣类型	折扣值
1	22:00:00	23:59:59	0(表示百分比折扣)	50

表四

表四的含义就是在 22：00~23：59 分使用业务的用户，都可以享受 5 折优

EX1060 - Page 597

惠。

将基本费率信息与计费因子信息相结合，就得到了一种计费策略，这样的一个计费策略就可以和一个业务相绑定。参见表五，表五为短信业务的一种计费策略。

业务 ID	费率索引	计费因子索引
8888	1	0

表五

其中 ID 为 8888 的业务代表短信业务，其计费策略就是：按次计费业务，每次收费 10 分，同时如果用户累积使用 30 次以上，可以享受 8 折优惠，如果在 22：00~23：59 之间享受业务，又可以享受 5 折优惠。

如果一个用户已经使用该业务 30 次，又在 22：30 使用该业务，那么该用户的实际收取金额=1（次）*10（分）*0.8*0.5=4（分）

如果需求产生变动，要求除支持以上两种折扣之外，再增加一种用户折扣，那么计费因子描述表只需进行修改，修改后的计费因子描述表参见表六。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3	0	累积折扣
0	5	1	时间折扣
0	6	2	用户折扣

表六

这样，启动用户折扣部件，就可以轻而易举的实现动态增加一种折扣类型了，完全不需要做代码的修改，真正达到了动态灵活配置计费规则的目的。其中 6 代表用户折扣。

例如：一个个人移动用户签约了互联网内容提供商的短信业务，当该用户接收短信时，互联网内容提供商向内容计费服务器发送内容计费记录，其中包含了该用户执行的是短信业务、发送短信的条数、发送的时间等信息。内容计费服务器收到该内容计费记录后，取出 OSS 预先存储在内容计费服务器中的该

EX1060 - Page 598

用户的个人信息，包括该用户的开户信息、付费类型（例如本用户为预付费用户）、该用户属性为个人用户、该用户没有欠费记录、用户已付费情况等信息。内容计费服务器根据该用户执行的是短信业务、发送短信的时间、发送短信的数目已超出预定额度，以及该用户为个人用户、且没有欠费记录，判断该用户应该享有表六所述的三种折扣，因此使用表六中ID号为0的计费因子进行计费，然后内容计费服务器将该计费结果发送给SCP，SCP在该用户的帐户上扣除相应的费用。

当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。其中内容计费记录信息可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

其中内容计费可以由以下步骤来实现：

步骤 A、根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

步骤 B、判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，对于移动数据业务是业务控制节点（SCP），预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

步骤C、营帐系统根据用户需要取出计费结果，生成用户帐单。

参见图1，图1为本发明一个较佳实施例的内容计费实现框图。本实施例是对移动数据业务进行计费。其中内容计费系统由专用的内容计费服务器110来实现，该内容计费服务器110与OSS 101、ICP/SP 102、SCP 104和营帐系统分别相连。内容计费服务器110与OSS 101为实时的同步消息接口，或以文件形式进行数据传输 ，ICP/SP 102、SCP 104之间均按照运营商接口规范进行连接。其中，内容计费服务器110与ICP/SP102采用消息或文件方式进行交互；内容计费服务

EX1060 - Page 599

器110与SCP 104之间采用EMPP协议消息进行交互。本实施例的接口均按照运营商接口规范设计，有利于与外部其他设备的对接。

本实施例中的内容计费服务器 110 包含了：

运营支撑系统（OSS）接口模块 111，将 OSS 101 与内容计费模块 113 相连，从 OSS 101 中获取签约移动数据业务用户的用户信息，发送给内容计费模块 113；

互联网内容提供商/ 业务提供商（ICP/SP）接口模块 112，将 ICP/SP102 与内容计费模块相连 113，ICP/SP 102 将内容计费记录信息发送给内容计费模块 110。

内容计费模块 113 是内容计费的主要功能模块，参见图 2，图 2 为图 1 所示实施例中内容计费模块的实现框图。内容计费模块 113 包含：计费引擎 201，其通过 OSS 接口模块 111、ICP/SP 接口模块与 OSS101 及 ICP/SP102 分别相连）从 OSS 101 中获取签约移动数据业务用户的用户信息，接收 ICP/SP 102 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件 202。

批价部件 202，存储了不同移动数据业务类型的基本费率，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录从相应的一个或多个计费规则部件 203 中取出相应的计费规则，对移动数据业务进行计费，并根据付费类型生成计费结果。

本实施例的内容计费服务器110预先定制了多个计费规则部件203，其根据不同移动数据业务类型分别存储不同的计费规则。计费规则部件203可以根据移动数据业务的变化，随时进行增加、删除和修改。可见，本实施例的内容计费系统以组件的方式实现，增加新需求即相当于增加新组件，对原有代码没有影响。同时各组件可以对外提供开放性接口，易于扩展。

总之，内容计费模块 113，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录对移动数据业务进行计费，并根据付费类型生成计费结果。

业务控制节点（SCP）接口模块 115，将 SCP 104 与内容计费模块 113 相连，将内容计费模块 113 产生的预付费用户的计费结果发送给业务控制节点 104；

话单接口模块 114，将内容计费模块 113 与营帐系统 103 相连；将内容计费模块 113 产生的后付费用户的计费结果发送给营帐系统 103。

本实施例中的业务控制节点（SCP）接口模块 115 和话单接口模块 114 构成了付费接口模块，根据数据业务的付费类型将计费结果发送给相应的计费处理设备——业务控制节点 104 或营帐系统 103。

话单接口模块 114 与营帐系统以 FTP 或 FTAM 传输信息，在用户需要时营帐系统通过话单接口模块 114 到内容计费服务器 110 取计费结果。话单接口模块 114 可以由一个独立的话单接口机来实现，其与内容计费模块 113 通过以文件格式传输信息。

在本实施例的内容计费服务器 110 计费过程中，用户信息和内容计费记录信息是计费中的重要信息，该用户信息具体可以包括：用户开户信息、付费类型、用户属性、欠费记录；内容计费记录信息具体可以包括：移动数据业务类型、该移动数据业务执行的时间、执行该移动数据业务的数据流量、该移动数据业务执行的次数。

另外，本实施例的内容计费服务器110可以由多个服务器来实现；其中，计费引擎201可以由专用的服务器来实现，批价部件202和计费规则部件203分布在其他的专用的服务器主机上。这样计费引擎201与计费规则部件203分布在不同主机上，能够确保内容计费系统的性能。

本实施例的内容计费系统，使用专用的服务器来实现，不依赖于其他设备，与其他设备的交互采用消息机制或 API 函数调用机制，使内容计费模块具有较高的独立性，可以进行独立的测试，减少了开发与测试的工作量，易于维护。

同时，本实施例可以动态增加或修改计费规则部件的组合，无需修改代码或重启计费系统，具有很大的灵活性，最大限度的满足了计费需求的灵活

EX1060 - Page 601

多变的特性。

由上述的实施例可见，本发明的这种数据业务的内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

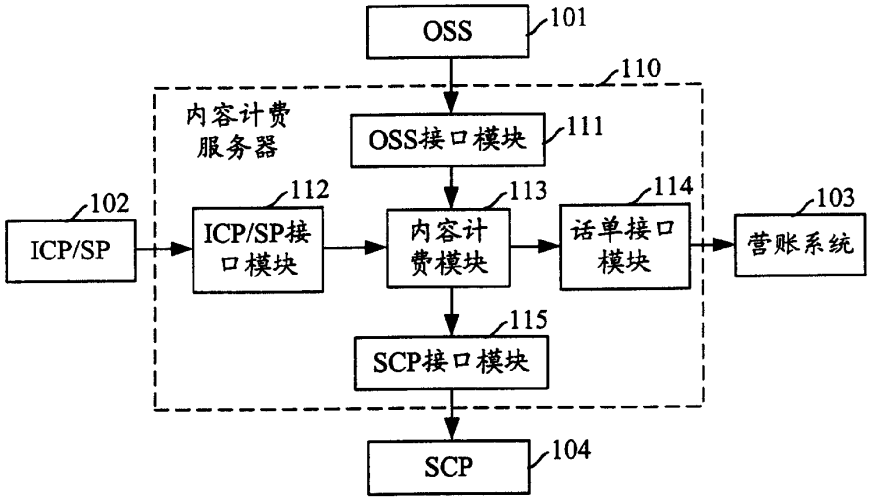


图 1

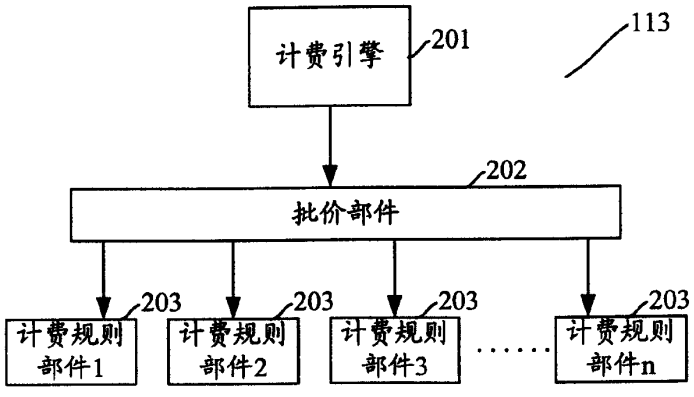


图 2

EX1060 - Page 603

Search Images Maps Gmail Drive Calendar Translate Docs More »

Google Patents Application Grant English Chinese Advanced Patent Search

Find prior art Discuss this application View PDF Download PDF

A content charging method of data service and charging system thereof

CN 1567818 A

Publication number	CN1567818 A
Publication type	Application
Application number	CN 03137490
Publication date	19 Jan 2005
Filing date	25 Jun 2003
Priority date	25 Jun 2003
Also published as	CN100550747C, CN101159566A, CN101159566B
Inventors	张庆, 于泽, 严雪松
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (9), Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a data service content charging method, customizing the charging rules as charging rule parts, as user executes data service, according to data service, user information and the content charging record obtained by Internet content provider/service provider (ICP/SP), using the corresponding charging rule part to making content charging. At the same time, it discloses a service content charging system, implemented by special content charging server and containing operation supporting system (OSS), ICP/SP interface module, content charging module, and payment interface module. It has the characters of independency, flexibility, extendability, openness and distributivity, realizes the charge according to data service content and meets the flexible and various charging requirements in data service.

DESCRIPTION translated from Chinese

A data service content charging method and charging system

Technical Field

The present invention relates to a data service charging technology, and more particularly to a data content service charging method and charging system.

Background

Currently, according to Universal Mobile Telecommunications System (UMTS) Forum Report 9 analysis, 3G data connection business into content categories and mobility class two categories, content connection type can be divided into: mobile Internet access and corporate Intranet / Extranet access; Mobility category can be divided into: customer information, entertainment; multimedia message service; location-based services; in addition to a total of six class enhanced voice services.

This 6 class of business represents a major demand for 3G services. Today, voice-dominated field of mobile communications, the future will be a data-centric business environment. Content at any time and any place to access the Internet will clearly be an important task of 3G.

3G billing is an important part of the 3G solutions. While 3G services are varied, prospects are tempting, but if there is no corresponding accounting solutions that do not establish the corresponding value chain system, which operators can not operate, then all talk.

Current traditional billing systems are designed for voice traffic, generally based on call duration, distance and other factors calling and called for billing. Namely the traditional billing and call duration and the Lord called location-related, regardless of the business content consumption.

The current 3G billing system, still based billing of voice services, its accounting policy commonly used hard-coded way, that the accounting formula in the code writing dead, once the billing rate tables to determine which accounting method correspondingly fixed.

CLAIMS (16) translated from Chinese

A method of data service billing content, characterized in that the method comprises the following steps: 1) according to the different types of data traffic of different charging rules, the one or more custom charging rules member; 2) pre-stored signed data service user's user information; 3) When the user performs data services, according to the data service, step 2) content of the user information and Internet content providers / service provider (ICP / SP) billing record information obtained using the corresponding charging rule components, content billing.

2. The content charging method according to claim 1, wherein said step a) further comprises: providing a charging member charging rules for each factor, by a combination of factors to achieve a variety of billing combination accounting rules for accounting.

3. The content billing method according to claim 1, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; and the content billing record information including at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

The content charging method according to claim 3, wherein said step 3) comprises the steps of: 31) in accordance with the type of data service, remove the corresponding charging rule corresponding charging rule member, then the data service based on the time for execution of data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if the prepaid The results will be sent to the prepaid billing processing equipment, processing equipment by prepaid billing deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

5. The content billing method according to claim 4, wherein: when

The main disadvantage is that the hard-coded code reuse, flexibility is poor, if the increase in new demand you need to change a lot of code, the code coupling between large, modification covers a wide, easy to maintain, is not conducive to the stability of the charging system. Billing flexibility for 3G services requirements, such implementations obviously can not meet.

Another way is to use a script curing accounting policy, using a scripting language for accounting formula. While using a scripting language can be very flexible to add new accounting policy, modify the accounting formula also having to modify the code, but is generally more complex due to the accounting formula, using scripts have great difficulty, poor readability. In addition, the interpretation of the scripting language for system performance will have some impact.

Billing systems existing 3G mobile communication system is composed of original equipment integration to achieve, namely accounting functions integrated in the SSP or SCP, the SSP / SCP complete user billing capabilities.

Traditional voice services and content user consumption billing is irrelevant, only the long (user talk time), distance (local or long-distance calls), and therefore do not have to report business information or content attributes, but users do not care about the consumer business traffic times, just in SSP / SCP side statistics users talk time, after the SSP / SCP complete user accounting function, the tent system based on accounting results generated user bill, presented to the user needs users.

3G the most attractive place is "always on" service, as long as open the phone you can enjoy the rich and varied business content, therefore limited to traditional voice services billing system obviously can not meet the diverse business brings diverse content billing requirements. Thus traditional voice billing does not meet the needs of content billing.

And because the prior art billing system via a mobile communication system to achieve the integration of existing equipment, takes up the resources of mobile communication systems, billing process cumbersome, inflexible, unable to meet the growing data business colorful count Fee required.

DISCLOSURE

In view of this, the present invention is to provide a data service content charging methods to achieve billing based on business content, data services to meet flexible billing requirements.

Another object of the present invention is to provide a data service content billing systems, saving mobile communication system resources, billing based on business content, data services to meet flexible billing requirements.

In accordance with one aspect of the above object, the present invention provides a data service billing content, the method comprising the steps of: 1) according to the different types of data traffic of different charging rules, one or more custom charging rules member; 2) the business user subscription data previously stored user information; 3) When the user performs data services, according to the data service, user information and Internet content provider in step 2) above / service provider (ICP / SP) obtained content billing record information, use the appropriate charging rule means content billing.

Wherein said step 1) may further comprise: providing a charging member charging rules for each factor, billing factor by charging a variety of combinations to achieve a combination of charging rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

Said step 3) may comprise the steps of: 31) in accordance with the type of data billing for mobile data services, prepaid processing equipment for the service control point (SCP).

Content billing method according to claim 6, wherein: the method further comprises, billing the result of step 3) obtained by the tent system according to the user needs to generate user billing.

A data service content billing system, wherein the system comprises content billing server, the content accounting server includes at least: Operations Support System (OSS) interface module, connect OSS and content billing module, Get the OSS in business user subscription data user information to the content billing module; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module, ICP / SP will content billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records billing data services, and generates accounting results based on the type of pay; Pay Interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment.

8. The content metering system according to claim 7, characterized in that said interface module comprises charge: prepaid interface module, the processing of prepaid billing module connected to the device with the content, the content of the billing module generates prepaid user accounting result to a prepaid processing equipment. If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

9. The content metering system according to claim 8, characterized in that the said prepaid module interfaces: service control point (SCP) interface module, the contents of the billing module connected to the SCP, the contents of the billing module generating prepaid subscribers accounting result to the SCP.

10. The content billing system according to claim 7, wherein the content of the billing module comprising at least: billing engine, connected respectively OSS and ICP / SP, get a business user subscription data from the OSS user information, content billing record information received ICP / SP transmitted, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data type of business, data service user's user information, content billing record is removed from the charging rule corresponding charging rule parts, billing for data services, and generates accounting results based on the type of charge, charging rules parts, depending on the type of data service store different charging rules.

11. The content billing system according to claim 7, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; content billing record information includes at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

12. The content billing system according to claim 8, wherein said interface module for the bill if a single interface machine, its content billing module to transmit information by file format.

13. The content billing system according to claim 9, wherein: the content accounting server and OSS real-time synchronous message interface, or as files for data transmission; the content accounting server and ICP / SP , content billing server between SCP and are in

service, remove the corresponding charging rule corresponding charging rule component, then the data service based on the time for execution of the data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if prepaid will send the results to the prepaid billing processing equipment, processing equipment by prepaid plan fee deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

When billing for mobile data services, prepaid processing device may be the service control point (SCP).

According to another aspect of the above object, the present invention provides a content billing system, which includes a dedicated server content billing, content billing server that includes at least: Operations Support System (OSS) interface module, the OSS and content Billing module is connected, access the user's subscription data service user information from OSS, and sent to the billing module content; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module , ICP / SP will send the contents of the billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records data services billing, and paying according to the type of generation accounting result; pay interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment. The pay-interface module comprising: a prepaid interface module, a prepaid processing billing module connected devices and content, the content billing module generates prepaid subscribers accounting result to a prepaid processing equipment.

If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

Wherein the prepaid interface module can be: service control point (SCP) interface module, connect the SCP and content billing module, content billing module generates prepaid subscribers accounting result to the SCP.

The contents of the billing module can at least contain: billing engine, connected respectively OSS and ICP / SP, business users get subscription data user information from OSS, the content billing record information received ICP / SP to send, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data service type, data service user's user information, content billing records from the accounting rule member Remove the appropriate accounting rules, data service billing, and generates accounting results based on the type of charge; charging rules parts, depending on the data stored in different types of business accounting rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

The CDRs CDR interface module can interface machine, with content billing module to transmit information to a file format.

The content of the accounting servers and OSS for real-time synchronous message interface, or as files for data transmission; can be carried out according to the operator interface specification between the content accounting server and ICP / SP, content billing server and SCP connection.

The content accounting server and ICP / SP can be used to interact with the message or file mode; the content may be used between the accounting server and SCP (EMPP) mobile PPP protocol message extension to interact.

If a single interface module and tent system can File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system via CDR interface module to fetch the content accounting server accounting results.

The content of the accounting server may contain one or more servers; billing and charging rules engine components distributed across different server host.

Seen from the aspect of the present invention, the content of the billing system and accounting methods of the present invention, the accounting rules for the charging rules customized parts, when the user performs data services, according to data services, user information and internet content provider content billing record information / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing, billing realized according to the data service content to meet the data services in flexible terms fee requirements.

accordance with the operator interface specification for the connection.

14. The content billing system as claimed in claim 13, characterized in that the content accounting server and ICP / SP messages or files using interactive manner; moving from point to point by the extended content billing server and SCP Protocol (EMPP) protocol message interaction.

15. The content billing system according to claim 8, wherein: if a single tent system interface module File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system By bill to content billing server interface modules take accounting results.

16. The content billing system according to claim 7, wherein the content of the accounting server contains more than one server; billing and charging rules engine components distributed across different server host.

Brief Description

Figure 1 is an example of content billing invention a preferred embodiment of realization diagram; Figure 2 is a block diagram of realization content billing module shown in FIG. 1 embodiment.

DETAILED DESCRIPTION

For the purposes of this invention, technical solutions and advantages more apparent, the following Examples and accompanying drawings, the present invention is described in further detail.

This data service content billing method of the present invention is to meet the characteristics of 3G services, the use of billing approach based on business content. And flexible billing based on the ever-changing needs, customize different charging rules. That is, the present invention can be customized according to different accounting rules billing formula, accounting policy, discount strategy flexible combination, easy expansion.

This data service content billing method of the present invention, the first data according to different accounting rules for different types of services, customized billing rule one or more parts; at the same time the business user subscription data previously stored user information, the user information including: user account information, payment types, user attributes, arrears records.

Among them, the custom component charging rules, the reference to the following factors: A, different ICP / SP may have different charging policies; B, different services may have different pricing strategies, such as different games, different games may charge; C, support long time and billing, such as casino games, duration and costs; D, support content-based traffic accounting, such as downloading pictures, according to traffic accounting, but the rates differ depending on the image; E, supported by using the number of billing (including Article, by page, pay-per), such as downloading pictures, MP3, ring tones; F, supported by time period or date using different accounting policies; as certain date free promotion, every day Some time access to give some discounts; G, support parity billing, support contract fee (monthly) + per use or duration or flow and other accounting policies; H, supports billing of individual users, different user You can choose according to their different tariff or billing strategy; I, the amount of support with the use of different (length, flow, frequency) using different accounting policies, which are similar to hop gear; J, advertising, allowing users to access the ICP advertising delivery fee service, and it can be divided Get royalty and Get amounts of the two to use; K, support access to different data networks using different accounting policies, and other factors to consider QoS; different L, support the use in different regions or areas billing policy, it is possible in the "hot spots" in different charge to the user. For example, with respect to the concept of "work area" on the "living area" to charge lower fees; M, support capping costs.

In addition, the discount is a very important means of SP and network operators to attract users, whether traditional voice services, or 3G for mobile data services, and discounts are pivotal position. Discount variety of ways, the current widespread use of rebates are the following: a, period discount - retaining the existing daily, week, holidays rebates. This approach can be extended to a metered charging mode.

b, the cumulative discount - including long cumulative discount, discount the cumulative flow, cumulative entry discount, the cumulative amount of discounts and other four kinds of rebates.

c, a cumulative discount - in accordance with the first use of the total, the total amount of time you use the discount d, user discounts - for certain user groups unified discount. All discounts can be tiring ride basis.

e, business discounts - for certain business unified discount.

In a specific embodiment of the present invention according to the above factors, a number of accounting rules customized components. Charging a business can be achieved by the grant price component and one or more charging rules components. Charging Rules components can be combined billing, and set a billing factor is a combination of the actual billing process using the grant price component of the base rate and billing factor to achieve a combination of a variety of additional charging rules count fee.

Basic Rate Information + billing factor information in practical applications, data services charging policies can be stored in approved price component parts of additional charging rules "to describe.

For example: corresponds to the short message service Internet content providers, its basic rate information as shown in Table I, Table I as a simple SMS tariff.

Image not available. View PDF

Table I Table it is the meaning of the pay-per-service, per charge 10 cents.

Different users additional accounting factor may be different, if the requirements of users while enjoying BONUS time discount factor accounting information as shown in Table II, Table II as a short message service charging factor table.

Image not available. View PDF

Table II Table II correspond to two discount, equivalent to two kinds of discount combined into a billing factor.

Both tables are basic information, practical application of the table structure is not limited to this.

Corresponding to the cumulative discount, as shown in Table III, Table 3 gives the BONUS table.

Image not available. View PDF

Table III Table III cumulative meaning that when users use the business 30 times, you can enjoy 20% discount Similarly, as shown in Table IV. Table IV is the time discount table.

Image not available. View PDF

Table 4 and Table IV meaning that at 22:00 ~ 23:59 minutes using business users, you can enjoy 50% discount.

The basic rate information and billing information combined factors, we get an accounting policy, such a billing policy can and bound to a business. Table V. Table V as an accounting policy SMS service.

Image not available. View PDF

Table V wherein the agent ID to SMS 8888, the accounting policy is: pay-per-service, a charge of 10 points, but if you use more than 30 times the cumulative, you can enjoy a 20% discount, if at 22:00 ~ 23: 59 between enjoying the business, you can enjoy a 50% discount.

If a user has used the service 30 times, and use the service at 22:30, then the user's actual charge amount = 1 (time) * 10 (points) * 0.8 * 0.5 = 4 (points) if demand fluctuates, Requirements In addition to supporting these two discount outside, and then add a user discount factor accounting description then just make changes, the revised accounting factor description in Table VI.

Image not available. View PDF

Table VI Thus, the launch customer discount member, you can easily add a dynamic type of discount, you do not need to modify the code completely, thereby achieving a dynamic and flexible accounting rules configuration purposes. Including six representatives user discounts.

For example: an individual mobile users subscribing to Internet content providers short message service, when the user receives messages, Internet content providers to send content billing records to the content accounting server, which contains the short message service is performed by the user, sending the number of text messages, send the time and other information. After the content accounting server receives the content billing records, remove OSS previously stored in the content accounting server in the user's personal information, including the user's account information, payment types (such as this user prepaid users), the user attributes for individual users, the user has no arrears records, and other information the user has paid. SMS content accounting server is performed based on the user, time to send text messages, send text messages number has exceeded a predetermined amount, and the user for individual users, and no arrears records to determine if the user should have the table of the six Three discount, so use Table 6 ID number is 0 billing factors accounting, billing and content billing server sends the results to the SCP, SCP deduct the cost on the user's account.

When the user performs data services, according to data services, content billing record information of the user information and Internet content providers / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing. Wherein the content billing record information may include: data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

Wherein the content billing can be achieved by the following steps: Step A, according to the data type of business, remove the corresponding charging rules in the corresponding parts in the accounting rules, according to the time the data service for execution of data flow of the data service the number of times the data service execution, an accounting rule for accounting; procedure B, determine whether the user charges prepaid type, if it is pre-paid billing results will be sent to the prepaid-processing equipment, for mobile data services is a service control point (SCP), prepaid billing processing apparatus according to the results of deductions from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

Procedure C, tent system takes the accounting results based on user needs, to generate user billing.

Referring to Figure 1, Figure 1 is a block diagram of an invention implement content billing preferred embodiment. In this embodiment, the mobile data service billing. Wherein the content billing system consists of a dedicated server 110 to implement content billing, content billing server 110 and OSS 101, ICP / SP 102, SCP 104 and tents are connected to the system. Content billing server 110 and OSS 101 is a real-time synchronous message interface, or as files for data

transmission, ICP / SP 102, between SCP 104 in accordance with the operator interface specification for the connection. Wherein the content accounting server 110 and ICP / SP102 messages or files using interactive mode; the content accounting server used between 110 and SCP 104 EMPP protocol messages to interact. Interface to the present embodiment in accordance with the operator interface specification design is conducive to docking and other external devices.

In this embodiment of the content billing server 110 includes: operations support systems (OSS) interface module 111, the OSS 101 is connected with the contents of the billing module 113 to obtain the user's mobile data service contract user information from OSS 101 and send it to content billing module 113; Internet content provider / service provider (ICP / SP) interface module 112, the ICP / SP102 and content billing module connected to 113, ICP / SP 102 content billing record information to the content billing module 110.

Content billing module 113 is the main function module content billing, see Figure 2, Figure 2 is a block diagram shown in Figure 1 to achieve the implementation of the contents of the accounting module. Content billing module 113 comprises: billing engine 201, which, ICP / SP interface module OSS101 and ICP / SP102 respectively connected via OSS interface module 111) to obtain the user's mobile data service contract user information from OSS 101, a receiving ICP / SP 102 content billing record information sent and the user information and content billing record information to grant price component 202.

Grant price component 202 stores a basic rate of different types of mobile data services, mobile data services based on the type of mobile data service user's user information, content billing records removed from the corresponding one or more of the appropriate accounting rules section 203 accounting rules, mobile data services billing, and generate results based on accounting charge type.

Content billing server 110 of the present embodiment a plurality of pre-charging rules customized member 203, which depending on the type of mobile data services are stored in different charging rules. Charging Rules section 203 may vary as mobile data services, at any time to add, delete and modify. Visible, content billing system of the present embodiment by way of implementation of the components, add the new requirement is equivalent to adding new components, there is no effect on the original code. At the same time the components can provide external open interfaces, easy to expand.

In short, content billing module 113, based on the type of mobile data services, mobile data service user's user information, content billing record for mobile data services billing, and generate results based on accounting charge type.

Service control point (SCP) interface module 115, the SCP 104 billing module 113 is connected with the content, content billing module 113 generates prepaid subscribers accounting result to the service control node 104; if a single interface module 114, the content billing module 113 is connected with the camp system 103; the contents of the billing module 113 generates after paying user accounting system 103 sends the results to the tent.

In this embodiment of the service control point (SCP) interface module 115, and then a single interface module 114 constitutes a charge interface module, based on the type of data services paid billing results will be sent to the appropriate accounting treatment equipment - service control node 104 or tent system 103.

If a single interface module 114 and tent systems to FTP or FTAM transfer information when the user needs tent system interface module 114 through the bill to take the accounting content billing server 110 results. If a single interface module 114 may be composed of a separate bill to implement the interface machine, with content billing module 113 to transmit information by file format.

In this embodiment, the content accounting server 110 billing process, user information and content billing record information is important billing information, the user information may include: user account information, payment types, user attributes, arrears record; content billing record information may include: a mobile data service type, time of the mobile data services for execution of the data flow of mobile data services, the number of times the mobile data service execution.

Further, the content accounting server 110 of the present embodiment may be implemented by a plurality of servers; wherein the billing engine 201 may be implemented by a dedicated server, rating and charging rules 202 parts 203 parts distributed in other dedicated server host. Such billing and charging rules engine 201 203 members distributed on different hosts, to ensure the performance of the contents of the billing system.

Examples of content billing system of this embodiment, the use of a dedicated server to achieve, is not dependent on other devices, messaging mechanism or API function calls to interact with other equipment used to make the contents of the billing module with high independence can be independent testing, reducing the effort required to develop and test, easy to maintain.

Also, the present embodiment can dynamically add or modify parts of combination accounting rules, without modifying the code or restart the billing system with great flexibility, and satisfy the changing needs Flexible billing features.

Seen from the above-described embodiment, the data traffic of the invention content billing method and billing system, independence, flexibility, scalability, openness and distribution characteristics, to achieve a data service based on content billing, data services to meet the flexible billing requirements.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100394737C	11 Jul 2005	11 Jun 2008	西安大唐电信有限公司	Method for accessing network server and supporting system
CN100596074C	9 Feb 2007	24 Mar 2010	华为技术有限公司	Charge mode providing method and charge control system
CN101582776B	15 May 2008	21 Nov 2012	浙江大学	Service charging method and service charging system
CN101800824A *	4 Mar 2010	11 Aug 2010	中兴通讯股份有限公司	Method and device for charging
CN102098650A *	21 Jan 2011	15 Jun 2011	中国联合网络通信集团有限公司	Content charging-based flow adaptive method and system
CN102098650B	21 Jan 2011	3 Jul 2013	中国联合网络通信集团有限公司	Content charging-based flow adaptation method and system
CN102255734A *	19 May 2010	23 Nov 2011	华为技术有限公司	Charging method of content business, apparatus and system thereof
WO2006116894A1 *	29 Apr 2005	9 Nov 2006	Utstarcom Telecom Co Ltd	A method of flexible setting the charging mode in ims system
WO2007051416A1 *	2 Nov 2006	10 May 2007	Huawei Tech Co Ltd	A charging method and system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04M17/00, H04L12/14

LEGAL EVENTS

Date	Code	Event	Description
14 Oct 2009	C14	Granted	
7 Dec 2005	C10	Request of examination as to substance	
19 Jan 2005	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Electronic Acknowledgement Receipt

EFS ID:	22761757
Application Number:	14667353
International Application Number:	
Confirmation Number:	8845
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3
Receipt Date:	26-JUN-2015
Filing Date:	24-MAR-2015
Time Stamp:	19:03:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3.pdf	613651 7de16f890a9f0d91b156ebc479361851ce72c0ea	no	8

Warnings:	
Information:	

2	Foreign Reference	2063.pdf	2400276 5c7addfc40b293a3442a4c140083d3fc5d876114	no	21
Warnings:					
Information:					
3	Foreign Reference	2064.pdf	2345898 db3b0051c6d9ab3dfa64f05d6324394e5fc54486	no	20
Warnings:					
Information:					
4	Foreign Reference	2065.pdf	2381976 7796f26254f7db3b899626b2e7332663eaff0633	no	25
Warnings:					
Information:					
5	Non Patent Literature	3040_Ahmed.pdf	698684 312cdbfa74f55adbbd7f0eee7032be26a77e3ad5	no	10
Warnings:					
Information:					
6	Non Patent Literature	3041_Kassar.pdf	840076 1b87a4e38876abbcb73a0c7a689d940a997ba013	no	14
Warnings:					
Information:					
7	Non Patent Literature	3042_Kaufmann.pdf	3412131 987a5e9e6c5cadcf6cd5982f4c181ac27b6dafe7	no	283
Warnings:					
Information:					
8	Non Patent Literature	3043_Sadeh.pdf	1095284 adc744cb7b194a97b6f3ac3e1b28a65e042a8d9f	no	16
Warnings:					
Information:					
			Total Files Size (in bytes):	13787976	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

106963 7590 07/10/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
07/10/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

Office Action Summary	Application No. 14/667,353	Applicant(s) RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *2-22* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *2-22* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant cancelled claim 1.

Claim Rejections - 35 USC § 112

3. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 2-22 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claim 1, line 3, “a first WWAN” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, line 4, “a device messaging agent” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, lines 4-5, “on behalf of a plurality of software applications” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, line 6, “a network message server” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, line 7, “a subset of the secure Internet data messages” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, line 8, “an identifier” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 2, line 11, “a secure interprocess communication service” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 3, line 2, “a first application” and “a first format” are not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 4, lines 2-3, “a second application” and “a second format” are not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 5, lines 2-3, “the device messaging agent decrypting each message in the subset” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 6, lines 2-3, “one or more of encryption on a transport services stack . . . and tunneling” is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Also, the “and tunneling is improper syntax in juxtaposition to the “one or more” preceding it.

Claim 8, lines 1-3, “the service downloader . . . secure Internet messages” is not clear from the descriptive portion, e.g. service downloader 1663, of the specification in juxtaposition to the drawings.

Claim 11, lines 1-10, “The mobile end-user . . . content received with the request” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 12, lines 1-2, “at least one of the upload . . . a key for the network” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 13, line 2, “to create a log. . . data messages” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 15, lines 2-3, “the interprocess . . . security policy” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 16, lines 1-2, “the secure . . . identifier/data pairs” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 17, lines 2-4, “an agent. . . . software application” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 20, lines 1-2, “a network stack. . . within the network stack” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 21, lines 1-2, “at least one of the applications . . . network message server” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Claim 22, line 3, “a first WLAN” is not clear from the descriptive portion of the specification in juxtaposition to the drawings.

Clarification of where specific support for the above noted deficiencies from the specification in juxtaposition to the drawings is requested. As is, the metes and bounds of the claim language may not be properly ascertained.

Also, it is noted that Applicant’s claim language is replete with intended use claim language, e.g. claim 2, line 2, “configurable to,” that does not affirmatively limit the positively recited claim language, e.g. claim 2, line 1, “A mobile end user device.”

5. Further pertinent references of interest are noted on the attached PTO-892.

6. Applicant’s five (5) Information Disclosure Statements (IDS’s) have been reviewed. Note the attached IDS’s.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/

Primary Examiner

Art Unit 3687

Notice of References Cited	Application/Control No. 14/667,353	Applicant(s)/Patent Under Reexamination RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-9,049,010	06-2015	Jueneman et al.	1/1
*	B	US-8,174,378	05-2012	Richman et al.	340/521
*	C	US-6,757,717	06-2004	Goldstein, Leonid	709/217
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20090307746		2009-12-10	DI, Jinwen et al.	
	212	20050009499		2005-01-13	KOSTER, Karl	
	213	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	214	20100041364		2010-02-18	LOTT, Robert Wayne et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	215	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	216	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	217	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	218	20080313730		2008-12-18	Iftimie, Sorin et al.	
	219	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	220	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	221	20080240373		2008-10-02	WILHELM, Robert D.	
	222	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	223	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	
	224	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	225	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	226	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	227	20090172077		2009-07-02	ROXBURGH, David et al.	
	228	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	229	20030171112		2003-09-11	Lupper, Alfred et al.	
	230	20070300252		2007-12-27	Acharya, Swarup et al.	
	231	20050007993		2005-01-13	Chambers, Mahdi et al.	
	232	20020164983		2002-11-07	Raviv, Li-On et al.	
	233	20070280453		2007-12-06	Kelley, Sean S.	
	234	20100241544		2010-09-23	Benson, Dan et al.	
	235	20090157792		2009-06-18	Fiatal, Trevor	
	236	20070109983		2007-05-17	Shankar, Rohit et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	237	20020049074		2002-04-25	Eisinger, Bernd et al.	
	238	20020161601		2002-10-31	Nauer, Bernhard et al.	
	239	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	240	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	241	20010048738		2001-12-06	Baniak, Paul G. et al.	
	242	20070033197		2007-02-08	Scherzer, Shimon et al.	
	243	20110013569		2011-01-20	Scherzer, Shimon et al.	
	244	20110159818		2011-06-30	Scherzer, Shimon et al.	
	245	20120020296		2012-01-26	Scherzer, Shimon et al.	
	246	20120196644		2012-08-02	Scherzer, Shimon et al.	
	247	20120238287		2012-09-20	Scherzer, Shimon	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	248	20130058274		2013-03-07	Scherzer, Shimon et al.	
	249	20130084835		2013-04-04	Scherzer, Shimon et al.	
	250	20090005000		2009-01-01	Baker, Matthew et al.	
	251	20090006116		2009-01-01	Baker, Matthew et al.	
	252	20090006200		2009-01-01	Baker, Matthew et al.	
	253	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	254	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	255	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	256	20130065555		2013-03-14	Baker, Matthew Donald et al.	
	257	20060135144		2006-06-22	Jothipragasam, Premkumar	
	258	20080089295		2008-04-17	Keeler, James D. et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	259	20080022354		2008-01-24	Grewal, Karanvir et al.	
	260	20040102182		2004-05-27	Reith, Lothar et al.	
	261	20030233332		2003-12-18	Keeler, James D. et al.	
	262	20080250053		2008-10-09	Aaltonen, Janne et al.	
	263	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	264	20130144789		2013-06-06	Aaltonen, Janne et al.	
	265	20100131584		2010-05-27	Johnson, William J.	
	266	20100080202		2010-04-01	Hanson, Mark	
	267	20070147324		2007-06-28	McGary, Faith	
	268	20070168499		2007-07-19	Chu, Jing-Long	
	269	20070025301		2007-02-01	Petersson, Justus et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	270	20070140145		2007-06-21	Kumar, Surender et al.	
	271	20080120129		2008-05-22	Seubert, Michael et al.	
	272	20060174035		2006-08-03	Tufail, Mudassir	
	273	20110264923		2011-10-27	Kocher, Paul C. et al.	
	274	20080201266		2008-08-21	Chua, Huina et al.	
	275	20060156398		2006-07-13	Ross, Alan D. et al.	
	276	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	277	20100284327		2010-11-11	Miklos, Gyorgy	
	278	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	279	20050079863		2005-04-14	Macaluso, Anthony G.	
	280	20060114832		2006-06-01	Hamilton, Thomas E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	281	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	282	20080070550		2008-03-20	Hose, David Alan	
	283	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	284	20030188117		2003-10-02	Yoshino, Kenji et al.	
	285	20040255145		2004-12-16	Chow, Jerry	
	286	20050055595		2005-03-10	Frazer, Mark et la.	
	287	20070259656		2007-11-08	Jeong, Jong Woo	
	288	20080263348		2008-10-23	Zaltsman, Etai et al.	
	289	20080313315		2008-12-18	Karaoguz, Jeyhan et al.	
	290	20090282127		2009-11-12	LeBlanc, Michael et al.	
	291	20100167696		2010-07-01	Smith, Christopher David et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	292	20030188006		2003-10-02	Bard, Steven R.	
	293	20060160536		2006-07-20	Chou, Joey	
	294	20060168128		2006-07-27	Sistla, Amber et al.	
	295	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	296	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	297	20070147317		2007-06-28	Smith, Brian K. et al.	
	298	20080270212		2008-10-30	Blight, Jeffrey et al.	
	299	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	300	20110110309		2011-05-12	Bennett, James D.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	06/17/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100030890		2010-02-04	Dutta, Satadip et al.	
	2	20080025230		2008-01-31	Patel, Alpesh et al.	
	3	20040170191		2004-09-02	Guo, Zihua et al.	
	4	20020188732		2002-12-12	Buckman, Charles R. et al.	
	5	20080034419		2008-02-07	Mullick, Amarnath et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	6	20080010379		2008-01-10	Zhao, Hang	
	7	20080139210		2008-06-12	Gisby, Doug et al.	
	8	20040243992		2004-12-02	Gustafson, James P. et al.	
	9	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	10	20100235329		2010-09-16	Koren, David et al	
	11	20090254857		2009-10-08	Romine, Christopher et al.	
	12	20080166993		2008-07-10	Gautier et al.	
	13	20040137890		2004-07-15	Kalke, Catherine	
	14	20070143824		2007-06-21	Shahbazi, Majid	
	15	20070266422		2007-11-15	Germano et al.	
	16	20090044185		2009-02-12	Krivopaltsev, Eugene	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	17	20040039792		2004-02-26	Nakanishi, Tomoaki	
	18	20050075115		2005-04-07	Corneille et al.	
	19	20050239447		2005-10-27	Holzman et al.	
	20	20070213054		2007-09-13	Han, Seung-Wook	
	21	20080032715		2008-02-07	Jia et al.	
	22	20090163173		2009-06-25	Williams, Timothy D.	
	23	20100075666		2010-03-25	Garner, Neil Robert	
	24	20080293395		2008-11-27	Matthews, Ajit et al.	
	25	20050245241		2005-11-03	Durand, Terry et al.	
	26	20080125079		2008-05-29	O'Neil, Douglas et al.	
	27	20050135264		2005-06-23	Popoff, Jeff et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	28	20070165630		2007-07-19	Rasanen, Jorma	
	29	20100287599		2010-11-11	HE, Xianhui	
	30	20070060200		2007-03-15	Boris et al.	
	31	20060030306		2006-02-09	Kuhn, Brian Gerald	
	32	20060035631		2006-02-16	White et al.	
	33	20060206709		2006-09-14	Labrou et al.	
	34	20090046707		2009-02-19	Smires et al.	
	35	20100311402		2010-12-09	Srinivasan et al.	
	36	20110277019		2011-11-10	Pritchard Jr., John Russell	
	37	20050250536		2005-11-10	Deng et al.	
	38	20070192460		2007-08-16	Choi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	39	20080080457		2008-04-03	Cole, Terry L.	
	40	20090049518		2009-02-19	Roman et al.	
	41	20100248719		2010-09-30	Scholaert, Hugh	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401A	CN		2000-02-22	Wang, Di Xing		☐
	2	1878160A	CN		2006-12-13	Jiang, Yong		☐
	3	101127988A	CN		2008-02-20	ZTE Corporation		☐
	4	1503548 A1	EP		2005-02-02	FG Microtec GmbH		☐
	5	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	6	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	7	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		☐
	8	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		☐
	9	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
	10	2009-212707	JP		2009-09-17	Fujitsu Ltd.		☐
	11	2008-301121	JP		2008-12-11	Kyocera Corp.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	06/17/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8447980		2013-05-21	Godfrey, James A. et al.	
	2	8429403		2013-04-23	Moret, Eric et al.	
	3	8411587		2013-04-02	Curtis, William et al.	
	4	8396929		2013-03-12	Helfman, Nadav et al.	
	5	8363658		2013-01-29	Delker, Jason R. et al.	
	6	8265004		2012-09-11	Toutonghi, Michael J.	
	7	8233895		2012-07-31	Tysowski, Piotr Konrad	
	8	7685254		2010-03-23	Pandya, Ashish A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	9	7181017		2007-02-20	Nagel, Robert H. et al.	
	10	6965872		2005-11-15	Grdina, Jerome M.	
	11	8402540		2013-03-19	Kapoor, Harsh et al.	
	12	8135657		2012-03-13	Kapoor, Harsh et al.	
	13	8271992		2012-09-18	Chatley, Scott P. et al.	
	14	8315999		2012-11-20	Chatley, Scott P. et al.	
	15	8332375		2012-12-11	Chatley, Scott P. et al.	
	16	8468337		2013-06-18	Gaur, Santosh P. et al.	
	17	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	18	6640097		2003-10-28	Corrigan, Louis et al.	
	19	7039713		2006-05-02	Van Gunter, David et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	20	5915008		1999-06-22	Dulman, Scott	
	21	8126476		2012-02-28	Vardi, Yosef et al.	
	22	8000276		2011-08-16	Scherzer, Shimon et al.	
	23	8358638		2013-01-22	Scherzer, Tamir et al.	
	24	8356336		2013-01-15	Johnston, Keith et al.	
	25	8307067		2012-11-06	Ryan, Nicholas M.	
	26	7286848		2007-10-23	Vireday, Richard P. et al.	
	27	7313237		2007-12-25	Bahl, Paramvir et al.	
	28	7444669		2008-10-28	Bahl, Paramvir et al.	
	29	7548976		2009-06-16	Bahl, Paramvir et al.	
	30	8027339		2011-09-27	Short, Joel E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	31	8095112		2012-01-10	Chow, Richard et al.	
	32	7881697		2011-02-01	Baker, Matthew Donald et al.	
	33	7899438		2011-03-01	Baker, Matthew Donald et al.	
	34	7945238		2011-05-17	Baker, Matthew Donald et al.	
	35	8078140		2011-12-13	Baker, Matthew Donald et al.	
	36	8285249		2012-10-09	Baker, Matthew Donald et al.	
	37	7493659		2009-02-17	Wu, Handong et al.	
	38	7801985		2010-09-21	Pitkow, Jim et al.	
	39	8242959		2012-08-14	Mia, Rashidus S. et al.	
	40	8326319		2012-12-04	Davis, Richard W.	
	41	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	42	7139569		2006-11-21	Kato, Akira	
	43	7529204		2009-05-05	Bourlas, Yair et al.	
	44	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	45	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	46	8032409		2011-10-04	Mikurak, Michael G.	
	47	8045973		2011-10-25	Chambers, Michael D.	
	48	8116781		2012-02-14	Chen, Xixian et al.	
	49	8126396		2012-02-28	Bennett, James D.	
	50	8351898		2013-01-08	Raleigh, Gregory G.	
	51	5630159		1997-05-13	Zancho, William F.	
	52	5633484		1997-05-27	Zancho, William F. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	53	5814798		1998-09-29	Zancho, William F.	
	54	7039403		2006-05-02	Wong, Gregory A.	
	55	7583964		2009-09-01	Wong, Gregory A.	
	56	7593730		2009-09-22	Khandelwal, Deepak et al.	
	57	7948953		2011-05-24	Melkote, Keerti G. et al.	
	58	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	59	8270972		2012-09-18	Otting, Marcia J. et al.	
	60	7929959		2011-04-19	DeAtley, Dallas et al.	
	61	7478420		2009-01-13	Wright, Michael et al.	
	62	7502672		2009-03-10	Kolls, H. Brock	
	63	7756757		2010-07-13	Oakes III, Charles Lee	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	64	7930446		2011-04-19	Kesselman, Alex et al.	
	65	8078163		2011-12-13	Lemond, Eric et al.	
	66	8068829		2011-11-29	Lemond, Eric et al.	
	67	8086497		2011-12-27	Oakes III, Charles Lee	
	68	8166040		2012-04-24	Brindisi, Richard G. et al.	
	69	6934249		2005-08-23	Bertin, Olivier et al.	
	70	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	71	8447607		2013-05-21	Weider, Chris et al.	
	72	8504729		2013-08-06	Pezzutti, David A.	
	73	8495227		2013-07-23	Kaminsky, David L. et al.	
	74	8472371		2013-06-25	Bari, Farooq et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	75	8134954		2012-03-13	Godfrey, James A. et al.	
	76	7535880		2009-05-19	Hinman, Brian L. et al.	
	77	7499438		2009-03-03	Hinman, Brian L. et al.	
	78	7496652		2009-02-24	Pezzutti, David	
	79	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	80	6654814		2003-11-25	Britton, Kathryn H. et al.	
	81	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	82	8325638		2012-12-04	Jin, Haipeng et al.	
	83	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	84	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	85	8090359		2012-01-03	Proctor Jr., James Arthur et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	86	8150431		2012-04-03	Wolovitz, Lionel et al.	
	87	8483135		2013-07-09	Cai, Yigang et al.	
	88	6104700		2000-08-15	Haddock, Stephen R. et al.	
	89	8185127		2012-05-22	Cai, Zheng et al.	
	90	8521110		2013-08-27	Rofougaran, Ahmadreza	
	91	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	92	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	93	7546460		2009-06-09	Maes, Stephane H.	
	94	7921463		2011-04-05	Sood, Kapil et al.	
	95	7940751		2011-05-10	Hansen, Christopher J.	
	96	8122249		2012-02-21	Falk, Rainer et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	97	8495360		2013-07-23	Falk, Rainer et al.	
	98	8520589		2013-08-27	Bhatt, Yogesh et al.	
	99	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	100	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	101	8296404		2012-10-23	McDysan, Dave et al.	
	102	8195163		2012-06-05	Gisby, Doug et al.	
	103	8437734		2013-05-07	Ray, Amar N. et al.	
	104	7460837		2008-12-02	Diener, Neil R.	
	105	7653394		2010-01-26	McMillin, Brian K.	
	106	8130793		2012-03-06	Edwards, Stephen K. et al.	
	107	8509082		2013-08-13	Heinz, John M. et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	108	8526329		2013-09-03	Mahany, Ronald L. et al.	
	109	5983270		1999-11-09	Abraham, Dalen M. et al.	
	110	6598034		2003-07-22	Kloth, Axel K.	
	111	7032072		2006-04-18	Quinn, Michael J. et al.	
	112	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	113	7742406		2010-06-22	Muppala, Suresh	
	114	7953877		2011-05-31	Vemula, Narendra et al.	
	115	7957381		2011-06-07	Clermidy, Fabien et al.	
	116	8031601		2011-10-04	Feroz, Azeem et al.	
	117	8255534		2012-08-28	Assadzadeh, Alireza	
	118	8489720		2013-07-16	Morford, Michael Robert et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	119	7774323		2010-08-10	Helfman, Nadav	
	120	7043268		2006-05-09	Yukie, Satoru et al.	
	121	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	122	8166554		2012-04-24	John, Pramod	
	123	7697540		2010-04-13	Haddad, Reda et al.	
	124	6748195		2004-06-08	Phillips, W. Garland	
	125	8583499		2013-11-12	De Judicibus, Dario et al.	
	126	8352360		2013-01-08	De Judicibus, Dario et al.	
	127	8463232		2013-06-11	Tuli, Amol et al.	
	128	7958029		2011-06-07	Bobich, Thomas et al.	
	129	7540408		2009-06-02	Levine, Judah Joseph et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	130	7826427		2010-11-02	Sood, Kapil et al.	
	131	8483694		2013-07-09	Lewis, Allan D. et al.	
	132	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	133	7610396		2009-10-27	Taglienti, Claudio et al.	
	134	7984511		2011-07-19	Kocher, Paul Carl et al.	
	135	7987510		2011-07-26	Kocher, Paul C. et al.	
	136	8571993		2013-10-29	Kocher, Paul C. et al.	
	137	8543265		2013-09-24	Ekhaguere, David E. et al.	
	138	6873988		2005-03-29	Hermann, Conrad K. et al.	
	139	7013469		2006-03-14	Smith, Adam W. et al.	
	140	7203169		2007-04-10	Okholm, Jon Eric et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	141	7286834		2007-10-23	Walter, Edward	
	142	7555757		2009-06-30	Smith, Adam W. et al.	
	143	7574509		2009-08-11	Nixon, Mark J. et al.	
	144	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	145	7940685		2011-05-10	Breslau, Lee Michel et al.	
	146	8196199		2012-06-05	Hrastar, Scott E. et al.	
	147	8204505		2012-06-19	Jin, Haipeng et al.	
	148	8228818		2012-07-24	Chase, Christopher J. et al.	
	149	8320244		2012-11-27	Muqattash, Alaa et al.	
	150	8411691		2013-04-02	Aggarwal, Rahul	
	151	8461958		2013-06-11	Saenz, Jorge E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	152	8484327		2013-07-09	Werner, Eran et al.	
	153	8522039		2013-08-27	Hyndman, Arn et al.	
	154	8544105		2013-09-24	Mclean, Ivan H. et al.	
	155	8571474		2013-10-29	Chavez, Timothy R. et al.	
	156	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	157	8095124		2012-01-10	Balia, Hinal K.	
	158	7797060		2010-09-14	Grgic, Richard J. et al.	
	159	7930327		2011-04-19	Craft, David Jones et al.	
	160	8264965		2012-09-11	Dolganow, Andrew et a.	
	161	6885997		2005-04-26	Roberts, David T.	
	162	8229394		2012-07-24	Karlberg, Johan	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	163	8495700		2013-07-23	Shahbazi, Majid	
	164	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	165	8572117		2013-10-29	Rappaport, Theodore S.	
	166	8589955		2013-11-19	Roundtree, Brian et al.	
	167	8660853		2014-02-25	Robb, Terence A. et al.	
	168	8601125		2013-12-03	Huang, Shibi et al	
	169	8046449		2011-10-25	Yoshiuchi, Hideya	
	170	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	171	8566236		2013-10-22	Busch, James David	
	172	8528068		2013-09-03	Weglein, Joseph et al.	
	173	8442015		2013-05-14	Behzad, Arya et al	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	174	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	175	7720464		2010-05-18	Batta, Puneet	
	176	8300575		2012-10-30	Willars, Per	
	177	8666395		2014-03-04	Silver, Andrew	
	178	8315593		2012-11-20	Gallant, John K. et al.	
	179	8180881		2012-05-15	Seo, Kyoung-Il et al.	
	180	7539132		2009-05-26	Werner, Carl E. et al.	
	181	7805606		2010-09-28	Birger, Chet et al.	
	182	8347378		2013-01-01	Merkin, Aaron E. et al.	
	183	6185576		2001-02-06	McIntosh, Lowrie	
	184	8175574		2012-05-08	Panda, Biswaranjan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	185	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	186	8527410		2013-09-03	Markki, Outi et al.	
	187	7320029		2008-01-15	Rinne, Janne Petri et al.	
	188	8275415		2012-09-25	Huslak, Nicholas S.	
	189	8554876		2013-10-08	Winsor, Gerald W.	
	190	8191124		2012-05-29	Wynn, Simon et al.	
	191	7805140		2010-09-28	Friday, Robert J. et al.	
	192	8605691		2013-12-10	Soomro, Amjad et al.	
	193	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	194	8706863		2014-04-22	Fadell, Anthony	
	195	6640334		2003-10-28	Rasmussen, John H.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	196	7668612		2010-02-23	Okkonen, Harri	
	197	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	198	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	199	5131020		1992-07-14	Liebesny, John P. et al.	
	200	8370483		2013-02-05	Choong et al.	
	201	8670334		2014-03-11	Keohane et al.	
	202	8693323		2014-04-08	McDysan, David E.	
	203	7409447		2008-08-05	Assadzadeh, Alireza	
	204	8725899		2014-05-13	Short, Joel et al.	
	205	8676925		2014-03-18	Liu, Jiawei et al.	
	206	8645518		2014-02-04	David, Scott L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	207	7756056		2010-07-13	Kim et al	
	208	8131281		2012-03-06	Hildner et al.	
	209	8160598		2012-04-17	Savoor, Raghvendra	
	210	8375136		2013-02-12	Roman et al.	
	211	6119933		2000-09-19	Wong et al.	
	212	8694772		2014-04-08	Kao et al.	
	213	8719423		2014-05-06	Wyld, Jeremy	
	214	8347104		2013-01-01	Pathiyal, Krishna K.	
	215	7149229		2006-12-12	Leung, Kent K.	
	216	7242668		2007-07-10	Kan, Chao et al.	
	217	8095640		2012-01-10	Guingo, Pierrick et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	218	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	219	8811991		2014-08-19	Jain, Nikhil et al.	
	220	7809351		2010-10-05	Panda et al.	
	221	8346210		2013-01-01	Balsan, Damien et al.	
	222	8355696		2013-01-15	Olding et al.	
	223	8422988		2013-04-16	Keshav, Srinivasan	
	224	8488597		2013-07-16	Nie et al.	
	225	6438575		2002-08-20	Khan et al.	
	226	7222304		2007-05-22	Beaton et al.	
	227	7561899		2009-07-14	Lee, Changseok	
	228	8200200		2012-06-12	Belser et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	229	8229914		2012-07-24	Ramer et al.	
	230	8522249		2013-08-27	Beaule, Stephane	
	231	8701015		2014-04-15	Bonnat, Pierre	
	232	6697821		2004-02-24	Ziff et al.	
	233	6763226		2004-07-13	McZeal Jr., Alfred	
	234	6982733		2006-01-03	McNally et al.	
	235	6983370		2006-01-03	Eaton, et al.	
	236	7318111		2008-01-08	Zhao, Wen	
	237	8064418		2011-11-22	Maki, Lasse	
	238	8249601		2012-08-21	Emberson et al.	
	239	8514927		2013-08-20	Sundararajan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	5	1802839A	CN		2006-07-12	Motorola Inc.		☐
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	7	101123553A	CN		2007-09-11	SouTheast University		☐
	8	1937511A	CN		2007-03-28	ZTE		☐
	9	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐
	10	2007133844	WO		2007-11-22	Camiant, Inc.		☐
	11	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐
	12	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	13	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐
	14	101815275A	CN		2010-08-25	Yang, Liu		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	5	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	06/17/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	174	7609700		2009-10-27	Ying, Wen-Ping et al.	
	175	8255515		2012-08-28	MELMAN, David et al.	
	176	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	177	7912056		2011-03-22	BRASSEM, Wayne	
	178	7920529		2011-04-05	MAHLER, Roger et al.	
	179	8184530		2012-05-22	SWAN, Tim L. et al.	
	180	8214536		2012-07-03	ZHAO, Wen	
	181	8213363		2012-07-03	YING, Wen-Ping et al.	
	182	8255689		2012-08-28	KIM, Eun Ah et al.	
	183	7746854		2010-06-29	AMBE, Shekhar et al.	
	184	7068600		2006-06-27	CAIN, Joseph Bibb	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	185	6876653		2005-04-05	AMBE, Shekhar et al.	
	186	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	187	7599288		2009-10-06	COLE, Raymond E. et al.	
	188	7546629		2009-06-09	ALBERT, Anthony et al.	
	189	7747730		2010-06-29	HARLOW, James D.	
	190	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	191	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	192	7283963		2007-10-16	FITZPATRICK, John E. et al.	
	193	8271049		2012-09-18	SILVER, Andrew et al.	
	194	7644151		2010-01-05	JERRIM, John et al.	
	195	8291238		2012-10-16	GINTER, Karl L. et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	196	8068824		2011-11-29	SHAN, Xueshan et al.	
	197	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	198	5283904		1994-02-01	CARSON, David G. et al.	
	199	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	200	8185152		2012-05-22	GOLDNER, Alla	
	201	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	202	7873344		2011-01-18	BOWSER, Robert et al.	
	203	7856226		2010-12-21	WONG, Ellis L. et al.	
	204	7948952		2011-05-24	HURTTA, Tuija et al.	
	205	7957020		2011-06-07	MINE, Ryuta et al.	
	206	7346410		2008-03-18	UCHIYAMA, Kenji	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	207	7167078		2007-01-23	POURCHOT, Shawn C.	
	208	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	209	7970350		2011-06-28	SHEYNMAN, Arnold	
	210	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	211	8135388		2012-03-13	Gailloux, Michael A. et al.	
	212	6947723		2005-09-20	Gurnani, Roger et al.	
	213	8350700		2013-01-08	Fast, Raymond D. et al.	
	214	8204190		2012-06-19	Bang, Jung-Hee et al.	
	215	7865182		2011-01-04	Macaluso, Anthony G.	
	216	7962622		2011-06-14	Friend, John et al.	
	217	7583964		2009-09-01	Wong, Gregory A.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	218	7565141		2009-07-21	Macaluso, Anthony G.	
	219	7373179		2008-05-13	Stine, Ted et al.	
	220	7236780		2007-06-26	Benco, David S.	
	221	7039403		2006-05-02	Wong, Gregory A.	
	222	8370477		2013-02-05	Short, Joel E. et al.	
	223	8364806		2013-01-29	Short, Joel E. et al.	
	224	8279067		2012-10-02	BERGER, Thomas R. et al.	
	225	8213296		2012-07-03	SHANNON, Frank M. et al.	
	226	8019868		2011-09-13	RAO, Goutham et al.	
	227	8005988		2011-08-23	MAES, Stephane H.	
	228	7978627		2011-07-12	TAYLOR, William Scott et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	229	7711848		2010-05-04	MAES, Stephane H.	
	230	6782412		2004-08-24	BROPHY, Kevin et al.	
	231	6081591		2000-06-27	SKOOG, Frederick H.	
	232	6064878		2000-05-16	DENKER, John Stewart et al.	
	233	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	234	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	235	8156206		2012-04-10	KILEY, Kevin J. et al.	
	236	8126722		2012-02-28	ROBB, Terence Alan et al.	
	237	6754470		2004-06-22	Hendrickson, Keith et al.	
	238	8122128		2012-02-21	Burke, II, Robert M. et al.	
	239	8149823		2012-04-03	Turcan, Diane Brown et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	240	8131256		2012-03-06	MARTTI, Jyrki et al.	
	241	6381316		2002-04-30	JOYCE, Simon James et al.	
	242	7965983		2011-06-21	SWAN, Tim et al.	
	243	8284740		2012-10-09	O'CONNOR, Dennis M.	
	244	8116223		2012-02-14	TIAN, Dan et al.	
	245	6154738		2000-11-28	CALL, Charles Gainor	
	246	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	247	6035281		2000-03-07	Crosskey, James P. et al.	
	248	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	249	7760711		2010-07-20	Kung, Fen-Chung et al.	
	250	8000318		2011-08-16	Wiley, William L. et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	251	8098579		2012-01-17	Ray, Amar N. et al.	
	252	8155670		2012-04-10	Fullam, Scott et al.	
	253	8374090		2013-02-12	Morrill, Robert J. et al.	
	254	7457265		2008-11-25	Julka, Vibhor et al.	
	255	7729326		2010-06-01	Sekhar, Ramesh	
	256	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	257	7945945		2011-05-17	Graham, Richard et al.	
	258	8059530		2011-11-15	Cole, Terry L.	
	259	8280354		2012-10-02	Smith, Christopher et al.	
	260	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	261	8331293		2012-12-11	Sood, Kapil	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	262	8019820		2011-09-13	Son, Giyeong et al.	
	263	8155155		2012-04-10	Chow, Albert T. et al.	
	264	8191116		2012-05-29	Gazzard, Daryl	
	265	6292828		2001-09-18	Williams, David L.	
	266	7043226		2006-05-09	Yamauchi, Toshiaki	
	267	7472189		2008-12-30	Mallya, Arvind R. et al.	
	268	7944948		2011-05-17	Chow, Albert T. et al.	
	269	7802724		2010-09-28	Nohr, Steven Paul	
	270	8005009		2011-08-23	McKee, Neil et al.	
	271	7760861		2010-07-20	Croak, Marian et al.	
	272	8060463		2011-11-15	Spiegel, Joel R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	273	8224773		2012-07-17	Spiegel, Joel R.	
	274	8352980		2013-01-08	Howcroft, Jerald Robert	
	275	8386386		2013-02-26	Zhu, Kevin	
	276	8340718		2012-12-25	Colonna, Massimo et al.	
	277	8385896		2013-02-26	Proctor Jr., James A. et al.	
	278	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	279	8279864		2012-10-02	Wood, Daniel M.	
	280	8271045		2012-09-18	Parolkar, Satish et al.	
	281	8233883		2012-07-31	De Froment, Eric	
	282	8224382		2012-07-17	Bultman, Michael J.	
	283	8184590		2012-05-22	Rosenblatt, Ariel	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	284	8174970		2012-05-08	Adamczyk, Maria et al.	
	285	8165576		2012-04-24	Raju, Vishwanath et al.	
	286	8073721		2011-12-06	Lewis, Lundy	
	287	8032899		2011-10-04	Archer, Charles J. et al.	
	288	7974624		2011-07-05	Gallagher, Michael D. et al.	
	289	7907970		2011-03-15	Park, Vincent D. et al.	
	290	7778176		2010-08-17	Morford, Michael Robert	
	291	7725570		2010-05-25	Lewis, Lundy	
	292	7634388		2009-12-15	Archer, Charles J. et al.	
	293	7633438		2009-12-15	Tysowski, Piotr Konrad	
	294	7593417		2009-09-22	Wang, James et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	295	7551922		2009-06-23	Roskowski, Steve et al.	
	296	7545782		2009-06-09	Rayment, Stephen G. et al.	
	297	7039037		2006-05-02	Wang, Jiwei R. et al.	
	298	6928280		2005-08-09	Xanthos, James et al.	
	299	6765925		2004-07-20	Sawyer, Wilson et al.	
	300	5889477		1999-03-30	Fastenrath, Ulrich	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	1	1463238	EP		2004-09-29	Alcatel		☐
	2	1739518	EP		2007-01-03	Research In Motion Limited		☐
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		☐
	6	2003014891	WO		2003-02-20	The Boeing Company		☐
	7	2003058880	WO		2003-07-17	Telia AB		☐
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		☐
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		☐
	10	2004095753	WO		2004-11-04	Motorola Inc.		☐
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		☐
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		☐
	14	2006077481	WO		2006-07-27	TrueContext Corporation		☐
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		☐
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		☐
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		☐
	18	2007018363	WO		2007-02-15	Upresto, Inc.		☐
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		☐
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		☐
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		☐
	22	2008017837	WO		2008-02-14	Symbian Software Limited		☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		☐
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		☐
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		☐
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		☐
	27	2008099802	WO		2008-08-21	NEC Corporation		☐
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		☐
	29	2006120558	WO		2006-11-16	Nokia Corp.		☐
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	34	2005008995	WO		2005-01-27	Starhub Ltd.		☐
	35	1998058505	WO		1998-12-23	Sonera Oy		☐
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	☐
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
	17	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	06/17/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6578076	B1	2003-06-10	Putzolu, David Matthew	
	2	7084775	B1	2006-08-01	Smith, Michael R.	
	3	7133695	B2	2006-11-07	Beyda, William J.	
	4	7260382	B1	2007-08-21	Lamb et al.	
	5	7271765	B2	2007-09-18	Stilp et al.	
	6	7627872	B2	2009-12-01	Hebeler et al.	
	7	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	8	7685530	B2	2010-03-23	Sherrard et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	7760137	B2	2010-07-20	Martucci et al.	
	10	7843843	B1	2010-11-30	Albert L. Papp et al.	
	11	7925778	B1	2011-04-12	Wijnands et al.	
	12	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	13	7937450	B2	2011-05-03	Janik, Craig M.	
	14	8010082	B2	2011-08-30	Sutaria et al.	
	15	8019846	B2	2011-09-13	ROELENS et al.	
	16	8050705	B2	2011-11-01	Sicher et al.	
	17	8086791	B2	2011-12-27	Caulkins, Jason	
	18	8103285	B2	2012-01-24	Kalhan, Amit	
	19	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	20	8233433	B2	2012-07-31	Kalhan, Amit	
	21	8259692	B2	2012-09-04	Bajko, Gabor	
	22	8406736	B2	2013-03-26	Das et al.	
	23	8489110	B2	2013-07-16	Frank et al.	
	24	8495181	B2	2013-07-23	Venkatraman et al.	
	25	8532610	B2	2013-09-10	Manning Cassett et al.	
	26	8571598	B2	2013-10-29	Valavi, John J.	
	27	8634425	B2	2014-01-21	Gorti et al.	
	28	8739035	B2	2014-05-27	Trethewey, Jim	
	29	8825109	B2	2014-09-02	Montemurro et al.	
	30	8831561	B2	2014-09-09	Sutaria et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	31	8880047	B2	2014-11-04	Konicek et al.	
	32	8930238	B2	2015-01-06	Coffman et al.	
	33	8977284	B2	2015-03-10	Reed, Mark J.	
	34	9014973	B2	2015-04-21	Ruckart, John	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070293191	A1	2007-12-20	Mir et al.	
	5	20070294410	A1	2007-12-20	Pandya et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	6	20080050715	A1	2008-02-28	Golczewski et al.	
	7	20080282319	A1	2008-11-13	Fontijn et al.	
	8	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	9	20100151866	A1	2010-06-17	Karpov et al.	
	10	20110145920	A1	2011-06-16	Mahaffey et al.	
	11	20130326356	A9	2013-12-05	Zheng et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	3	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	4	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	06/30/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination	
14/667,353	RALEIGH, GREGORY G.	
Examiner	**Art Unit**	
ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
370	252,351	6/30/2015	AJR
380	44, 277	6/30/2015	AJR
705	28	6/30/2015	AJR
709	229,238	6/30/2015	AJR
713	150	6/30/2015	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	6/30/2015	AJR
Inventor name search conducted.	6/30/2015	AJR
Bibliographic data updated	6/17/2015	AJR

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 8845

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/667,353	03/24/2015 RULE	705	3687	RALEP007C11C3

APPLICANTS
Headwater Partners I LLC, Redwood City, CA;

INVENTORS
Gregory G. Raleigh, Woodside, CA;

**** CONTINUING DATA **************************
This application is a CON of 14/263,604 04/28/2014 PAT 9037127
which is a CON of 12/380,780 03/02/2009 PAT 8839388
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

**** FOREIGN APPLICATIONS **************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
04/02/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /ANDREW JOSEPH RUDY/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	106	21	1

ADDRESS
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065
UNITED STATES

TITLE
Mobile device with common secure wireless message service serving multiple applications

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
1570	No._____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No._____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)
		☐ Other _____
		☐ Credit

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3

CONFIRMATION NO. 8845

106963
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

PUBLICATION NOTICE

OC000000076323947

Title: Mobile device with common secure wireless message service serving multiple applications

Publication No.US-2015-0201331-A1
Publication Date:07/16/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	Rudy, Andrew J.
Serial No.:	14/667,353	Art Unit:	3687
Filed:	March 24, 2015	Conf. No.:	8845
Title:	Mobile Device With Common Secure Wireless Message Service Serving Multiple Applications		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

In response to the Office Action dated July 10, 2015, the deadline for response being October 12, 2015, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 6.

AMENDMENTS TO THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Canceled).

2. (Currently Amended) A mobile end-user-area device comprising:

a wireless wide-area network (WWAN) modem ~~configurable~~ to exchange Internet data via a connection to a first WWAN, when configured for and connected to the first WWAN;

a device messaging agent to receive secure Internet data messages, on behalf of a plurality of software applications capable of execution on the device, and over a secure connection to a network message server reachable via the WWAN, wherein at least a subset of the secure Internet data messages contain an identifier for a corresponding one of the software applications and application data from a respective network application server corresponding to that application; and

a secure interprocess communication service, wherein the device messaging agent, for each message in the subset of the secure Internet data messages, maps the identifier to the corresponding one of the software applications in order to forward the application data on the secure interprocess communication service to a software process corresponding to the identified software application.

3. (Previously Presented) The mobile end-user device of claim 2, further comprising the plurality of software applications.

4. (Previously Presented) The mobile end-user device of claim 3, wherein the plurality of applications include a first application that receives the application data in a first format, and a second application that receives the application data in a second format different than the first format.

5. (Previously Presented) The mobile end-user device of claim 2, wherein the secure Internet data messages are received encrypted, the device messaging agent decrypting each message in the subset to obtain the corresponding identifier and application data.

6. (Currently Amended) The mobile end-user device of claim 5, wherein the secure Internet data messages are transported to the device messaging agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and transport via a tunnel ~~tunneling~~.

7. (Previously Presented) The mobile end-user device of claim 2, wherein at least one of the applications comprises a service downloader, the service downloader authenticating a downloaded software application based on application data from at least one of the secure Internet data messages.

8. (Currently Amended) The mobile end-user device of claim 7, wherein the service ~~software~~ downloader is to download the downloaded software application using an Internet data connection other than the secure connection used for the secure Internet data messages.

9. (Previously Presented) The mobile end-user device of claim 7, wherein the downloaded software application comprises an updated version of the device messaging agent.

10. (Previously Presented) The mobile end-user device of claim 2, wherein the device messaging agent runs in a secure execution environment on the device, and at least one of the applications runs outside of the secure execution environment on the device.

11. (Previously Presented) The mobile end-user device of claim 2, wherein the device messaging agent is further to send secure upload Internet data messages to the network message server over the secure connection, wherein at least a subset of the secure upload Internet data messages are sent responsive to a corresponding request received on the secure interprocess communication channel from a corresponding one of the software applications, the device messaging agent constructing from each such request a secure upload Internet data message containing:

an identifier for a respective network application server corresponding to the requesting software application; and

content received with the request.

12. (Previously Presented) The mobile end-user device of claim 11, wherein at least one of the upload Internet data messages comprises a key for the network application server corresponding to the requesting software application.

13. (Currently Amended) The mobile end-user device of claim 2, wherein the device messaging agent ~~is configurable to~~ creates a log for the received secure Internet data messages.

14. (Previously Presented) The mobile end-user device of claim 2, wherein the secure interprocess communication channel and the secure connection to the network message server are separately secured.

15. (Previously Presented) The mobile end-user device of claim 2, wherein access by the software applications to the interprocess communication channel is subject to a security policy.

16. (Previously Presented) The mobile end-user device of claim 2, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.

17. (Previously Presented) The mobile end-user device of claim 2, the device messaging agent comprising an agent router to forward the application data on the secure interprocess communication channel to the software process corresponding to the identified software application.

18. (Previously Presented) The mobile end-user device of claim 2, wherein the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format.

19. (Previously Presented) The mobile end-user device of claim 2, the device messaging agent further to initiate the secure connection to the network message server.

20. (Previously Presented) The mobile end-user device of claim 2, further comprising a network stack in communication with the device messaging agent and the WWAN modem, the secure connection terminated within the network stack.

21. (Previously Presented) The mobile end-user device of claim 2, wherein at least one of the applications and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent and network message server.

22. (Currently Amended) The mobile end-user device of claim 2, further comprising a wireless local area network (WLAN) modem ~~configurable~~ to exchange Internet data via a connection to a first WLAN, when configured for and connected to the first WLAN, the device messaging agent further ~~configurable~~ to receive [[the]] secure Internet data messages over a secure connection via the first WLAN to the network message server.

REMARKS

Claims 2-22 are pending and stand rejected by the Office Action dated July 10, 2015. Claim 1 was previously canceled. Applicant has amended claims 2, 6, 8, 13, and 22. In view of the amendments to the claims and the following remarks, Applicant respectfully requests reconsideration.

In section 4, the Office Action rejects claims 2-22 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. Applicant addresses each particular rejection in order below. As a preliminary comment, however, the specification and drawings are rich in examples—Applicant has not endeavored to find all possible support for the claim terms, and the citation to specific examples below is intended to illustrate that those skilled in the art have the material at hand to ascertain what is meant by the various terms, while not precluding an appropriate inquiry into the actual scope of a claim by one skilled in the art and/or a tribunal tasked with such an effort.

Claim 2, line 3: The Office Action states that "a first WWAN" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The modifier "first" is merely indicative that this is an identifiable WWAN to which the modem can connect, and there could be several. Figure 3, for example, illustrates the existence of multiple WWAN networks and central providers that a device can roam between. (Specification at [00115]). Figure 8 illustrates a network architecture for service-processor-enabled wireless devices, with exemplary ones of the devices connected to selected ones of multiple wireless access networks described as "3G and 4G Wireless Wide Area Networks (WWANs)." (Specification at [0012]). The specification states "[i]t is a common network architecture for multi-access central providers to have one or more wired access networks and one or more wireless networks. As shown, Figure 8 includes both 3G and 4G wireless access networks, including a 4G base station 125 and a 3G base station 125…" Figure 9 includes a basic structure for a mobile end-user device that includes a service processor 115 (e.g., like the devices shown in Figure 8) and the accompanying text describes modem aspects. (Specification at [00135]). Figure 11 and accompanying text describes another WWAN embodiment. (Specification at [00141]-[00145]). Figure 18 shows a

device with a modem selection and control 1811 to select an access network connection, and multiple modem drivers/modems including a WWAN modem driver. (Specification at [00301]; *see also* Figure 21 and [00314]). Finally, with particular applicability to the present messaging claims, paragraph [00322] states that "embodiments described herein disclose a secure and bandwidth efficient control plane that … provides for consistent device assisted service monitoring, control, verification and/or billing while roaming across multiple networks with different access technologies…." Such examples clarify a variety of ways in which the WWAN modem of claim 1 can achieve a connection to a first WWAN, and based on such, one skilled in the art would readily understand the meaning of a "first WWAN" in claim 1.

Claim 2, line 4: The Office Action states that "a device messaging agent" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The specification states that the service processor "includes various components, such as device agents, that perform service policy implementation or management functions" including "service control plane communication." (Specification at [00100]). This same paragraph acknowledges that the division of functionality between agents is a design choice and "that the placing divisions on the naming and functional breakouts for device agents aids in understanding." (*Id.*). For instance, Figure 18, also referenced in the paragraph above, illustrates a device messaging agent embodiment as a "service control device link 1691" with messaging functionality as described in claim 2 and acknowledged to be, in some embodiments, "equivalent to an agent for communication purposes." (*Id.* at [00184]). The service control device link is further illustrated in Figure 24, and the data units passed between the service control server link and the service control device link are referred to interchangeably as "communications," "communication messages," and "messages." (*Id.* at [00323]-[00327]; *see also* [00173]-[00181] for message examples). Applicant has selected the most predominantly used one of the synonymous terms ("messages") as descriptive of the device agent in the claims, thus "device messaging agent" is the selected term. The term "device messaging agent" is preferred over the more embodiment-limited term "service control device link" as the specification envisions such an agent being useful for more than just service control, e.g., also useful to manage "a set of secure messages that allow communication between certain agents or service processor functions and entities outside of the service processor operating environment." (*Id.* at [00184]). Applicant respectfully

submits that such specification teachings, in conjunction with the further descriptive limitations present in claim 2, present a clear meaning for the claim term "device messaging agent."

Claim 2, lines 4-5: The Office Action states that "on behalf of a plurality of software applications" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. For the various device agents, functions, and other entities that execute on the device and can receive messages from the device messaging agent, various embodiments describe such entities as implemented in software as different software components, applications and/or agents. (Specification at [0089], [00100], [00186]). The idiom "on behalf of" is used in its ordinary meaning indicating operation in a proxy capacity—thus the term "on behalf of a plurality of software applications capable of execution on the device" as understood from the specification merely indicates that the secure Internet data messages are directed to the device messaging agent, with the expectation that the device messaging agent will deliver the internal contents of the messages to the appropriate processes on the device based on the application ID(s) in each message.

Claim 2, line 6: The Office Action states that "a network message server" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The "service controller 122" shown throughout the drawings and described throughout the specification "in various embodiments includes one or more server functions." (Specification at [00101]). The specification clarifies "that the server names and functional breakouts do not imply that each name is an individual server, and, for example, a single named function in the various embodiments can be implemented on multiple servers, or multiple named functions in the various embodiments can be implemented on a single server." (*Id.*). In this context, Figure 18 illustrates an embodiment of a "network message server"—the "service control server link 1638" that communicates with a given device over a "service control link 1653" that is reachable over the WWAN. The specification describes this server link as important to provide "an efficient and flexible control plane communication link between the device agents (e.g., of the service processor) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy." (Specification at [00259]). This paragraph further provides "this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122." (*Id.*). Although a typographical error appears to

have omitted the word "messages," this same paragraph also states that "the service control server link 1638 provides the network side of a system for transmission and reception of service agent [messages] to/from network element functions." (*Id.*). Further, the specification states that "it is assumed that the device base[d] service control plane channel for service processor 115 to service controller 122 communications is established through the Internet 120 or through the access network using IP protocols as this is the more general case and applies to overlay network applications for various embodiments…" (*Id.* at [00105]). Accordingly, it is clear from the specification that the "network message server" is the network-side peer of the "device messaging agent," and is responsible for formatting and sending the messages received by the device messaging agent, as further limited by the claim features.

Claim 2, line 7: The Office Action states that "a subset of the secure Internet data messages" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The use of the language "at least a subset" is intended to indicate that the secure Internet data messages sent to the device messaging agent can be sent for multiple purposes, only one of which is to provide data to applications. For instance, in Figure 18 the service control device link communicates with multiple applications/agents over bus 1630, but also is in direct communication with service downloader 1663. As described in the specification, software elements can be communicated to the device, using device link 1691, as single files or as multiple messages that the service downloader aggregates, verifies, and installs. (Specification at [00182]).

Claim 2, line 8: The Office Action states that "an identifier" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. One example of such an identifier is shown in the Figure 25 multi-message frame format, where each separate message payload comprises an agent function ID, a message length, and the message data. Thus one skilled in the art will understand that the identifier is a value that the device messaging agent and network message server both associate with an agent/function/process/application on the device.

Claim 2, line 11: The Office Action states that "a secure interprocess communication service" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. As shown, e.g., in the Figure 24 embodiment, the device messaging agent "Agent Route 2416" element 2416 routes the unpacked messages to the appropriate software process/agent over an agent communication bus 1630. (Specification at [00183]-[00186],

[00325]). In various embodiments the secure interprocess communication service is embodied as "an inter-process software communication bus," which can be "a variant of D-bus (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another)," or "another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, signed, encrypted or otherwise protected." (*Id.* at [00186]).

Claim 4, lines 2-3: The Office Action states that "a first application," "a first format," "a second application," and "a second format" are not clear from the descriptive portion of the specification in juxtaposition to the drawings. As discussed above, the software elements that can receive the messages can be embodied as different software components, agents, and/or applications. As depicted, e.g., in Figure 18, many different ones of these elements can all use the message service (e.g., elements 1690, 1692, 1693, 1694, 1695, 1696, 1697, 1655, 1804 couple to the communication bus in Figure 18). Thus the use of "first" and "second" applications merely indicates two such elements that receive different types of formatted data in the messages from their respective network application servers. The specification contains many examples of the "first" and "second" data formats. For instance, Figures 26A-H illustrate different types of data that are messaged between different network application servers and different device applications. Many other examples and further details exist in the specification.

Claim 5, lines 2-3: The Office Action states that "the device messaging agent decrypting each message in the subset" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Figure 24 shows, within an embodiment 1691 of a device messaging agent, a "decode element 2412" which the specification describes as "for decoding any received service controller 122 communications (e.g., decrypting encrypted communications)." (Specification at [00325]).

Claim 6, lines 2-3: The Office Action states that "one or more of encryption on a transport services stack ... and tunneling" is not clear from the descriptive portion of the specification in juxtaposition to the drawings, and that the term "and tunneling" is improper syntax in juxtaposition to the term "one or more" preceding it. Applicant has modified the syntax of the claim. The different alternatives called out in the claim, including an explanation that multiple ones of them may be used together, appear in paragraph [00323] of the specification.

Claim 8, lines 1-3: The Office Action states that "the service downloader ... secure Internet messages" is not clear from the descriptive portion, e.g. service downloader 1663, of the specification in juxtaposition to the drawings. Applicant has corrected an inadvertent error in claim 8, wherein the "service downloader" was inadvertently called out as a "software downloader." Support for the claim limitation may be found, e.g., as follows: "[i]n some embodiments, the files [for a software download] are sent using other delivery means, such [as] a direct TCP socket connection to the service downloader 1663 or some other software installer, which can also involve secure transport and additional levels of encryption." (Specification at [00182]).

Claim 11, lines 1-10: The Office Action states that "the mobile end-user ... content received with the request" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Claim 11 is intended to cover the reverse or upload channel that allows various device applications to send data to a respective corresponding application server. The supporting sections of text for the forward or download channel, identified in the comments regarding claim 2 above are instructive as analogous. (See, e.g., Specification at [00259], "this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122."). Figure 24 shows that the device messaging agent contains "framing" and "encrypt" functions, like the server-side peer, to prepare and package upload messages. Figure 25 shows analogous message constructs for upload and download messages. The "service control server link 1638 provides the network side of a system for transmission and reception of service agent to/from network element functions." (Specification at [00259]).

Claim 12, lines 1-2: The Office Action states that "at least one of the upload ... a key for the network" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Secure device agent-to-corresponding network element communication examples, including various types of keys and signing, are described, e.g., at specification paragraphs [00173]-[00181].

Claim 13, line 2: The Office Action states that "to create a log... data messages" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Specification paragraph [00191] describes a communication trace log for, e.g., "service controller 122 to agent communications."

Claim 15, lines 2-3: The Office Action states that "the interprocess... security policy" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Specification paragraph [00185] describes several different security policies that can be used to limit application access to the agent bus, which as described above is an embodiment of the secure interprocess communication channel.

Claim 16, lines 1-2: The Office Action states that "the secure ... identifier/data pairs" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. Figure 25 illustrates such a message structure, wherein the portion of the data message after the framing sequence and time stamp is composed of a variable number of agent messages, each formatted as an agent identifier with a paired message payload (length field followed by a message of that length). (Specification at [00326]-[00327]).

Claim 17, lines 2-4: The Office Action states that "an agent.... software application" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The device messaging agent embodiment of Figure 24 includes an "agent route" function 2416 to route the messages to the appropriate software process over the interprocess communication channel 1630. (Specification at [00325]).

Claim 20, lines 1-2: The Office Action states that "a network stack... within the network stack" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. The traffic monitoring function is taught to monitor various kinds of traffic, including "traffic transmitted and/or received by one or more activities associated with the service control plane link or other network related functions…" (Specification at [00221]). The traffic monitoring function is shown implementing measurement at various points in the network stack in Figures 29-37, and the stack is shown in several of these figures in communication with one or more modems (one of which can be a WWAN modem), thus it can be readily understood that the measured traffic passes through the stack (IP and TCP layers are also shown). Finally, the methods for providing security layers for the communications link used for the service control device link include "basic IP layer security" and "TCP layer security." (Specification at [00260]). Accordingly, those skilled in the art will understand that the secure connection can include security terminated in the network stack illustrated in the figures.

Claim 21, lines 1-2: The Office Action states that "at least one of the applications ... network message server" is not clear from the descriptive portion of the specification in

juxtaposition to the drawings. One example of this is the challenge/response example in paragraphs [00178]-[00179], e.g., between the access control integrity server and the policy implementation agent.

Claim 22, line 3: The Office Action states that "a first WLAN" is not clear from the descriptive portion of the specification in juxtaposition to the drawings. As addressed above with regard to claim 2, the term "first" merely indicates one of several potential WLAN connections. Specification paragraph [00257] describes several considerations for WLAN connection and network selection. Figure 6 shows one example where service-processor-equipped mobile devices connect to a service controller over either a WWAN or a WLAN.

The Office Action further notes "that Applicant's claim language is replete with intended use claim language, e.g. claim 2, line 2, 'configurable to,' that does not affirmatively limit the positively recited claim language, e.g. claim 2, line 1, 'A mobile end user device.'" Applicant has revised the claims to replace "configurable to" language, as suggested.

CONCLUSION

Applicant respectfully requests entry of these amendments as provided herein. The application is believed to be in condition for allowance, and a Notice of Allowance is hereby respectfully requested. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: October 9, 2015 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Oct. 9, 2015 By: /Ann Taylor/
Ann Taylor

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	5974439	A	1999-10-26	Bollella, Gregory	
	4	6393014	B1	2002-05-21	Daly et al.	
	5	6397259	B1	2002-05-28	Lincke et al.	
	6	6445777	B1	2002-09-03	Clark, Curtis	
	7	6628934	A	2003-09-30	Rosenberg et al.	
	8	6662014	B1	2003-12-09	Walsh, Patrick Jay	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	6901440	B1	2005-05-31	Bimm et al.	
	11	6970692	B2	2005-11-29	Tysor, Arthur James	
	12	7007295	B1	2006-02-28	Rose et al.	
	13	7017189	B1	2006-03-21	DeMello et al.	
	14	7039027	B2	2006-05-02	Bridgelall, Raj	
	15	7047276	B2	2006-05-16	Liu et al.	
	16	7058022	B1	2006-06-06	Carolan et al.	
	17	7149521	B2	2006-12-12	Sundar et al.	
	18	7162237	B1	2007-01-09	Silver et al.	
	19	7200112	B2	2007-04-03	Sundar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	20	7203752	B2	2007-04-10	Rice et al.	
	21	7222190	B2	2007-05-22	Klinker et al.	
	22	7224968	B2	2007-05-29	Dobson et al.	
	23	7266371	B1	2007-09-04	Amin et al.	
	24	7366654	B2	2008-04-29	Moore, Robert C.	
	25	7379731	B2	2008-05-27	Natsuno et al.	
	26	7391724	B2	2008-06-24	Alakoski et al.	
	27	7395244	B1	2008-07-01	Kingsford, Bryan	
	28	7411930	B2	2008-08-12	Montojo et al.	
	29	7454191	B2	2008-11-18	Dawson et al.	
	30	7457870	B1	2008-11-25	Lownsbrough et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	31	7508799	B2	2009-03-24	Sumner et al.	
	32	7515926	B2	2009-04-07	Bu et al.	
	33	7536695	B2	2009-05-19	Alam et al.	
	34	7554983	B1	2009-06-30	Muppala, Suresh	
	35	7564799	B2	2009-07-21	Holland et al.	
	36	7586871	B2	2009-09-08	Hamilton et al.	
	37	7627767	B2	2009-12-01	Sherman et al.	
	38	7752330	B2	2010-07-06	Olsen et al.	
	39	7792257	B1	2010-09-07	Vanier et al.	
	40	7801783	B2	2010-09-21	Kende et al.	
	41	7817615	B1	2010-10-19	Breau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	42	7844034	B1	2010-11-30	Oh et al.	
	43	7849161	B2	2010-12-07	Koch et al.	
	44	7849477	B2	2010-12-07	Cristofalo et al.	
	45	7860088	B2	2010-12-28	Lioy, Marcello	
	46	7865187	B2	2011-01-04	Ramer et al.	
	47	7894431	B2	2011-02-22	Goring et al.	
	48	7899039	B2	2011-03-01	Andreasen et al.	
	49	7933274	B2	2011-04-26	Verma et al.	
	50	7978686	B2	2011-07-12	Goyal et al.	
	51	7987496	B2	2011-07-26	Bryce et al.	
	52	7990049	B2	2011-08-02	Shioya, Shunsuke	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	53	8005726	B1	2011-08-23	Bao, Yulin	
	54	8050690	B2	2011-11-01	Neeraj, Chawla	
	55	8073427	B2	2011-12-06	Koch et al.	
	56	8086398	B2	2011-12-27	Sanchez et al.	
	57	8104080	B2	2012-01-24	Burns et al.	
	58	8107953	B2	2012-01-31	Zimmerman et al.	
	59	8112435	B2	2012-02-07	Epstein et al.	
	60	8150394	B2	2012-04-03	Bianconi et al.	
	61	8180886	B2	2012-05-15	Overcash et al.	
	62	8190122	B1	2012-05-29	Alexander et al.	
	63	8195661	B2	2012-06-05	Kalavade, Asawaree	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	64	8200163	B2	2012-06-12	Hoffman, George E.	
	65	8200818	B2	2012-06-12	Freund et al.	
	66	8208788	B2	2012-06-26	Ando et al.	
	67	8254880	B2	2012-08-28	Aaltonen et al.	
	68	8270955	B2	2012-09-18	Ramer et al.	
	69	8326828	B2	2012-12-04	Zhou et al.	
	70	8331223	B2	2012-12-11	Hill et al.	
	71	8339991	B2	2012-12-25	Biswas et al.	
	72	8358975	B2	2013-01-22	Bahl et al.	
	73	8385964	B2	2013-02-26	Haney, Richard D.	
	74	8503455	B2	2013-08-06	Heikens, Heico	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	75	8504032	B2	2013-08-06	Lott et al.	
	76	8522337	B2	2013-08-27	Adusumilli et al.	
	77	8527662	B2	2013-09-03	Biswas et al.	
	78	8533775	B2	2013-09-10	Alcorn et al.	
	79	8538394	B2	2013-09-17	Zimmerman et al.	
	80	8538458	B2	2013-09-17	Haney, Richard D.	
	81	8565746	B2	2013-10-22	Hoffman, George E.	
	82	8571501	B2	2013-10-29	Miller et al.	
	83	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	84	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	85	8644813	B1	2014-02-04	Gailloux et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	86	8667542	B1	2014-03-04	Bertz et al.	
	87	8713535	B2	2014-04-29	Malhotra et al.	
	88	8713641	B1	2014-04-29	Pagan et al.	
	89	8730842	B2	2014-05-20	Collins et al.	
	90	8732808	B2	2014-05-20	Sewall et al.	
	91	8761711	B2	2014-06-24	Grignani et al.	
	92	8793304	B2	2014-07-29	Lu et al.	
	93	8948726	B2	2015-02-03	Smith et al.	
	94	8966018	B2	2015-02-24	Bugwadia et al.	
	95	9002342	B2	2015-04-07	Tenhunen et al.	
	96	RE44412		2013-08-06	Naqvi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020154751	A1	2002-10-24	Thompson et al.	
	2	20020191573	A1	2002-12-19	Whitehill et al.	
	3	20030084321	A1	2003-05-01	Tarquini et al.	
	4	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	5	20040260766	A1	2004-12-23	Barros et al.	
	6	20050041617	A1	2005-02-24	Huotari et al.	
	7	20060095517	A1	2006-05-04	O'Connor et al.	
	8	20060098627	A1	2006-05-11	Karaoguz et al.	
	9	20060136882	A1	2006-06-22	Noonan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	10	20060143066	A1	2006-06-29	Calabria	
	11	20070073899	A1	2007-03-29	Judge et al.	
	12	20070174490	A1	2007-07-26	Choi et al.	
	13	20070234402	A1	2007-10-04	Khosravi et al.	
	14	20080018494	A1	2008-01-24	Waite et al.	
	15	20080034063	A1	2008-02-07	Yee, Robert	
	16	20090048913	A1	2009-02-19	Shenfield et al.	
	17	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
	18	20090181662	A1	2009-07-16	Fleischman et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-10-09
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

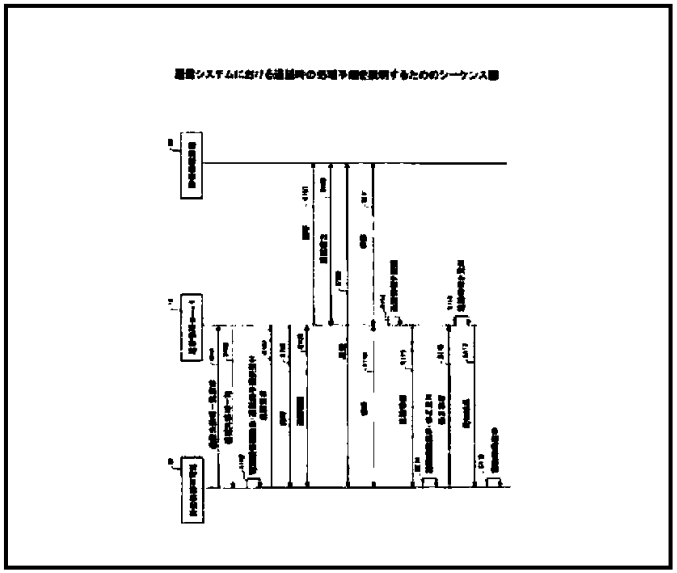
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(11)Publication number 2009-232107
(43)Date of publication of application 08.10.2009
(51)Int.Cl. *H04M 15/00 (2006.01)*

(21)Application number 2008-074306
(22)Date of filing 21.03.2008
(71)Applicant FUJITSU LTD
(72)Inventor TSUJIUCHI HIDETOSHI



(54)SPEECH COMMUNICATION INFORMATION RECORDING PROGRAM, SPEECH COMMUNICATION INFORMATION RECORDING APPARATUS AND SPEECH COMMUNICATION INFORMATION RECORDING METHOD

(57)Abstract
PROBLEM TO BE SOLVED: To provide a speech communication information recording program, a speech communication information recording apparatus and a speech communication information recording method, for appropriately dividing the burden origin of a call charge for one telephone number.
SOLUTION: A computer is made to execute: a procedure of receiving information specifying a call originating telephone number and information specifying a call terminating telephone number from a telephone set on a call originating side; a speech communication relay procedure of establishing speech communication between the telephone set on the call originating side and the telephone set on the call terminating side on the basis of the received information; a billing destination determination procedure of determining a billing destination for the call terminating telephone number using a management means for managing the identification information of the billing destination of the call charge by telephone number; and a billing destination recording procedure of relating the identification information of the determined billing destination and the identification information of the speech communication and recording them in a storage device.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-232107
(P2009-232107A)
(43)公開日　平成21年10月8日(2009.10.8)

(51)Int.Cl.		F I		テーマコード（参考）
H04M 15/00	(2006.01)	H04M 15/00	E	5K025

審査請求 未請求　請求項の数 7　OL　（全 21 頁）

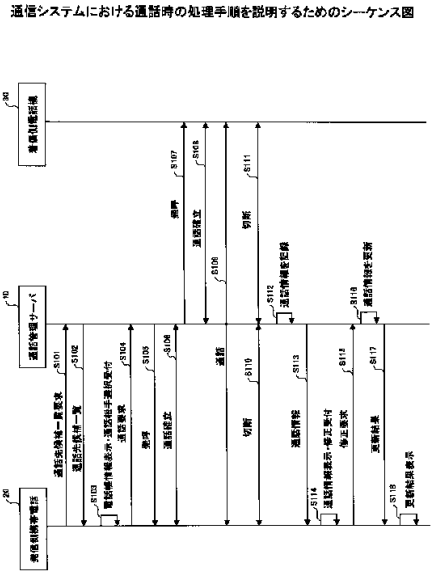
(21)出願番号　特願2008-74306(P2008-74306)
(22)出願日　平成20年3月21日(2008.3.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　辻内　秀敏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K025 AA01　CC01　CC07　GG10　GG12

(54)【発明の名称】通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法

(57)【要約】
【課題】一つの電話番号に対する通話料の負担元を適切に区分することのできる通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法の提供を目的とする。
【解決手段】コンピュータに、発信側の電話機より発信電話番号を特定する情報と着信電話番号を特定する情報とを受信する手順と、受信された情報に基づいて前記発信側の電話機と着信側の電話機との間の通話を確立する通話中継手順と、電話番号ごとに通話料の請求先の識別情報を管理する管理手段を用いて、前記着信電話番号に対する請求先を判定する請求先判定手順と、判定された請求先の識別情報と前記通話の識別情報とを関連付けて記憶装置に記録する請求先記録手順とを実行させることにより上記課題を解決する。
【選択図】図４



10

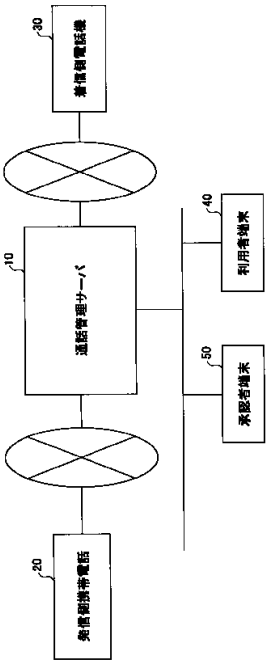
20

30

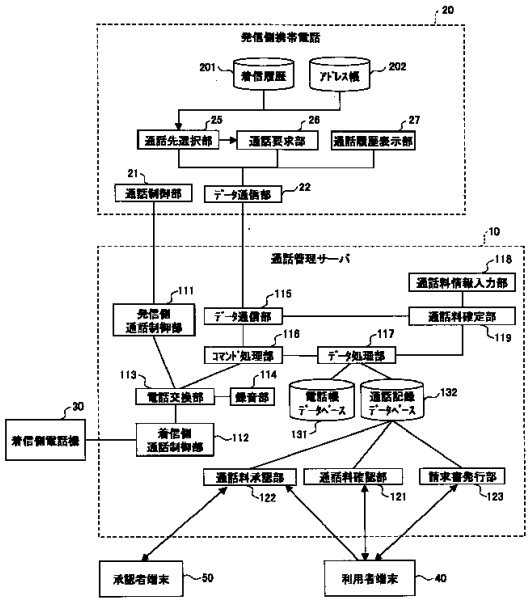
40

50

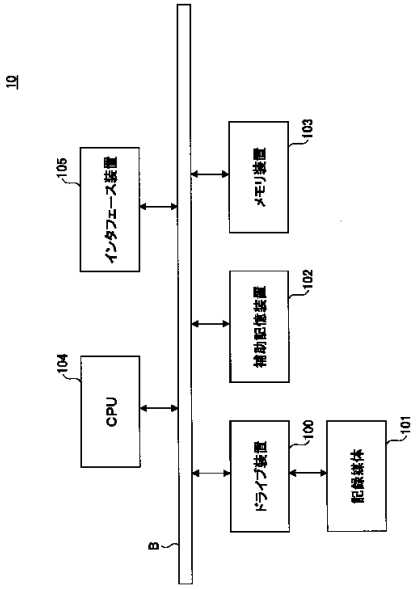
本発明の実施の形態における通信システム構成例を示す図



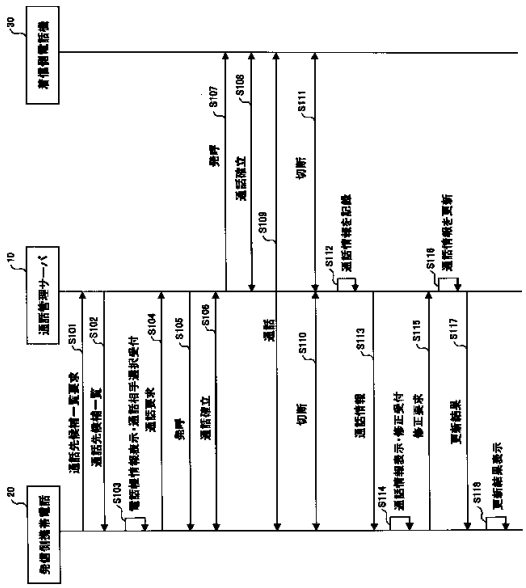
本発明の実施の形態における通信システムの機能構成例を示す図



本発明の実施の形態における通話管理サーバのハードウェア構成例を示す図



通信システムにおける通話時の処理手順を説明するためのシーケンス図

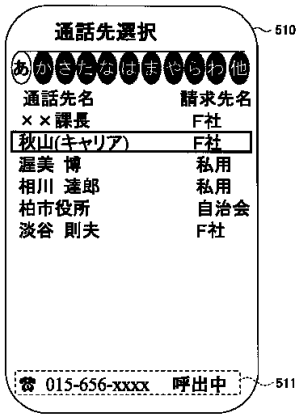


電話帳データベースの構成例を示す図

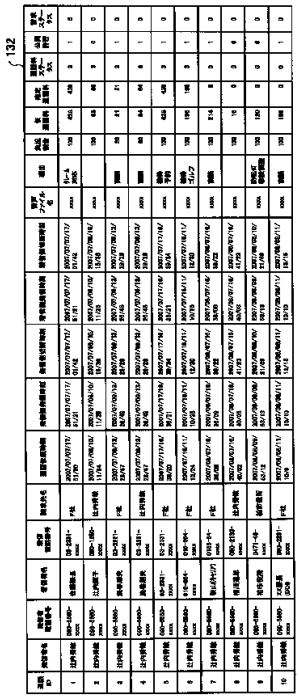
131

発信者名	発信者電話番号	通話先名	通話先電話番号	関係	請求先名	メールアドレス
辻内秀敏	090-5560-xxxx	辻内園子	090-1250-xxxx	妻	辻内秀敏	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	渡谷則夫	03-3221-xxxx	投上電器	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	柏市役所	0471-46-xxxx	自治会	柏市役所	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	佐藤耕兵	03-2331-xxxx	OO商事	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	秋山(キャリア)	0156-64-xxxx	F社	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	相川達郎	050-2133-xxxx	親戚	辻内秀敏	
辻内秀敏	090-5560-xxxx	××課長	090-2231-xxxx	顧客	F社	xxx@xxxxxxx

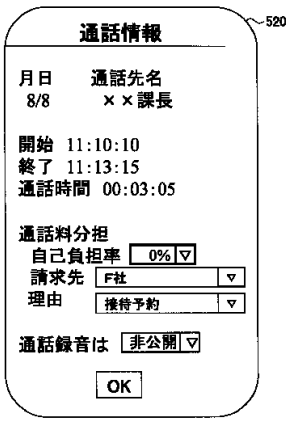
通話先選択画面の表示例を示す図



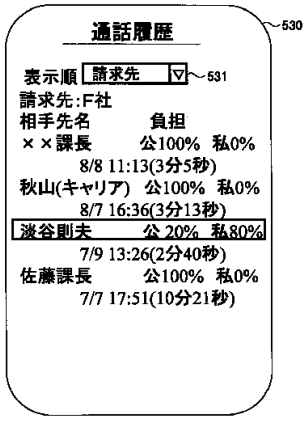
通話記録データベースの構成例を示す図



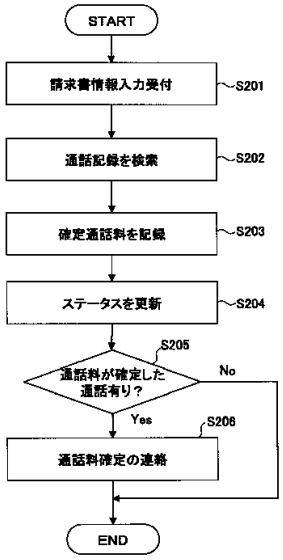
通話情報画面の表示例を示す図



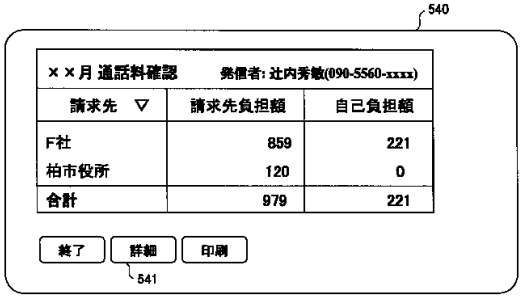
通話履歴画面の表示例を示す図



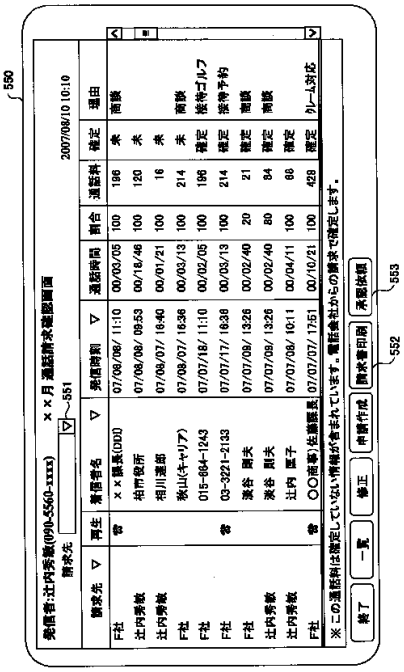
通話料の請求に応じて通話管理サーバによって実行される通話料の確定処理の処理手順を説明するためのフローチャート



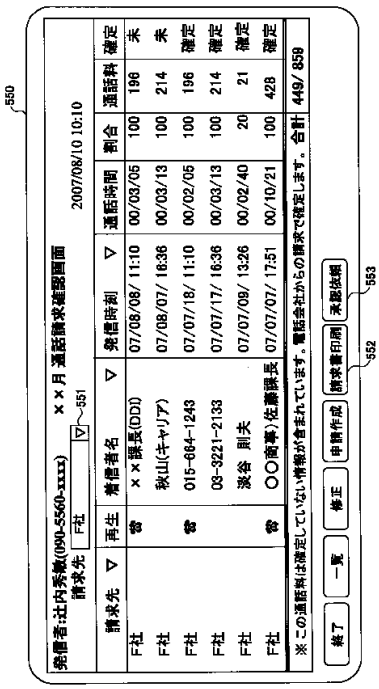
通話料確認画面の表示例を示す図



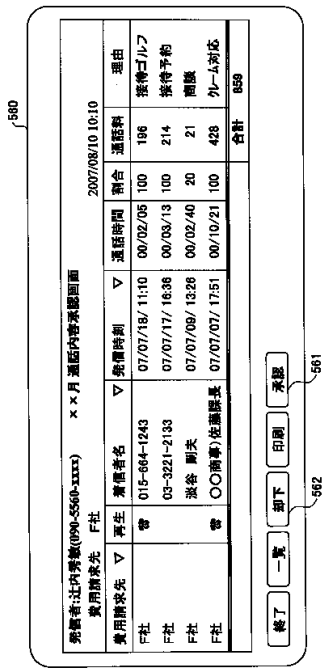
通話料確認詳細画面の表示例を示す図



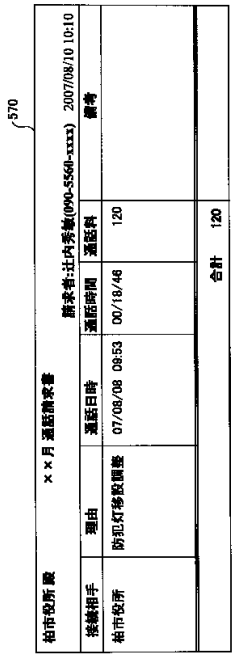
請求先が所属企業に絞り込まれた場合の通話料詳細画面の表示例を示す図



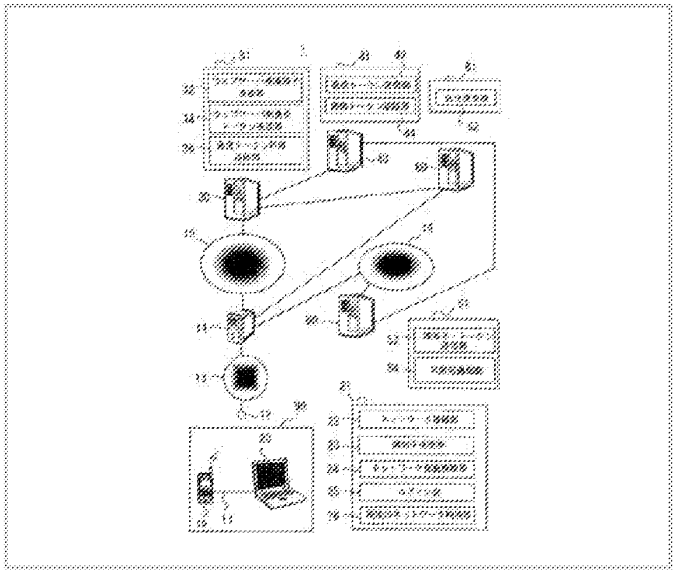
承認画面の表示例を示す図



請求書画面の表示例を示す図



(11)Publication number	2009-111919
(43)Date of publication of application	21.05.2009
(51)Int.Cl.	***H04L 12/56 (2006.01)*** ***H04M 15/00 (2006.01)*** ***H04M 11/00 (2006.01)***
(21)Application number	2007-284415
(22)Date of filing	31.10.2007
(71)Applicant	KYOCERA COMMUNICATION SYSTEMS CO LTD
(72)Inventor	MASUDA KEIICHI



(54)SYSTEM, PROGRAM AND RECORDING MEDIUM FOR BILLING DATA COMMUNICATION FEE, AND METHOD OF BILLING DATA COMMUNICATION FEE

(57)Abstract

PROBLEM TO BE SOLVED: To provide a system or the like for billing a data communication fee, which can make account separately between official and private expenses when accessing a predetermined network 16 in a business-related matter, and which is also highly reliable as viewed from the carrier side.

SOLUTION: When a mobile party purchases a communication token T for a given network 16, the mobile party transmits the ID of the mobile phone 10 to a communication token issuing server 40 through the web server 30. The communication token T is generated based on the ID and transmitted to a PC 20 through the web server 30 and the mobile phone 10. After once disconnecting between the mobile phone and the network 15 for contents of the mobile phone, the mobile party tests the use of the predetermined network 16 through an authentication server 50 using the ID and the communication token T. The ID and the communication token T are transmitted to the communication token issuing server 40 and the validity of the communication token T is authenticated. The amount of the fee for data communication of the mobile phone 10, from which the fee for the communication token T is deducted, is charged to a billing destination on the mobile phone 10 side, and the fee for the communication token T is charged to another billing destination.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-111919
(P2009-111919A)
(43)公開日　平成21年5月21日(2009.5.21)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/56	(2006.01)	H04L 12/56	C	5K025
H04M 15/00	(2006.01)	H04M 15/00	G	5K030
H04M 11/00	(2006.01)	H04M 15/00	E	5K201
		H04M 11/00	302	

審査請求 有　請求項の数 23　ＯＬ　（全 26 頁）

(21)出願番号　特願2007-284415 (P2007-284415)
(22)出願日　平成19年10月31日 (2007.10.31)

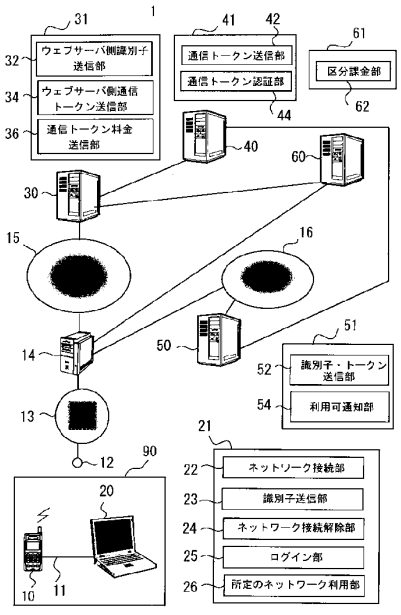
(71)出願人　596100812
京セラコミュニケーションシステム株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100108372
弁理士　谷田　拓男
(72)発明者　増田　景一
京都府京都市伏見区竹田鳥羽殿町６番地
京セラコミュニケーションシステム株式会社内

Ｆターム(参考)　5K025 BB08 CC09 DD06 EE19 EE24
FF22 GG10 GG18
5K030 GA15 GA19 HA08 HB08 HB11
HC01 JA10 JT02 KA04 KA06
LB01 MC07

最終頁に続く

(54)【発明の名称】データ通信料金課金システム、プログラム、記録媒体およびデータ通信料金課金方法

(57)【要約】
【課題】業務上所定のネットワーク１６へアクセスする場合に公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供する。
【解決手段】所定のネットワーク１６用の通信トークンＴを購入する際、携帯電話器１０のＩＤをウェブサーバ３０経由で通信トークン発行サーバ４０へ送信する。ＩＤに基づき通信トークンＴが生成されウェブサーバ３０及び携帯電話器１０を介してＰＣ２０へ送信される。携帯電話コンテンツ用ネットワーク１５との接続を一旦解除した後、ＩＤ及び通信トークンＴを用い認証サーバ５０を介し所定のネットワーク１６の利用を試す。ＩＤ及び通信トークンＴは通信トークン発行サーバ４０へ送信され通信トークンＴの正当性が認証される。携帯電話器１０のデータ通信に対する料金から通信トークンＴの料金を控除した額が携帯電話器１０側の請求先に課金され通信トークンＴの料金は他の請求先に課金される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、
前記移動情報端末は、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、
前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、
前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段と、
前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、
前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、
前記ウェブサーバは、
前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、
前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、
前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、
前記認証サーバは、
前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、
前記通信トークン発行サーバは、
前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、
前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、
前記課金サーバは、
前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とするデータ通信料金課金システム。
【請求項２】
請求項１記載のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを

介して前記所定のネットワークの利用を行う場合、
前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、
前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金システム。
【請求項３】
請求項１又は２記載のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えたことを特徴とするデータ通信料金課金システム。
【請求項４】
請求項１乃至３のいずれかに記載のデータ通信料金課金システムにおいて、
前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することを特徴とするデータ通信料金課金システム。
【請求項５】
請求項１乃至４のいずれかに記載のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により送信された識別子とを送信し、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金システム。
【請求項６】
請求項１乃至５のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金システム。
【請求項７】
請求項１乃至６のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金システム。
【請求項８】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、

前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、

前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、

前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、

前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、

前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、

前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、

前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、

前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラム。

【請求項９】

請求項８記載のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、

前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、

前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、

前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。

【請求項１０】

請求項８又は９記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、

前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、

前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信

され、
前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、
前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、
前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、
前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラム。
【請求項１２】
請求項１１記載のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、
前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。
【請求項１３】
請求項１１又は１２記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動

通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、
前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１４】
請求項８乃至１３のいずれかに記載のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするプログラム。
【請求項１５】
請求項８乃至１４のいずれかに記載のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするプログラム。
【請求項１６】
請求項８乃至１５のいずれかに記載のプログラムを記録したコンピュータ読取り可能な記録媒体。
【請求項１７】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、
前記移動情報端末が、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、
前記ウェブサーバが、
前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、
前記通信トークン発行サーバが、
前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、
前記ウェブサーバが、
前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、
前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、
前記移動情報端末が、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、
前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、

前記認証サーバが、
前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、
前記通信トークン発行サーバが、
前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証ステップと、
前記認証サーバが、
前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、
前記移動情報端末が、
前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、
前記課金サーバが、
前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とするデータ通信料金課金方法。

【請求項１８】
請求項１７記載のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、
前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、
前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金方法。

【請求項１９】
請求項１７又は１８記載のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えたことを特徴とするデータ通信料金課金方法。

【請求項２０】
請求項１７乃至１９のいずれかに記載のデータ通信料金課金方法において、
前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することを特徴とするデータ通信料金課金方法。

【請求項２１】
請求項１７乃至２０のいずれかに記載のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対

応する前記他の請求先との対応表をさらに備え、
前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、
前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金方法。
【請求項２２】
請求項１７乃至２１のいずれかに記載のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金方法。
【請求項２３】
請求項１７乃至２２のいずれかに記載のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動情報端末装置のデータ通信料金を当該移動情報端末装置側の請求先と他の請求先とに区分して課金するデータ通信料金課金システム等に関する。
【背景技術】
【０００２】
近年、社外で携帯電話器とパーソナルコンピュータ（以下、「ＰＣ」と省略する。）とを用いてモバイル通信を行うことにより、業務を行う必要に迫られているビジネスマン等が増加している。所持している携帯電話器はビジネスマン等の個人契約によるものであることが多く、この場合、モバイル通信によるアクセスで発生したパケット通信料はビジネスマン等へ請求されることになる。ビジネスマン等は当該請求の明細書を用いて会社にパケット通信料を請求することは可能であるが、業務上であるのか個人使用であるのかという、いわゆる公私区分の事務処理は極めて面倒且つ困難である。このため、当該パケット通信料はビジネスマン等の個人負担になってしまうことが多いというのが実情である。
【０００３】
従来、携帯電話器の通話の分野では、公私区分の事務処理を容易にするために、相手の電話番号の前にいわゆる特番と呼ばれる認識番号を入力することにより、会社と個人とで通話料金を区分する公私分計サービスが行われている（非特許文献１参照）。
【０００４】
携帯電話器を用いたデータ通信向けの種々の公私分計サービスも既に行われている。例えば、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことにより、リアルタイムにデータ通信料およびデータ通信料金の概算を表示することもできる（非特許文献２参照）。
【０００５】
予めアクセス先を登録しておくことにより、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。あるいは、企業側ネットワークへアクセスする場合を業務利用とし、他

のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する（特許文献１参照）。

【０００６】

【非特許文献１】日経ＢＰ社、ITpro 、Network“ケータイonBussiness”、［online］、２００４年９月１６日、［平成１９年２月１日検索］、インターネット<URL: http://itpro.nikkeibp.co.jp/free/TIS/keitai/20040915/149943/?ST=keitai&P=2>

【非特許文献２】ＫＤＤＩ、モバイル通信、各種ソフトダウンロード“パケットカウンター”、［online］、［平成１９年２月１日検索］、インターネット<URL: http:// http://www.au.kddi.com/mobile/soft/packet_counter/index.html>

【特許文献１】国際公開第ＷＯ２００４／０７７７６５号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上述のように、携帯電話器の通話の分野では特番を用いることにより会社と個人とで通話料金を区分する公私分計サービスが行われている。しかし、通話の場合と比較してデータ通信の場合、パケットは同時に複数の箇所にアクセスすることができるため、特番のような認識番号を付加することにより公私分計することは困難であるという問題があった。

上述のように、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておく公私分計サービスも行われている。しかし、当該分計は概算にすぎない上、ＰＣ上でのパケットカウントはユーザがカウントしたものと同様であるため、当該分計はキャリヤ側からみて信頼度が低く、従って当該分計はキャリヤ側の請求に反映できるものではないという問題があった。上述のように、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。しかし、この場合、宛先を登録する必要があるという問題があった。企業側ネットワークへアクセスする場合を業務利用とし、他の一般のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する。しかし、業務上、インターネット上のサーバへアクセスする場合は私的利用となってしまうため、業務利用として分けて課金することができないという問題があった。

【０００８】

そこで、本発明の目的は、上記問題を解決するためになされたものであり、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することにある。

【課題を解決するための手段】

【０００９】

この発明のデータ通信料金課金システムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、前記移動情報端末は、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの

接続を解除する移動通信部側ネットワーク接続解除手段と、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、前記ウェブサーバは、前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、前記認証サーバは、前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、前記通信トークン発行サーバは、前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、前記課金サーバは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とする。

【００１０】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することができる。

【００１１】

ここで、この発明のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えることができる。

【００１２】

ここで、この発明のデータ通信料金課金システムにおいて、前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することができる。

【００１３】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により

送信された識別子とを送信し、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１４】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００１５】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００１６】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラムである。

【００１７】

ここで、この発明のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記通信

トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００１８】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信され、前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１９】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラムである。

【００２０】

ここで、この発明のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部

へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００２１】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００２２】

ここで、この発明のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００２３】

ここで、この発明のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００２４】

この発明の記録媒体は、本発明のいずれかのプログラムを記録したコンピュータ読取り可能な記録媒体である。

【００２５】

この発明のデータ通信料金課金方法は、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、前記移動情報端末が、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、前記ウェブサーバが、前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、前記記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、前記ウェブサーバが、前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、前記移動情報端末が、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、前記認証サーバが、前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する

通信トークン認証ステップと、前記認証サーバが、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、前記移動情報端末が、前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、前記課金サーバが、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とする。

【００２６】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することができる。

【００２７】

ここで、この発明のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えることができる。

【００２８】

ここで、この発明のデータ通信料金課金方法において、前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することができる。

【００２９】

ここで、この発明のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００３０】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００３１】
ここで、この発明のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。
【発明の効果】
【００３２】
本発明のデータ通信料金課金システム等によれば、所定のネットワーク用の通信トークンを携帯電話コンテンツ用ネットワークに接続された配信サイトが稼動するウェブサーバ経由で購入するに際し、好適には携帯電話器およびＰＣから構成される移動情報端末のＰＣから携帯電話器を介して携帯電話器の識別子ＩＤをウェブサーバへ送信する。送信された識別子ＩＤはウェブサーバにより通信トークン発行サーバへ送信される。通信トークン発行サーバは送信された携帯電話器の識別子ＩＤに基づき通信トークンを生成し、この生成された通信トークンをウェブサーバへ送信する。生成した通信トークンは携帯電話器の識別子ＩＤと紐付けされた状態で記録しておく。送信された通信トークンはウェブサーバにより携帯電話器を介してＰＣへ送信される。その後、携帯電話コンテンツ用ネットワークとの接続を一旦解除した後、改めて携帯電話器の識別子ＩＤおよび上記通信トークンを用い、ＰＣ側から携帯電話器および認証サーバを介して所定のネットワークの利用を試みる。認証サーバは携帯電話器の識別子ＩＤおよび通信トークンを通信トークン発行サーバへ送信する。通信トークン発行サーバは送信された識別子ＩＤおよび通信トークンに基づき当該通信トークンの正当性を認証する。従前に、生成された通信トークンＴ（従前）は携帯電話器の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、送信された識別子ＩＤおよび通信トークンと、記録されている識別子ＩＤ（従前）および通信トークン（従前）とが一致する場合、従前に携帯電話コンテンツ用ネットワークを介して通信トークン（従前）を購入する際に用いられた携帯電話器と、現在所定のネットワークの利用を試みようとしている際に用いられている携帯電話器とが同一であると認証することができる。認証結果はウェブサーバ側へ通知される。以上のように、上記通信トークン購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワークから所定のネットワークへの通信の切替を行った場合であってもユーザ（携帯電話器）の対応が付けられる。このため、課金サーバは通信事業者側サーバから送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器のデータ通信に対する料金から、当該所定の期間におけるウェブサーバにより送信された通信トークンの料金を控除した額を携帯電話器側の請求先（携帯電話器の所有者または利用者であるユーザ）に課金し、当該通信トークンの料金を他の請求先（上記ユーザに対して所定の関係を有する側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワークの一例）上のサーバへアクセスする場合であっても、上述した通信トークンを用いることにより容易に公私分計することができる。さらに、本発明のデータ通信料金課金システムはキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができるという効果がある。
【発明を実施するための最良の形態】
【００３３】
以下、各実施例について図面を参照して詳細に説明する。
【実施例１】
【００３４】
図１は、本発明の実施例１におけるデータ通信料金課金システム１を示す。図１において、符号９０は移動通信機能を有する移動通信部１０と情報処理機能を有する情報処理部

２０とを備えた移動情報端末である。移動情報端末９０は移動通信部１０と情報処理部２０とを備えた１台の装置として構成することができる。あるいは移動情報端末９０は、好適には移動通信部１０を携帯電話器１０とし、好適には情報処理部２０をパーソナルコンピュータＰＣ２０とし、携帯電話器１０とＰＣ２０とを脱着可能に接続した構成とすることもできる。以下では、移動情報端末９０は携帯電話器１０とＰＣ２０とが脱着可能に接続した構成であるものとする。携帯電話器１０のユーザは携帯電話器１０の所有者または利用者と想定する。携帯電話器１０とＰＣ２０との間の接続は脱着可能な接続方式、例えばＵＳＢ（Universal Serial Bus）ケーブル１１を用いることが好適である。しかし、ＵＳＢ等の接続方式に限定されるものではなく、無線等であってもよいことは勿論である。なお本明細書において、「携帯電話器」は携帯電話装置または携帯電話機と呼んでもよい。続いて、符号１３は移動体通信網、１４は移動体通信網１３に接続された通信事業者側サーバ、１２は移動体通信網１３に接続された基地局であり、携帯電話器１０は基地局１２のエリア内に在圏しているものと想定する。符号１５は通信事業者側サーバ１４と接続された携帯電話コンテンツ用ネットワーク（移動通信部側ネットワーク）、３０は携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブ（Ｗｅｂ）サーバである。通信事業者側サーバ１４は携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う。続いて、符号４０はウェブサーバ３０と接続され所定のネットワーク１６の利用権を示す通信トークン（ワンタイム通信トークン）を発行する通信トークン発行サーバ、６０はウェブサーバ３０と接続され移動情報端末９０の携帯電話器１０に掛かるデータ通信料金を課金する課金サーバ、５０は所定のネットワーク１６に接続された認証サーバである。所定のネットワークとしては、携帯電話器１０のユーザが業務上使用する企業内ネットワーク、インターネット等が好適である。認証サーバ５０は通信トークン発行サーバ４０と接続されている。図１に示されるように、携帯電話器１０は移動体通信網１３および携帯電話コンテンツ用ネットワーク１５を介してウェブサーバ３０と接続されている。ウェブサーバ３０と通信トークン発行サーバ４０との間の接続、ウェブサーバ３０と課金サーバ６０との間の接続、通信事業者側サーバ１４と課金サーバ６０との間の接続、認証サーバ５０と通信トークン発行サーバ４０との間の各接続はＶＰＮ（Virtual Private Network）等の専用通信網によることが好適である。上述のように、移動通信部の例として携帯電話器１０を用いて説明するが、移動通信部１０は携帯電話器１０に限定されるものではなく、ＰＨＳ（Personal Handyphone System）等であってもよい。同様に、情報処理部２０の例としてＰＣ２０を用いて説明するが、ＰＣ２０に限定されるものではなく、ＰＤＡ（Personal Digital Assistant）等、携帯電話器１０と接続可能な情報処理装置であれば他の装置であってもよい。

【００３５】

図１において、符号２１はＰＣ２０が備える機能を示す機能ブロックである。機能ブロック２１において、符号２２は携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続するネットワーク接続部（移動通信部側ネットワーク接続手段）、２３は、例えば携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入するに際し、携帯電話器１０の識別子（例えば携帯電話器１０の電話番号等）をウェブサーバ３０へ送信する識別子送信部（識別子送信手段）、２４はウェブサーバ３０側から携帯電話器１０を介して通信トークンが携帯コンテンツとみなされて送信された後、ネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除するネットワーク接続解除部（移動通信部側ネットワーク接続解除手段）、２５は携帯電話器１０の識別子およびウェブサーバ３０側から送信された通信トークンを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みるログイン部（ログイン手段）、２６は認証サーバ５０から所定のネットワーク１６の利用を認める通知が送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う所定のネットワーク利用部（所定のネットワーク利用手段）である。以上のＰＣ２０が備える機能は、ＰＣ２０に配置されＰＣ２０のコンピュータに上述の各機能を実行させるための通信認証接

続ソフトウェアとして実現することができる。識別子送信部２３がウェブサーバ３０へ送信する識別子は、携帯電話器１０の識別子に限定されるものではなく、ＰＣ２０の識別子（例えばＰＣ２０の製造番号等）であってもよい。あるいは、携帯電話器１０およびＰＣ２０から構成される移動情報端末９０の識別子とすることもできる。

【００３６】

図１において、符号３１はウェブサーバ３０が備える機能を示す機能ブロックである。機能ブロック３１において、符号３２は識別子送信部２３により送信された識別子を通信トークン発行サーバ４０へ送信するウェブサーバ側識別子送信部（ウェブサーバ側識別子送信手段）、３４は通信トークン発行サーバ４０から送信された通信トークンを携帯電話器１０を介してＰＣ２０へ送信するウェブサーバ側通信トークン送信部（ウェブサーバ側通信トークン送信手段）、３６は課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金を送信する通信トークン料金送信部（通信トークン料金送信手段）である。携帯電話器１０のユーザが通信トークンを購入する時点では、通常、通信トークンの料金は予め定まっているが、未確定であってもよい。後述するように、課金サーバ６０が通信料金の公私分計を行うため、携帯電話器１０のユーザは業務上使用する通信トークンの料金を考慮する必要はない。

【００３７】

図１において、符号５１は認証サーバ５０が備える機能を示す機能ブロックである。機能ブロック５１において、符号５２はログイン部２５により用いられた携帯電話器１０の識別子および通信トークンを通信トークン発行サーバ４０へ送信する識別子・通信トークン送信部（識別子・通信トークン送信手段）、５４は通信トークン発行サーバ４０により上記通信トークンの正当性が認証された場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知を送信する利用可通知部（利用可通知手段）である。

【００３８】

図１において、符号４１は通信トークン発行サーバ４０が備える機能を示す機能ブロックである。機能ブロック４１において、符号４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子に基づき上記通信トークンを生成し、この生成された通信トークンをウェブサーバ３０へ送信する通信トークン送信部（通信トークン送信手段）、４４は識別子・通信トークン送信部５２により送信された識別子および通信トークンに基づき当該通信トークンの正当性を認証する通信トークン認証部（通信トークン認証手段）である。通信トークン送信部４２は、生成した通信トークンを携帯電話器１０の識別子と紐付けされた状態で記録しておく。通信トークン認証部４４の認証結果は認証サーバ５０側へ通知される。

【００３９】

図１において、符号６１は課金サーバ６０が備える機能を示す機能ブロックである。機能ブロック６１において、符号６２は、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ等）に課金し、当該通信トークンの料金を他の請求先（携帯電話器１０の所有者または利用者であるユーザに対して所定の関係を有する側等）に課金する区分課金部（区分課金手段）である。以上により、携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入した場合、業務上用いた通信トークンの料金は上記他の請求先に課金されることになる。この結果、携帯電話器１０のユーザが私用で用いたデータ通信料金と業務上用いたデータ通信料金(通信トークンの料金)とが公私分計されることになる。所定の関係を有する側としては、例えばユーザが会社員である場合、当該会社員の雇用者、即ち会社であるものとすることができる。当該会社員が自社のネットワーク（所定のネットワーク１６）にログインする場合、業務上用いた当該自社のネットワークに関する通信トークンの料金

は会社側に課金されることになり、公私分計されることになる。あるいは、所定の関係を有する側としては、例えばユーザがコンシューマー向けの会員制情報提供サービスの会員である場合、当該コンシューマー向けの会員制情報提供サービスの提供者であるものとすることもできる。当該会員が当該会員制情報提供サービスのネットワーク（所定のネットワーク１６）にログインする場合、利用した当該会員制情報提供サービスのネットワークに関する通信トークンの料金は、当該会員制情報提供サービスの提供者側に課金されることになり、一種の分計が行なわれることになる。

【００４０】

図２は、データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法をフローチャートで示す。図２において、左側からＰＣ２０で実行されるプログラム等のフローチャート、ウェブサーバ３０で実行されるプログラム等のフローチャート、通信トークン発行サーバ４０で実行されるプログラム等のフローチャート、認証サーバ５０で実行されるプログラム等のフローチャート、課金サーバ６０で実行されるプログラム等のフローチャートであり、各構成要素間の通信は点線で示す。

【００４１】

図２に示されるように、まず、ＰＣ２０が、携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続する（移動通信部側ネットワーク接続ステップ。ステップＳ２２）。移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバ３０へ、所定のネットワーク１６の利用権を示す通信トークンの購入を行うために、携帯電話器１０の識別子ＩＤを送信する（識別子送信ステップ。ステップＳ２３）。

【００４２】

次に、ウェブサーバ３０が、ウェブサーバ３０と接続され通信トークンを発行する通信トークン発行サーバ４０へ、識別子送信ステップ（ステップＳ２３）で送信された識別子ＩＤを送信する（ウェブサーバ側識別子送信ステップ。ステップＳ３２）。

【００４３】

続いて、通信トークン発行サーバ４０が、ウェブサーバ側識別子送信ステップ（ステップＳ３２）で送信された識別子ＩＤに基づき通信トークンＴを生成してウェブサーバ３０へ送信する（通信トークン送信ステップ。ステップＳ４２）。通信トークン発行サーバ４０は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。

【００４４】

ウェブサーバ３０が、通信トークン送信ステップ（ステップＳ４２）で送信された通信トークンＴを携帯電話器１０を介してＰＣ２０へ送信する（ウェブサーバ側通信トークン送信ステップ。ステップＳ３４）。ウェブサーバ３０と接続され携帯電話器１０のデータ通信料金を課金する課金サーバ６０へ、ウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴの料金Ｂを送信する（通信トークン料金送信ステップ。ステップＳ３６）。

【００４５】

ＰＣ２０が、移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する（移動通信部側ネットワーク接続解除ステップ。ステップＳ２４）。携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用い、携帯電話器１０および所定のネットワーク１６に接続された認証サーバ５０を介して所定のネットワーク１６の利用を試みる（ログインステップ。ステップＳ２５）。

【００４６】

認証サーバ５０が、ログインステップ（ステップＳ２５）で用いられた識別子ＩＤおよ

び通信トークンＴを通信トークン発行サーバ４０へ送信する（識別子・通信トークン送信ステップ。ステップＳ５２）。

【００４７】

通信トークン発行サーバ４０が、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴに基づき通信トークンＴの正当性を認証する（通信トークン認証ステップ。ステップＳ４４）。上述のように、通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン発行サーバ４０は従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴを購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証ステップ（ステップＳ４４）において、上記認証結果Ｎは認証サーバ５０側へ通知される。

【００４８】

認証サーバ５０は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、すなわち通知された認証結果Ｎが正当性を認証したことを示す場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍを送信する（利用可通知ステップ。ステップＳ５４）。

【００４９】

ＰＣ２０は、認証サーバ５０から所定のネットワーク１６の利用を認める通知Ｍが送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う（所定のネットワーク利用ステップ。ステップＳ２６）。

【００５０】

課金サーバ６０は、携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴの料金Ｂを控除した額を携帯電話器１０側の請求先に課金し、通信トークンＴの料金Ｙを他の請求先に課金する（区分課金ステップ。ステップＳ６２）。

【００５１】

以上より、本発明の実施例１によれば、識別子送信部２３は所定のネットワーク１６用の通信トークンＴを配信サイト経由で購入するに際し、携帯電話器１０の識別子ＩＤをウェブサーバ３０へ送信する。識別子送信部２３により送信された識別子ＩＤはウェブサーバ側識別子送信部３２により通信トークン発行サーバ４０へ送信される。通信トークン送信部４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子ＩＤに基づき通信トークンＴを生成し、この生成された通信トークンＴをウェブサーバ３０へ送信する。通信トークン送信部４２は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。送信された通信トークンＴはウェブサーバ側通信トークン送信部３４により携帯電話器１０を介してＰＣ２０へ送信される。その後、ネットワーク接続解除部２４がネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する。携帯電話器１０とＰＣ２０との間は接続状態のままでよい。一旦携帯電話コンテンツ用ネットワーク１５との接続が解除された後、改めてログイン部２５が携帯電話器１０の識別子ＩＤおよび上記通信トークンＴを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。識別子・通信トークン送信部５２はログイン部２５により用いられた携帯電話器１０の識別子ＩＤおよび通信トークンＴを通信トークン発行サーバ４０へ送信する。通信トークン認証部４４は識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴに基づき当該通信トークンＴの正当性を認証する。従前に通信トークン送信部４２により生成された通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付

けされた状態で記録されているため、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証部４４の認証結果Ｎは認証サーバ５０側へ通知される。

【００５２】

以上のように、上記通信トークンＴ購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワーク１５から所定のネットワーク１６への通信の切替を行った場合であってもユーザ（携帯電話器１０のユーザ）の対応が付けられる。このため、区分課金部６２は通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴの料金（＝Ｂ）を控除した額（＝Ａ－Ｂ）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴの料金（＝Ｂ）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴを用いることにより即時に公私分計することができる。さらに、本発明のデータ通信料金課金システム１はキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器１０の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ２０上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット１６上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができる。

【実施例２】

【００５３】

実施例２では、携帯電話器１０が無線ＬＡＮを介して所定のネットワーク１６の利用を行う場合について説明する。

【００５４】

図３は、本発明の実施例２におけるデータ通信料金課金システム２を示す。図２で図１と同じ符号を付した箇所は同じ要素を示すため説明は省略する。図２に示されるデータ通信料金課金システム２が図１に示されるデータ通信料金課金システム１と異なる点は、ＰＣ２０が無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行う場合のために、無線ＬＡＮ１７および無線ＬＡＮ１７に接続された無線ＬＡＮ基地局１８が追加された点と、当該追加に伴い、ＰＣ２０のログイン部２５の機能および認証サーバ５０の利用可通知部５４の機能が一部変更された点とである（各々、ログイン部２５’、利用可通知部５４’と示す）。

【００５５】

データ通信料金課金システム２では、通信トークン料金送信部３６により送信された通信トークンＴ’の料金Ｂ’には、実施例１で説明した所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金が含まれている。この無線ＬＡＮ１７の回線使用料金は、例えば無線ＬＡＮ基地局１８があるホットスポットの臨時課金である。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。他の処理

は実施例１と同様であるため説明は省略する。

【００５６】

実施例２のデータ通信料金課金方法は、上述した実施例１のデータ通信料金課金方法において、通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴ’の料金Ｂ’が無線ＬＡＮ１７の回線使用料金を含み、ログインステップ（ステップＳ２５）は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みることになる。利用可通知ステップ（ステップＳ５４）は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信することになる。他の処理は図２に示される実施例１の処理と同様であるため説明は省略する。

【００５７】

以上より、本発明の実施例２によれば、データ通信料金課金システム２における通信トークンＴ’の料金Ｂに、所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金を含ませておく。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。この結果、携帯電話器１０は無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行うことができる。区分課金部６２は、実施例１と同様に、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴ’の料金（＝所定のネットワーク１６の利用料＋無線ＬＡＮ１７の回線使用料金＝Ｂ’）を控除した額（＝Ａ－Ｂ’）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴ’の料金（＝Ｂ’）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、ホットスポットにおいて臨時的にインターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴ’を用いることにより、実施例１と同様に即時に公私分計することができる。

【実施例３】

【００５８】

上述した実施例１および２の各データ通信料金課金システム１および２において、所定のネットワーク１６への接続が認証を必要とする場合のために、ウェブサーバ３０は当該認証（ユーザ認証）を行うウェブサーバ側認証部（ウェブサーバ側認証手段。不図示）をさらに備えることができる。所定のネットワーク１６が企業内ネットワーク等である場合、当該企業内ネットワーク等へログインするためにはユーザ認証を必要とする。あるいは、接続料金定額サービスの場合、通信時間またはパケット量の測定をしないケースもあるため、接続料金定額サービスを利用する場合にはユーザ認証を必要とする。本実施例３によれば、ウェブサーバ３０はユーザ認証を行うウェブサーバ側認証部を備えているため、所定のネットワーク１６への接続が認証を必要とする場合、当該認証を行うことができる。

【００５９】

実施例３のデータ通信料金課金方法は、上述した実施例１または２の各データ通信料金課金方法において、ウェブサーバ側識別子送信ステップ（ステップＳ３２）に先立ち、ウェブサーバ３０が上記認証を行うウェブサーバ側認証ステップ（不図示）をさらに備えればよい。他の処理は図２に示される実施例１の処理、上述した実施例２の処理と同様であるため説明は省略する。

【実施例４】
【００６０】
本実施例４では、上述した各実施例において通信トークンの生成の際に暗号化を用いる場合について説明する。暗号化以外については上述した各実施例と同様である。以下では、図１を適宜引用して説明する。
【００６１】
通信トークン送信部４２は、ウェブサーバ側識別子送信部３２により送信された識別子ＩＤと所定の鍵（秘密鍵等）Ｋと所定の乱数Ｒとに基づき通信トークンＴ＊（暗号化されたことを上付＊で示す。）を生成する。生成した通信トークンＴ＊をウェブサーバ３０へ送信する。通信トークン送信部４２は携帯電話器１０の識別子ＩＤと所定の乱数Ｒとを関連付け（紐付け）した状態で記録しておく。所定の鍵Ｋは携帯電話器１０によらず一定の鍵としておけばよいが、所定の鍵Ｋも識別子ＩＤと関連付けて記録しておいてもよいことは勿論である。通信トークン認証部４４は、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴ＊と、所定の鍵Ｋと、通信トークン送信部４２により識別子ＩＤと関連付けて記録された所定の乱数Ｒとに基づき、通信トークンＴ＊の正当性を認証する。従前に通信トークン送信部４２により通信トークンＴ＊（従前）が生成された際、携帯電話器１０の識別子ＩＤ（従前）および所定の乱数Ｒとは紐付けされた状態で記録されている。このため、識別子・通信トークン送信部５２により送信された識別子ＩＤと同じ値の識別子ＩＤ（従前）を検索し、当該識別子ＩＤ（従前）に紐付けされている所定の乱数Ｒを求め、この所定の乱数Ｒと所定の鍵Ｋと識別子ＩＤとから通信トークンＴ＊（従前）を求める。この通信トークンＴ＊（従前）と識別子・通信トークン送信部５２により送信された通信トークンＴ＊とが一致した場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ＊（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。
【００６２】
以上より、本発明の実施例４によれば、上述した各実施例で説明した機能に加えて、暗号化された通信トークンＴ＊を用いることができる。この結果、通信トークンＴ＊がコピーされていた場合、ＰＣ２０からのログイン要求を拒否することができる。この結果、上述した各実施例の効果に加えて、通信トークンＴ＊をコピーされないようにすることができるセキュリティ機能を有するデータ通信料金課金システムを構築することができる。
【実施例５】
【００６３】
上述したデータ通信料金課金システム１等では、携帯電話器１０の識別子は１つであることを想定していた。本実施例５では、携帯電話器１０は１つ以上の識別子を有し、上述した他の請求先も当該１つ以上の識別子に対応して１つ以上ある場合について説明する。
【００６４】
移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００（後述する図４参照）をさらに備えている。対応表１００は、例えばＰＣ２０および課金サーバ６０の記録装置７８ａ（図４参照）に記録されている。ＰＣ２０側では、識別子送信部２３’’（不図示）は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。ウェブサーバ３０側では、通信トークン料金送信部３６’’（不図示）は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。課金サーバ６０側では、区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に

課金する。

【００６５】

以上により、本発明の実施例５によれば、移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００をさらに備えている。識別子送信部２３’’は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。通信トークン料金送信部３６’’は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に課金する。この結果、携帯電話器１０は複数の識別子を使い分けることにより、通信トークンの料金を複数の他の請求先へ課金させることができる。

【実施例６】

【００６６】

図４は、上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。図４に示されるように、ＣＰＵ７１、ＲＯＭ７２、ＲＡＭ７３、画像制御部７６、コントローラ７７、入力制御部７９、無線ＬＡＮ１７とのインタフェース機能を有する通信メディアインタフェース（Ｉ／Ｆ）部８１および入出力Ｉ／Ｆ部８２はバス８３に接続されている。図４において、上述の本発明のコンピュータ・プログラム（ＰＣ２０側のプログラム、課金サーバ６０側のプログラム等）は、ＲＯＭ７２、ＨＤ等の記録装置７８ａ、またはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体（脱着可能な記録媒体を含む）に記録されている。本発明のコンピュータ・プログラムは、ＲＯＭ７２からバス８３を介し、あるいは記録装置７８ａまたはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体からコントローラ７７を経由してバス８３を介しＲＡＭ７３へロードされる。内部回路７０がＰＣ２０および課金サーバ６０の場合、図４に示されるように記録装置７８ａには対応表１００が記録されている。入力制御部７９は、マウス、テンキー等の入力操作部８０と接続され入力制御等を行う。画像メモリであるＶＲＡＭ７５はＰＣ２０の表示部７４の少なくとも一画面分のデータ容量に相当する容量を有しており、画像制御部７６はＶＲＡＭ７５のデータを画像データへ変換して表示部７４へ送出する機能を有している。入出力Ｉ／Ｆ部８２は入出力インタフェース機能を有しており、ＵＳＢケーブル１１等により携帯電話器１０の入出力Ｉ／Ｆ部（不図示）と接続されている。

【００６７】

上述のようにＣＰＵ７１が本発明のコンピュータ・プログラムを実行することにより、本発明の目的を達成することができる。当該コンピュータ・プログラムは上述のようにＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体の形態でコンピュータＣＰＵ７１に供給することができ、当該コンピュータ・プログラムを記録したＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体も同様に本発明を構成することになる。当該コンピュータ・プログラムを記録した記録媒体としては上述された記録媒体の他に、例えばメモリ・カード、メモリ・スティック、光ディスク、ＦＤ等を用いることができる。

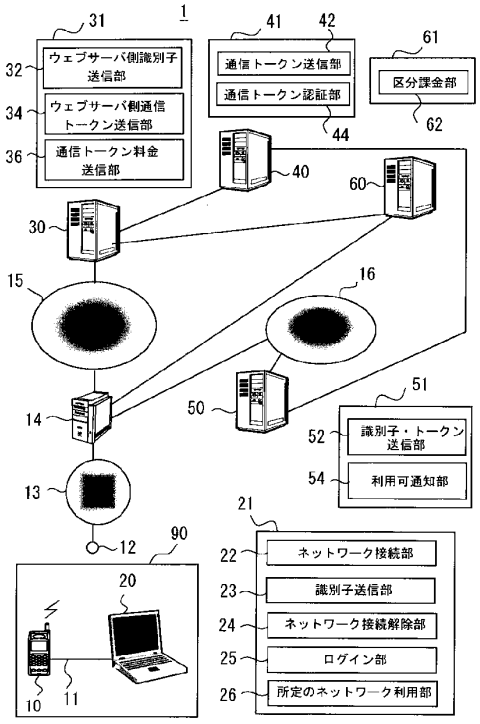
【産業上の利用可能性】

【００６８】

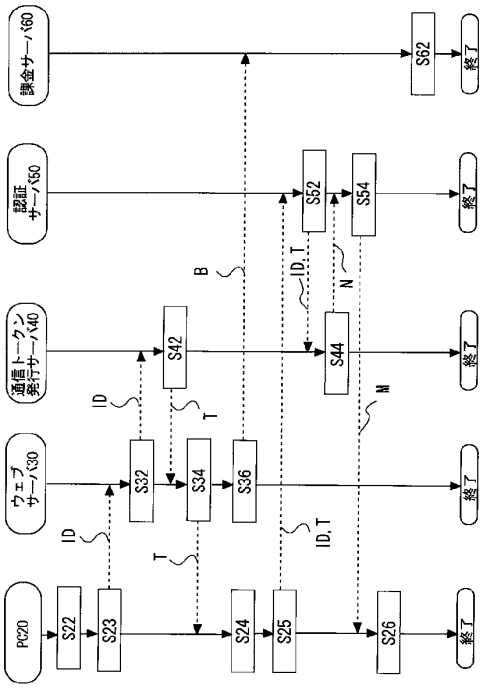
本発明の活用例として、上述のように公私分計を即時に行うことができるため、会社所有のＰＣおよび携帯電話器を用いた所定のネットワーク１６の利用に対する従来の会社側との割引契約に、個人所有のＰＣおよび携帯電話器を用いた場合における所定のネットワーク１６の利用に対しても即時に割引を適用するシステムへの応用が挙げられる。

【図面の簡単な説明】
【００６９】
【図１】本発明の実施例１におけるデータ通信料金課金システム１を示す図である。
【図２】データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法を示すフローチャートである。
【図３】本発明の実施例２におけるデータ通信料金課金システム２を示す図である。
【図４】上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。
【符号の説明】
【００７０】
１、２　データ通信料金課金システム、　１０　携帯電話器、　１１　ＵＳＢケーブル、　１２　基地局、　１３　移動体通信網、　１４　通信事業者側サーバ、　１５　携帯電話コンテンツ用ネットワーク、　１６　所定のネットワーク、　１７　無線ＬＡＮ、　１８　無線ＬＡＮ基地局、　２０　ＰＣ、　２１、３１、４１、５１、６１　機能ブロック、　２２　ネットワーク接続部、　２３　識別子送信部、　２４　ネットワーク接続解除部、　２５、２５’　ログイン部、　２６　所定のネットワーク利用部、　３０　ウェブサーバ、　３２　ウェブサーバ側識別子送信部、　３４　ウェブサーバ側通信トークン送信部、　３６　通信トークン料金送信部、　４０　通信トークン発行サーバ、　４２　通信トークン送信部、　４４　通信トークン認証部、　５０　認証サーバ、　５２　識別子・通信トークン送信部、　５４、５４’　利用可通知部、　６０　課金サーバ、　６２　区分課金部、　７０　内部ブロック、　７１　ＣＰＵ、　７２　ＲＯＭ、　７３　ＲＡＭ、　７４　表示部、　７５　ＶＲＡＭ、　７６　画像制御部、　７７　コントローラ、　７８ａ　記録装置、　７８ｎ　記録媒体、　７９　入力制御部、　８０　入力操作部、　８１　通信メディアＩ／Ｆ部、　８２　入出力Ｉ／Ｆ部、　８３　バス、　９０　移動情報端末、　１００　対応表。

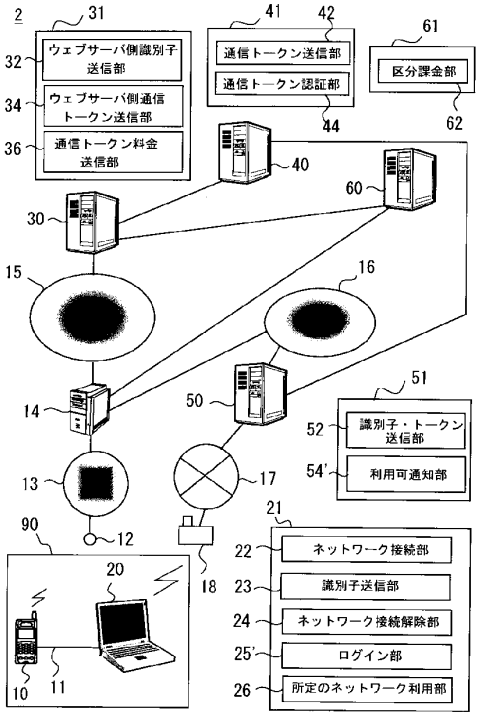
【図１】


1
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
識別子・トークン送信部
52
利用可通知部
54
13
12
90
21
ネットワーク接続部
22
識別子送信部
23
ネットワーク接続解除部
24
ログイン部
25
所定のネットワーク利用部
26
20
10
11

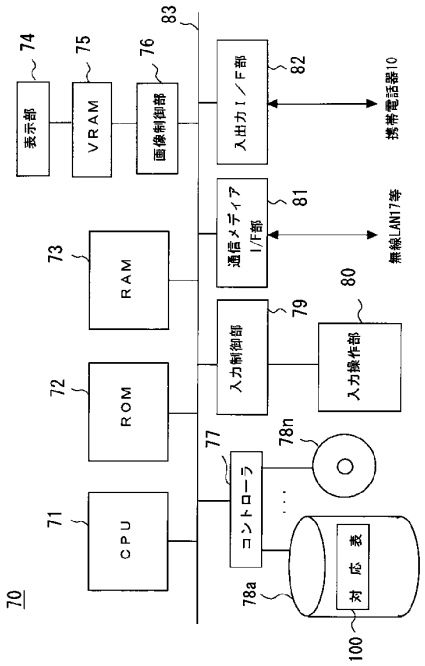
【図２】


課金サーバ60
認証サーバ50
通信トークン発行サーバ40
ウェブサーバ30
PC20
S22
S23
S24
S25
S26
S32
S34
S36
S42
S44
S52
S54
S62
終了
ID
T
ID,T
N
B

【図３】


2
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
識別子・トークン送信部
52
利用可通知部
54'
13
17
12
90
21
ネットワーク接続部
22
識別子送信部
23
ネットワーク接続解除部
24
ログイン部
25'
26
所定のネットワーク利用部
18
20
10
11

【図４】


70
CPU
71
ROM
72
RAM
73
表示部
74
VRAM
75
画像制御部
76
コントローラ
77
入出力I/F部
82
通信メディアI/F部
81
入力制御部
79
入力操作部
80
78n
78a
対応表
100
携帯電話器10
無線LAN17等
83

フロントページの続き

Ｆターム(参考) 5K201 AA05 AA09 BD05 CB13 DC02 EA07 EC06 ED06 FA07

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2006 (02.02.2006)

PCT

(10) International Publication Number
WO 2006/012610 A2

(51) International Patent Classification[7]: H04L 29/08, 29/06

(21) International Application Number: PCT/US2005/026296

(22) International Filing Date: 22 July 2005 (22.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/590837	23 July 2004 (23.07.2004)	US
60/601431	13 August 2004 (13.08.2004)	US
60/607420	3 September 2004 (03.09.2004)	US
60/608814	10 September 2004 (10.09.2004)	US

(71) Applicant *(for all designated States except US)*: **CITRIX SYSTEMS, INC.** [US/GB]; 851 West Cypress Creek Road, Fort Lauderdale, FL 33309 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RAO, Goutham, P.** [US/US]; 6963 Starling Valley Drive, San Jose, CA 95120 (US). **BRUEGGEMANN, Eric** [US/US]; 5642 Stevens Creek Blvd., no.606, Cupertino, CA 95014 (US). **RODRIGUEZ, Robert** [US/US]; 5647 Wells Court, San Jose, CA 95123 (US).

(74) Agents: **LANZA, John, D.** et al.; Lahive & Cockfield, LLP, 28 State Street, Boston, MA 02109 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

(57) **Abstract:** The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access.

WO 2006/012610 A2

SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

Related Applications

This present application claims priority to U.S. Provisional Patent Application Number 60/590,837, entitled "Ad Hoc Distributed Networks And Remote Access Architecture", filed July 23, 2004, and U.S. Provisional Patent Application Number 60/601,431, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed August 13, 2004, and U.S. Provisional Patent Application Number 60/607,420, entitled "Virtual Network Bridging", filed September 3, 2004, and U.S. Provisional Patent Application Number 60/608,814, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed September 10, 2004, all of which are incorporated herein by reference.

Technical Field

The invention generally relates to optimizing network communications between nodes on a network.

Background Information

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, to maintain privacy through the use of tunneling and security mechanisms. As such, a VPN provides for data encryption and security for corporate data traversing the public network. In addition to addressing secure access to corporate data via a public network, VPNs are also directed towards routing network traffic from two disconnected, otherwise non-routable networks. For example, a first private network with private internet protocol addresses in the range 10.0.0.0 – 10.255.255.255 may communicate via a VPN with a second private network with private internet protocol addresses in the range 192.168.0.0 – 192.168.255.255. The VPN allows a remote machine on the first private network to communicate with an internal machine on the second private network by tunneling network traffic from the remote machine and making the network traffic appear on the second private network. This may work well for client-server protocols where a remote computer is transacting with an enterprise server located on a remote network.

However, traditional VPNs may not work well in the case where two remote computers tunnel via a VPN gateway to communicate directly with each other, such as in peer-to-peer protocols. The VPN achieves this peer-to-peer computing by flattening the disjoint private network address spaces in which the two remote computers tunnel all peer-to-peer communications via the VPN gateway. As a result, network traffic from one of the peers flows through the VPN gateway and switches tunnels on the intranet to flow back out on the internet to the peer computer. The network traffic between the peer computers may travel longer and less optimal routes event though the peer computers may have a shorter direct path between then. It would be useful to allow remote computers to benefit from the security afforded by VPNs without incurring the drawback of longer data paths routes.

Other inefficiencies exist with direct communications over a network between two computers. For example, the network connection is susceptible to breakdown. For instance, a wireless connection between a client and a server is often unreliable. In other cases, the network connection is intermittent. A connection can be lost when one enters an elevator or tunnel and may only be restored following one's exit from the elevator or tunnel. In another example, a connection can be disrupted when a mobile computing device moves from network access point to network access point, such as in a wireless network topology.

If an established communication session between the client and the server computer abnormally terminates, the client generally has to re-establish the connection by starting a new communication session. To begin the new communication session, the user typically has to retransmit the authentication credentials, such as a login/password pair, to the server computer so that the server computer can authorize the user for the new communication session. This retransmission of the authentication credentials of a user across multiple communication sessions repeatedly exposes the authentication credentials of that user to potential attackers, thereby decreasing the level of security of the authentication credentials. In addition, this often is a slow process that also results in user frustration and inefficiency. Furthermore, in establishing a new communication session, the network may require the client obtains a new network identifier, such as an internet protocol address. The applications or programs on the client may need to be restarted because of the change in the client's network identifier. Thus, it would be desirable to shield the computing devices from network disruptions.

Another inefficiency associated with direct communication between peer computing devices is that the protocol used for communications may not be as efficient or secure as desired. As an example, the network communications may include real-time data communications such as voice over IP (VoIP) communications. The real-time data communications may be communicated via an unreliable protocol such as the user datagram protocol in order to reduce latency in the telephone call. However, the VoIP communication may traverse a TCP/IP network or secure SSL gateway, which provides a reliable protocol to the VoIP communications. This may increase the latency in the telephone call that the unreliable protocol was intended to reduce. Techniques are needed for transmitting data via a lossless protocol that is intended for communication using a lossy protocol.

Another inefficiency in direct communication result from the use of encryption. Encryption, such as SSL, may be used to provide secure network communications. Although the communication is secure, the encryption of the network traffic increases the size of the network packets, which can cause the packet payload to become too large for a single packet. This can result in packet fragmentation, causing more overhead for communication processing. Techniques for adjusting the maximum size of a packet to account for encryption overhead would be useful.

Another inefficiency result from the fact that a client typically sends network communications as they are generated by the activity of the user and applications of the client, and processes incoming network communications as they are received. For example, in one case, although an application is running in the foreground and currently in active use by the user, a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground. In another example, the client may be running a VoIP application to provide a telephone call to a remote computing device. One or more other applications on the client may be running that are not related to the real-time data communication of VoIP. The network packets for these applications may be processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication. It is desirable to provide application-aware, client-specific prioritization of packet traffic.

Summary of the Invention

The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present invention provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides various techniques for optimizing peer-to-peer communications, including real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. The present invention provides the following peer to peer optimization techniques: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile computing.

In one aspect, the present invention relates to a method for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device. The third computing device may be a gateway, such as an SSL VPN gateway. The first computing device initiates a communication session to the second computing device via the third computing device, such as via a signaling protocol. A server receives a signal to establish the initiated communication session, and the server communicates to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session. The first computing device communicates a request to initiate a connection with the second computing device using the first network address. The method further

includes intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a request to the second computing device to allow a connection from the first computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment of the present invention, the first tunneling session or the second tunneling session is established using a Secure Socket Layer or a virtual private network The third computing device may be a remote access gateway. In another embodiment, the second computing device is located behind a firewall associated with the second network address.

In another embodiment, the method of the present invention includes providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session. In an additional embodiment, the method of includes providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data to the other computing device.

In some embodiments of the present invention, the method associates a first telecommunication device with the first computing device, and associates a second telecommunication device with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the method of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device

may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the method communicates a remote display protocol via the connection between the first computing device and the second computing device. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the method may include sharing a screen view or screen data of the first computing device with the second computing device via the connection.

In one aspect, the present invention relates to a method performed in a gateway for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing a first tunneling session with the first computing device on a first network, and establishing a second tunneling session with the second computing device on the second network. The gateway receives a request by the first computing device to initiate a communication session with the second computing device. The first computing device provides a first network address for contacting the second computing device. The first network address identifies a network address of the second computing device associated with the second tunneling session. The gateway receives a request by the first computing device to initiate a connection with the second computing device using the first network address, intercepts the request to initiate the connection, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The gateway communicates to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment, the first tunneling session or the second tunneling session via the gateway includes a Secure Socket Layer or a virtual private network. In another embodiment, the second computing device is located behind a firewall associated with the second network address. In a further embodiment, the method of the present invention provides the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling

session. Additionally, the gateway may communicate a key to the first computing device and to the second computing device.

In another aspect, the present invention is related to a system for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device. The first network may be disconnected from and not routable to the second network. The system includes a first computing device on the first network, and a second computing device on the second network. A third computing device establishes a first tunneling session with the first computing device and a second tunneling session with the second computing device. The system also includes a server accessible via the third computing device. In operation of the system, the server communicates via the third computing device to the first computing device a first network address identifying a network address of the second computing device associated with the second tunneling session. The first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address. The third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

In one embodiment of the system, the first tunneling session or the second tunneling session includes a Secure Socket Layer or a virtual private network. Furthermore, the third computing device may be a remote access gateway, such as an SSL VPN gateway. In another embodiment of the system, the second computing device is located behind a firewall associated with the second network address.

In an additional embodiment of the present invention, the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session, such as via an out of band TLS session. In one embodiment, the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the system of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data.

In some embodiments of the present invention, the system includes a first telecommunication device associated with the first computing device, and a second telecommunication device associated with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the system of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the first computing device and the second computing device communicate a remote display protocol via the connection. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the first computing device may share a screen view or screen data with the second computing device via the connection.

In another aspect, the present invention is related to a method for communicating via a lossless protocol a packet constructed to be transmitted via a lossy protocol. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a connection between a first computing device and a second computing device via a lossless protocol. In some embodiments, the second computing device may be a gateway, such as an SSL VPN gateway. The first computing device detects a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol. The first computing device communicates a false acknowledgement of receipt of the lossless protocol packet to the first computing device and/or the second computing device. The false acknowledgement of receipt of the lossless protocol packet prevents

employing the reliability algorithms and mechanisms of the lossless protocol. The first computing device communicates the lossless protocol packet to the second computing device. In some embodiments, the false acknowledgement of receipt of the lossless protocol packet is communicated prior to communicating the lossless protocol packet.

In one embodiment, the method of the present invention includes encrypting, by the first computing device, the one or more packets using a key. In some embodiments, the encryption key may be provided to the first computing device via an out of band transport security layer session between the first computing device and the second computing device. In a further embodiment, the method encrypts the one or more packets on a packet by packet basis.

In another embodiment of the method of the present invention, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by the first computing device and/or the second computing, the first computing device and/or the second computing prevents executing an operation associated with providing a lossless characteristic of the lossless protocol. In one embodiment, the lossless protocol is a transport control protocol.

In a further embodiment, the method of the present invention prevents the network stack of the first computing device and/or the second computing device from executing one or more of the following in connection with the lossless protocol: 1) a retransmit, 2) an ordering, 3) a flow control algorithm, 4) a naple's algorithm, and 5) a sliding window algorithm.

In one embodiment, the lossy protocol includes a user datagram protocol. In another embodiment, the method includes communicating, by the first computing device, the
lossless protocol packet via a secure socket layer or a transport security layer tunnel to the second computing device.

In another embodiment, the one or more packets of the payload comprises a real-time protocol. In an additional embodiment, the method includes communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

In one aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes receiving, at a first device, a first packet to be transmitted using an unreliable

transport protocol, and creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device. The first device transmits the first TCP packet to the second device. The method further includes receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol, and creating a second TCP packet including a second payload of the received second packet and the first TCP header information. Before receipt of an acknowledgement of the receipt of the first payload from the second device, the first device transmits the second TCP packet to the second device.

In one embodiment, the method of the present invention establishes the TCP connection with a port number associated with the unreliable transport protocol. In another embodiment, the method includes dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol. In some embodiments, the unreliable transport protocol is UDP.

In an additional embodiment, the method includes receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism. In some embodiments, the method establishes by the first device, the TCP connection with a VPN gateway device. In other embodiments, the method includes establishing peer-to-peer communications between the first device and the second device via the TCP connection. In another embodiment of the present invention, the method includes encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

In another aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes intercepting, at a second device, a first TCP packet created on a first device and received on the second device. The first TCP packet includes a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device. The intercepting of the method occurs before the first TCP packet is provided to a TCP stack on the second device. The method includes identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable

transport protocol, stripping the TCP header of information from the first TCP packet, and forwarding the first payload to an application using the unreliable data protocol.

In one embodiment, the unreliable protocol is UDP. In another embodiment, the step of identifying comprises identifying that the TCP header information includes a port number associated with the unreliable transport protocol. In some embodiments, the method includes intercepting, by the second device, the first TCP packet using a packet capture driver.

In some embodiments, the first device is a client device and the second device is a VPN gateway. Additionally, the method of the present invention includes performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

In a further aspect, the present invention relates to a system for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The system includes a first device and a second device. The first device has an application that generates a first and second packet. The first and second packet are intended to be transmitted using an unreliable transport protocol. The first device also has a filter process and a tunneling process. The filter process intercepts the first and second packets from the application and forwards the intercepted packets to the tunnel process. The tunnel process requests the opening of a TCP connection between the first device and a second device. The request to open the TCP connection indicates to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol. The tunnel process forwards the first and second packets as payloads in a first and second TCP packet to the second device. The tunnel process sends the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet.

The second device of the system of the present invention is in communication with the first device. The second device has second filter process and tunneling process. The second tunnel process opens the TCP connection requested by the first device, and identifies and forwards the source address of the TCP connection to the second filter process. The second filter process intercepts packets from the application received at the second device with the TCP connection source address in a header. The second filter process strips the TCP header from the received packets and forwards the stripped

packets to an intended destination, and circumventing the TCP/IP stack on the second device.

In one embodiment of the system of the present invention, the filter process on the first device and/or the second filter process of the second device is a packet capture driver. In some embodiments, the first device is a client device and the second device is a VPN gateway device. In one embodiment, the unreliable data protocol is UDP.

In another embodiment, the system also includes a third device to which the stripped packets are transmitted. Additionally, the second device may further include a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to the third device.

In a further aspect, the present invention is related to a method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a session between a first computing device and a second computing device. The session may established by an agent of the first computing device. The first computing device has a first network stack. The method detects, by the first computing device, a network packet having an encrypted payload, and determines a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload. The method alters the maximum transmission unit (MTU) parameter of the first network stack to the determined setting. As such, the reported MTU parameter is reduced to account for the encryption.

In one embodiment, the method of the present invention includes communicating the network packet via a secure socket layer or a transport layer security tunnel to the second computing device. The second computing device may be a gateway, such as an SSL VPN gateway. In another embodiment, the payload comprises a real-time protocol.

Additionally, in one embodiment, the method may further comprise altering the maximum transmission unit parameter via a network driver interface specification (NDIS) level mechanism of the first network stack In another embodiment, the method determines the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device. In one embodiment, the agent of the first computing device communicates via an IOCTL

application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

In some embodiments, the method of the present invention establishes the session between the first computing device and the second computing device via a gateway. In other embodiments, the method communicates by the first computing device real-time voice, audio, or data to the second computing device via the payload of the network packet. In yet another embodiment, the method may include communicating a false acknowledgement of receipt of the network packet to the first computing device and/or the second computing device before communicating the network packet. In one embodiment, the network packet comprises a lossless protocol packet, such as a transport control protocol. In another embodiment, the payload comprises a lossy protocol packet, such as a user datagram protocol.

In an additional aspect, the present invention is related to a method for a client to prioritize network communications of the client associated with an application of the client. The method includes intercepting, by the client, one or more network packets associated with one or more applications of the client, and storing the one or more network packets to a queue. The client determines the queued one or more network packets is associated with a first application of the client. The client indicates a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client. The client
provides the prioritized one or more network packets for communications via a network stack of the client.

In one embodiment, the method of the present invention includes determining, by the client, the queued one or more networks packets of the first application comprises real-time data. The real-time data may include one of the following: 1) a real-time protocol, 2) a user datagram protocol, and 3) a representation of voice or audio.

In another embodiment, the method includes preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In a further embodiment, the method includes holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon

communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In yet another embodiment of the present invention, the method includes intercepting, by the client, the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background.

In one embodiment of the present invention, the method includes associating a priority with the first application higher than a priority associated with the second application. In another embodiment, a user may specify the priority of the first application or the second application. In a further embodiment, the client receives the one or more network packets from a computing device. Also, the one or more applications may provide the one or more network packets for communicating from the client to a computing device.

In another aspect, the present invention is related to a client for prioritizing network communications of the client associated with an application of the client. The client includes a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client. The client also includes a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client. The client further includes an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

In one embodiment, the agent of the present invention determines the one or more networks packets of the first application comprises real-time data. The real-time data comprises one of the following: 1) a real-time protocol, 2) a user datagram protocol, and a 3) representation of voice or audio.

In a further embodiment, the agent or the network driver of the present invention prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In one embodiment, the network driver holds in the queue a network packet associated with the second application, and releases the held network packet upon communication

of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In another embodiment, the present invention, via the mechanism, intercepts the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background. Also, the first application may have a priority higher than the second application of the client. Furthermore, the client may include a configuration mechanism for a user to specify the priority. In some embodiments, the client receives the one or more network packets from a computing device. In other embodiments, the one or more applications provides the one or more network packets for communicating from the client to a computing device.

In an additional embodiment, the network driver includes a Network Driver Interface Specification (NDIS) driver. Also, the network driver may operate in kernel-mode of an operating system of the client. In some cases, the agent operates in user-mode of an operating system of the client. Furthermore, the agent or the network driver includes the mechanism for intercepting one or more network packets of the client.

In yet another aspect, the present invention is related to a method for shielding from a network disruption a session established via a first protocol. The method includes the steps of establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device. The network connection is associated with a network stack. A first portion of the network stack has one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack includes a layer for the first protocol and one or more layers of the network stack above the first protocol. The method includes detecting a disruption in the network connection causing the second portion of the network stack to be disestablished, and maintaining, by the agent, the session and the second portion of the network stack during the disruption. The method further includes re-establishing the first portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

In one embodiment, the method includes continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

In some embodiments, the method also includes dropping, by the first and/or second portion of the network stack, any network packets received during the disruption.

In another embodiment, the device comprises a remote access gateway or another computing device. In some cases, the method includes establishing the session via the first protocol of one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. Additionally, the method of the present invention may include communicating, by the agent, real-time data via the session between the client and the device. The real-time data may include a real-time protocol or the real-time data may represent voice or audio.

In some embodiments, the agent operates in user-mode of an operating system of the client. In one embodiment, the first portion of the network comprises one of a transport control protocol or an internet protocol. In another embodiment, the second portion of the network stack comprises one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol. The remote display protocol may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the method of the present invention is performed transparently to an application of the client communicating via the network connection. In one embodiment, the method includes intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application. In one embodiment, the method includes intercepting, by a network driver associated with the first portion of the stack, transparently to the application on the client one or more network packets associated with the application.

In an additional aspect, the present invention is related to a system for shielding from a network disruption a session established via a first protocol. The system has an agent of a client establishing a session between the client and a device over a network connection via a first protocol. The system includes a network stack having a first portion and a second portion, such as the network stack of the client. The second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol, and a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol. The system includes a detector for detecting a disruption in the network

connection causing the first portion of the network stack to be disestablished. In operation of the system and upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption. The client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

In one embodiment of the system of the present invention, the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack. In some embodiments, the first and/or second portion of the network stack drops any network packets received during the disruption.

In one embodiment, the device of the system is a remote access gateway or another computing device The first protocol used by the system of the present invention may include one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. In another embodiment, the agent of the present invention communicates real-time data via the session between the client and the device. The real-time data may include a real-time protocol, or a representation of voice or audio.

In some embodiments of the system, the agent operates in user-mode of an operating system of the client. In one system embodiment, the first portion of the network comprises a transport control protocol and/or or an internet protocol. In another embodiment, the second portion of the network stack includes one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol, which may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the system of the present invention maintains the second portion of the network stack and re-establishes the first portion of the network stack transparently to an application of the client communicating via the network connection. In one embodiment, the agent intercepts network packets transparently to an application of the client one or more network packets associated with the application. In one embodiment, the system also includes intercepting, by a network driver associated with

the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

The details of various embodiments of the invention are set forth in the accompanying drawings and the description below.

Brief Description of the Drawings

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent and may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

Figure 1A is a block diagram depicting an embodiment for practicing the operations of the present invention via a gateway in a network environment;

Figure 1B is a block diagram depicting another embodiment for practicing the operations of the present invention in a peer-to-peer network environment;

Figure 1C is a block diagram depicting an embodiment of a remote access client of the present invention for network communications;

Figures 1D and 1E are block diagrams depicting embodiments of a computing device useful in practicing an embodiment of the present invention;

Figure 2A is a block diagram depicting an embodiment of a peer-to-peer network environment for practicing an embodiment of the technique of the present invention for establishing a peer-to-peer communication route;

Figure 2B is a flow diagram depicting an embodiment of the steps performed to optimize peer-to-peer route optimization technique of the present invention;

Figure 3A is a block diagram depicting an embodiment of network stacks of any of the computing devices of illustrative environments depicted in Figures 1A-1C;

Figure 3B is a flow diagram depicting an embodiment of the steps performed to use a false acknowledgement of receipt of network packets to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 3C is a flow diagram depicting an embodiment of the steps performed to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 4 is a flow diagram depicting one embodiment of steps performed for adjusting the maximum transmission unit parameter;

Figure 5A is a block diagram depicting an environment of a client for providing client-side application-aware prioritization techniques;

Figure 5B is a flow diagram depicting one embodiment of the steps performed to provide client-side application-aware prioritization;

Figure 6A is a block diagram depicting an environment of an apparatus for shielding a network disruption from a device; and

Figure 6B is a flow diagram depicting one embodiment of the steps performed in to shield network disruption from a device.

Description

Certain illustrative embodiments of the present invention are described below. It is, however, expressly noted that the present invention is not limited to these embodiments, but rather the intention is that additions and modifications to what is expressly described herein also are included within the scope of the invention. Moreover, it is to be understood that the features of the various embodiments described herein are not mutually exclusive and can exist in various combinations and permutations, even if such combinations or permutations are not expressly made herein, without departing from the spirit and scope of the invention.

The illustrative embodiments of the present invention are generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one illustrative embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. The present invention also provides various techniques for optimizing the peer-to-peer communications established with or without the gateway. The peer-to-peer communications may include real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. In addition to establishing a peer-to-peer connection via gateway, the present invention also provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol, 2) payload shifting of

network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile clients. These techniques may be practiced in peer-to-peer communications between two clients in some embodiments, or in other embodiments, in communications between a client and a gateway or between one computing device via a gateway to another computing device, such as via an SSL VPN gateway of an illustrative embodiment of the present invention.

In the illustrative embodiments of the present invention, the peer-to-peer route optimization technique determines a more optimal route to a resource a client may be trying to access via a gateway. The client and the resource accessed by the client, such as a server or a peer computer, may have a more direct route than via the gateway. For example, the client and the server may be located near each other but distant from the gateway, and thus, are closer to each other than via the gateway. Furthermore, using a gateway causes at least one additional hop in the end-to-end network communications between the client and the server. Instead of the client and server communicating via the gateway using their virtual private network (VPN) assigned internet protocol (IP) network addresses, the gateway and remote access architecture of the present invention facilitates the client and server communicating to each other via a direct route in a peer-to-peer fashion without using the gateway. In some cases, however, the client and server may not have a direct path between each other as either the client and/or server may be behind a firewall, such as a Network Address Translation (NAT) firewall. The peer-to-peer route optimization techniques and remote access architecture of the present invention also provide techniques for the client and server to communicate directly via traversal of the firewall. As such, the peer-to-peer route optimization techniques of the present invention provides a shorter more optimal route between peer computers than via the gateway.

In the illustrative embodiments of the present invention, the false acknowledgement technique of an embodiment of the present invention enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. For example, a real time protocol (RTP) may be implemented over a user

datagram protocol (UDP) for voice over IP (VoIP) communications. A lossy or unreliable protocol, such as UDP, may be used for voice communications because, in some real-time voice applications, it may be more important to get network packets to a recipient on time rather than getting the network packets in order or guaranteeing the delivery of network packets. However, by way of virtual private network and remote access solutions using a secure communication and/or tunneling protocol, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS), a real-time application data constructed to be transmitted via a lossy protocol, such as UDP, may be communicated via a lossless or reliable protocol such as a transport control protocol (TCP). The techniques of the present invention allow a lossy protocol, such as RTP over UDP, to be communicated via a lossless protocol such as TCP, while avoiding one or more of the lossless characteristics of the lossless protocol from being applied to the communication. In the illustrative embodiment of the present invention, this technique communicates a false acknowledgement of receipt of the lossless protocol network packet to the corresponding network stacks to prevent the lossless protocol from executing algorithms that provide for reliability of the protocol. Using this technique, the lossy protocol can be communicated over a lossless protocol, such as via TCP, SSL or via a tunneling protocol of a gateway, for example, to make the communication secure, and have the lossy protocol network packets get to the recipient on time rather than getting to the recipient reliably. In one embodiment, this technique can be used to securely communicate real-time data communications such as VoIP over SSL or TLS between peers or via a gateway.

The illustrative embodiments of the present invention also provide another technique of payload shifting that enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. A first computing device receives a first packet to be transmitted using an unreliable transport protocol, and creates a first TCP packet including a first payload of the received first packet. The first TCP packet is created with a TCP header having information associated with a TCP connection established between the first and a second computing device. The first TCP packet is transmitted to the second computing device. A second packet to be transmitted using an unreliable transport protocol is received by the first computing, which in turn creates a second TCP packet including the payload of the received second packet but with the TCP header information of the first TCP packet. The second TCP packet is

transmitted to the second computing device before receiving an acknowledgement of the receipt of the first TCP packet from the second device. As such, the payload shifting technique communicates multiple unreliable transport protocol payloads under a TCP header until an acknowledgement of receipt is received.

In the illustrative embodiments of the present invention, the maximum transmission unit adjustment technique reduces the reported size of the maximum transmission unit (MTU) parameter of a network stack of a client to take into consideration the effect of the network packet size due to encryption of a payload. Encryption of the payload of a network packet increases the size of the network packet communicated to or by the client, and may cause a network packet to be fragmented. For example, a server may communicate to the client a network packet via an SSL gateway to the client. Although the server sends a network packet that should meet the MTU size the network stack of the client can handle, the encryption provided by the gateway increases the size of the network packet before it reaches the client. This may cause the network packet communicated from the server to the client via the gateway to be fragmented as the increased packet size from encryption may be too large for the MTU size of the client. The technique of the present invention adjusts the client's reported MTU size to report a smaller size to take in account for the overhead of the encryption. This technique reduces network fragmentation or otherwise prevents non-optimal fragmentation.

In the illustrative embodiments of the present invention, the prioritization technique provides for client-side and application-aware prioritization of network communications. That is, the remote access client of the present invention manages and controls network communication prioritizations on the client. The prioritizations are based on priorities of the application on the client. The remote access client transparently intercepts network communications associated with applications executing on the client, detects the network communication is associated with an application, and determines priorities for the network communications based on a priority for the application. For example, an application on the client may be communicating real-time data communications, such as VoIP, to a peer client or via a gateway. The remote access client may intercept a network packet, and detect, for example, the network packet contains real-time data or is from a VoIP application. The remote access client may indicate a priority for this network packet such that the network packet may be

communicated ahead of non-real-time data communications or ahead of network communications from other applications. As such, the prioritization techniques of the present invention may improve or increase the performance, operational characteristics, and user experience on the client based on the applications running on the client.

In the illustrative embodiments of the present invention, the network disruption shielding technique provides a persistent and reliable connection of a client to a network, such as a peer-to-peer communication session or a connection to a gateway. For example, a mobile client, such as a laptop with a software based IP telephone, may connect to a network for VoIP communications. A temporary disruption in a network connection may occur when the mobile client roams between different access points in the same network, or when the client switches between networks (*e.g.*, from a wired network to a wireless network). This disrupts the network service to the client and may drop the VoIP telephone call. Additionally, as the mobile client moves between access points, the mobile client may obtain a different IP network address, such as from a new Dynamic Host Configuration Protocol (DHCP) lease. This can also cause network connectivity and VoIP telephone communication disruption. The techniques of the present invention detects a disruption in the network and shields a portion of the network stack from the network disruption. The shielded portion of the network stack is maintained while the other portion of the network stack is reestablished and reconnected to the network. Once the network is available, the present invention continues with the client's network communications. In some embodiments, the network communications are queued during the network disruption and transmitted once the network is available. In other embodiments, such as for real-time data communications, network packets are dropped during the disruption to prevent the queuing of network packets that may cause latency in the real-time communication, such as VoIP telephone call.

Although the illustrative embodiments of the present invention may be generally described in connection with an internet protocol (IP) based protocol, such as a transport control protocol (TCP) or user datagram protocol (UDP), the techniques of the present invention may be used in any other types of networking environments with other networking protocols, such as any Internetwork Packet Exchange (IPX) protocol based networks using a Sequenced Packet Exchange (SPX) protocol. Also, although a lossy or unreliable protocol such as UDP and a lossless or reliable protocol such as TCP may be used for illustrating an embodiment of the present invention, any lossless/reliable and

lossy/unreliable protocol as known to those ordinarily skilled in the art may be used in practicing the operations of the present invention described herein. Furthermore, although some of the illustrative embodiments of the present invention may be described below in relation to real-time data communications, such as VoIP, the techniques of the present invention may be applied for non-real-time data communications as one ordinarily skilled in the art will also recognize and appreciate.

Additionally, at times, the illustrative embodiments of the present invention may be described in regards to peer-to-peer communications. In one aspect, a peer-to-peer model comprises a type of network in which any computer can act as both a server by providing access to its resources to other computers, and can act as a client by accessing shared resources from other computers. Although in another aspect, a peer-to-peer model may not comprise a notion of a client and a server, a client and a server may provide peer-to-peer communications as well as client to client, server to server, or a client/server to a computing device such as a gateway. In an additional aspect, peer-to-peer communications comprises a process whereby computers can exchange information between each other directly without the assistance of a third party network or a device, such as a gateway. Although peer-to-peer communications may be generally described as direct communication between computers, there may be other network elements between the computing devices to facilitate the transmission and/or communication, such as for example, a network hub.

Furthermore, although the illustrative embodiments of the present invention may be described peer-to-peer, point-to-point, client to server, or otherwise, one ordinarily skilled in the art will recognize and appreciate that the present invention may be practiced between computing devices in any manner via any network topology, and that any reference to peer-to-peer, client/server, or otherwise is not intended to limit the present invention in any way.

In one aspect, the present invention is related to a remote access architecture having a remote access client for communicating to a network via a gateway or peer-to-peer to another remote access client or another computing device. The remote access architecture of the present invention provides systems and methods for securely communicating network traffic transmitted between a private network behind a gateway to a client on an external network, such as public network. The remote access architecture of the present invention enables separation of the client from the private

network by providing network address translation (NAT) functionality on the gateway. A VPN gateway that uses Network Address Translation (NAT(provides masquerading of IP addresses of a client to shield the private network from direct layer-2 access by the client.

Referring now to Figure 1A, the environment 180 depicts a system for deploying the remote access architecture in an illustrative embodiment of the present invention. In brief overview, the environment 180 includes multiple computing devices 102a-102c (herein also referred to as clients 105a-105c) connected to a network 104 via one or more network connections 341a-341n. One or more of the clients 105a-105n may connect to a server 102a, a server farm 102e, or a peer computing devices 102d via a gateway 350.

Each client 105a-105n includes a remote access client 120a-120c, which will be described in more details in connection with Figure 1C, and one or more applications 338a-338n. Each of the clients 105a-105n communicate over the network 104 to the gateway 340 via a tunneling or gateway connections 341a-341n using any type and/or form of suitable tunneling or gateway protocols. In some embodiments, the gateway connections 341a-341n may be used for communicating securely, such as via encapsulating and encryption, or otherwise may use any other protocols, such as any real-time, lossless, or lossy protocol. In other embodiments, the gateway 340 provides a virtual private network connection between one or more of the clients 105a-105n and any of the computing devices 102d-102n.

The client 105 can be any type and/or form of computing device 102 that can run one or more applications 338 that access a network, such as network 104. The application 338 can be any type and/or form of application such as any type and/or form of web browser, web-based client, client-server application, a thin-client computing client, an ActiveX control, or a Java applet, or any other type and/or form of executable instructions capable of executing on client 105 or communicating via a network 104. The application 338 can use any type of protocol and it can be, for example, an HTTP client, an FTP client, an Oscar client, or a Telnet client. In some embodiments, the application 338 uses a remote display or presentation level protocol. In one embodiment, the application 338 is an ICA client, developed by Citrix Systems, Inc. of Fort Lauderdale, Florida. In other embodiments, the application 338 includes a Remote Desktop (RDP) client, developed by Microsoft Corporation of Redmond, Washington.

In other embodiments, the application 338 comprises any type of software related to VoIP communications, such as a soft IP telephone. In further embodiments, the application 338 comprises any application related to real-time data communications, such as applications for streaming video and/or audio.

The clients 105a-105n may access any of the resources provided via computing devices 102d-102n which may be on the same network 104, or which may be on a separate network, such as a private network. In some embodiments, computing devices 102a-102n may be on a network disconnected and not routable from the network 104 of the clients 105a-105n. In one embodiment, any of the clients 105a-105n may communicate with a peer computing device 102d having a remote access client 102n and application 338d. For example, the application 338d may comprise a portion of a client/server or distributed application corresponding to any of the applications 338a-338c on clients 105a-105n. In some embodiments, any of the remote access clients 120a-120n may communicate with the remote access client 120n via the gateway 340.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server 102e running an application 338e, which for example, may be an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Washington, a web or Internet server, or a desktop sharing server, or a collaboration server. In some embodiments, any of the application 338e may comprise any type of hosted service, such as GoToMeeting.com provided by Citrix Systems, Inc. of Ft. Lauderdale, Florida, WebEx.com provided by WebEx, Inc. of Santa Clara, California, or LiveMeeting.com provided by Microsoft Corporation of Redmond, Washington.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server farm 102n or server network, which is a logical group of one or more servers that are administered as a single entity. The server farm 102n may be running one or more applications 338N, such as an application 338f providing a thin-client computing or remote display presentation application. In one embodiment, the server 102e or server farm 102n executes as an application 338e-338n, any portion of the Citrix Access Suite™ by Citrix Systems, Inc., such as the MetaFrame or Citrix Presentation Server™, and/or any of the Microsoft Windows Terminal Services manufactured by the Microsoft Corporation.

Still referring to Figure 1A, the gateway 340 may comprise any type and/or form of gateway, such as a remote access server, that may be used to connect one or more computing devices on one network to other networks. In another aspect, the gateway 340 may be used to provide a virtual private network connection to give a client 105a-105c access to a private network. In a further aspect, the gateway 340 may be a hardware or software set-up that translates between two dissimilar protocols or disjoint or disconnected networks or systems. The gateway 340 may comprise a specialized hardware or networking device, or may be a computing device configured to act as a gateway. As such, the gateway 340 may comprise software, hardware, or any combination of software and hardware. In one embodiment, the client 105 and the gateway 340 communicate via any type and/or form of gateway or tunneling protocol 341a-341n, such as SSL or TLS, or the Citrix Gateway Protocol manufactured by Citrix Systems, Inc. of Ft. Lauderdale, Florida.

In some embodiments, the gateway 340 may decrypt encrypted packets received from a client 105a-105c, and may encrypt packets communicated to a client 105a-105n. The gateway 340 may be used to protect a private network, such as network 104. In some embodiments, the gateway 340 associates a client 105a-105c with a private IP address or an IP address of the private network. In one of these embodiments, when the gateway 340 receives a packet from the client 105a-105c, the gateway 340 transforms the IP address of the packet to the IP address associated with the client 105a-105c for the private network. In some embodiments, the gateway 340 may apply access control policies to network traffic to and/or from a client 105a-105c. For example, access controls policies may be applied to a packet received from the client prior to routing the packet to a final destination.

In one embodiment of the gateway 340, once a frame enters the gateway 340 via an SSL tunnel, the packet and its payload are dispatched via callbacks into a handlers executing in user mode, which provide functionality for SSL decryption. In another embodiment, openSSL may be used. In other embodiments, a hardware accelerator is used. In a further embodiment, the gateway 340 comprises one or more blades for providing remote access. Once the packet is decrypted, it is injected into an HTTP network stack where headers are assembled and passed on to the remote access blade. In a remote access blade, a packet is classified by the type of data contained within the packet. In one embodiment, the packet contains an HTTP header requesting login and

registration. In another embodiment, the packet seeks TCP/UDP/RAW/OTHER connection establishment. In still another embodiment, the packet contains connection-specific data. In yet another embodiment, the packet contains a special feature request such as collaboration with other users, fetching of user directory and presence or requesting telephony functionality such as conferencing and web cast. The remote access module dispatches the packet appropriately to the corresponding sub handler. For example, the client 105 may request that a connection be set up to a specific machine on the private network behind the gateway 340. The remote access module may consult with the access control module and if a positive response is returned, the remote access module may grant the request. In some embodiments, the remote access module 120 may grant the request by injecting subsequent frames on the private network using a frame forwarding module utilizing NAT/PAT to correlate incoming frames to corresponding SSL tunnels 341a-341n to a client 105a-105c.

The network 104 as illustrated in Figure 1A can be any type of network. The network 104 can be a local-area network (LAN), such as a company Intranet, a metropolitan area network (MAN), or a wide area network (WAN), such as the Internet or the World Wide Web. The topology of the network 104 may be a bus, star, or ring network topology. The network 104 and network topology may be of any such network or network topology capable of supporting the operations of the present invention described herein. The client 108 and gateway 340 can connect to one or more networks 104 through a variety of connections including standard telephone lines, LAN or WAN links (e.g., T1, T3, 56 kb, X.25, SNA, DECNET), broadband connections (ISDN, Frame Relay, ATM, Gigabit Ethernet, Ethernet-over-SONET), and wireless connections or any combination thereof. Connections can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, ARCNET, Fiber Distributed Data Interface (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and direct asynchronous connections).

In one embodiment of the present invention, the gateway 340 illustrated in Figure 1A is used to facilitate a direct peer-to-peer connection between computing devices 102a-102n. For example, client 105a may establish a tunneling session with the gateway 340 to access the peer computing device 102d. The gateway 340 negotiates with the remote access client 120a of client 105a and the remote access client 120n of computing device 102d to enable the client 105a to directly connect to the computing

device 102d without traversing the gateway 340. Once the network connection between the client 105a and computing device 102d is established, the client 105a can communicate in a peer-to-peer manner with computing device 102d. The gateway 340 of the present invention can facilitate a direct peer-to-peer connection between any of the computing devices 102a-102n illustrated in the environment 180. In one embodiment, the gateway 340 can facilitate a peer-to-peer connection between any of the clients 105a-105n, for example between client 105a and client 105b or between client 105b and client 105c. In another embodiment, the gateway 340 facilitates a peer-to-peer connection between computing devices 102d-120n, for example, between computing device 102d and server 102e or server farm 102n. In other embodiments, the gateway 340 facilitates a peer-to-peer connection between one of the clients 105a-105n and one of the computing devices 102d-102n. The techniques of facilitating a peer-to-peer connection via the gateway 340 will be discussed in more detail below in conjunction with Figures 2A and 2B.

Referring now to Figure 1B, the remote access client 120 of the present invention may be used in an illustrative embodiment of a peer-to-peer connection without a gateway 304. For example, the gateway 340 may facilitate a peer-to-peer connection between any of the computing device 102a-102n illustrated in Figure 1, and thereafter the computing devices 102a-102n communicate directly to each other in a peer-to-peer manner. In other embodiments, any computing device 102a may communicate directly to another computing device 102b or 102c via a network 104 without a gateway 340 facilitating the connection.

In brief overview of Figure 1B, the remote access client 120a may be deployed on a client 102a running one or more application 338a. The computing device 102a may connect over the network 104 to computing device 102b and/or computing device 102c. Computing device 102b may be a peer or client computing device also comprising a remote access client 120b. In some embodiments, remote access client 120a and 120b may communicate with each other via network 104, and may work in conjunction with each other for application 338a to communicate to application 338b, such as for a web-based or client/server application. In other embodiments, the remote access client 120a may communicate with computing device 120c which may be a server that does not execute a remote access client 120.

Figure 1C depicts a block diagram illustrating a system having a remote access client 120 for routing network packets from a client 105 to a network 104. In brief overview, the system includes a computing device102 (herein also referred to as a client 105) having an operating system that includes a user mode 332, also referred to as an application or user space, and a kernel-mode 334, which may be also referred to as the kernel or system level space. The client 105 runs an agent 326 that in one embodiment, may run in user-mode 332. The client 105 also runs a filter 322, which may, in one embodiment, execute in kernel-mode or the kernel space 334. In one embodiment, the filter 322 and the agent 326 form the remote access client 120 for routing packets via a network, or for otherwise providing remote access connectivity in accordance with the operations of the present invention described herein. The remote access client 120, or any portion thereof, such as the agent 326 or the filter 322, may execute in user-mode 332 or kernel-mode 334.

The client 105 may also have a network stack 310, which may comprise one or more network layers, such as any networks layers of the Open Systems Interconnection (OSI) communications model as those skilled in the art will recognize and appreciate. The network stack 310 may comprise one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11, as those skilled in the art will recognize and appreciate. Furthermore, the network stack 310 may include one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver. The network drivers may be included as part of the operating system of the computing device 102 or as part of any network interface cards or other network access components of the computing device 102. Additionally, any of the network drivers of the network stack 310 may be customized, modified or adapted to provide a custom or modified portion of the network stack 310 in support of any of the techniques of the present invention described herein. Additionally, some portions of the network stack 310 may operate in kernel-mode 334 while other portions run in user-mode 332, such as an application layer of the network stack 310.

The filter 322 may include a packet capturing mechanism 365, and the filter 322 and/or packet capturing mechanism 365 may comprise a network driver, such as a network driver operating at any layer, or portion thereof, of a network stack 310 of the client 105. The filter 322 and/or the packet capture mechanism 365 may comprise a driver complying with the Network Driver Interface Specification (NDIS), or a NDIS

driver. In another embodiment, the filter 322 and/or the packet capture mechanism 365 may comprise a min-filter or a mini-port driver. The packet capture mechanism 365 may also in some embodiments operate in kernel mode 334. Although the packet capture mechanism 365 is illustrated as part of the filter 322, the packet capture mechanism 365 may be separate from the filter 322. Additionally, the filter 322 and the packet capture mechanism 365 may operate at different layers, or portions thereof, of a network stack of the client 105.

The filter 322 may use a filter table for filtering packets. The filtering table is used to determine what action to take against packets, such as packets intercepted by the packet capture mechanism 365. The filter 322 can inspect the contents of the packets, such as routing information, to determine the action to take based on the filtering table. In some embodiments, the filter 322 may drop or accept the network packets depending on their content. In other embodiments, the filter 322 may route the network packets to the agent 326 based on the packets content and/or the filtering table. The filter table may also be used to ensure that unwanted packets are discarded. The filter 322 may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses.

In some embodiments, the filtering table includes information about a private network. In other embodiments, a filter 322 on a client computing device 102 receives the filtering table. In one of these embodiments, the filter 322 receives the filtering table from an application 338 or an agent 326 on the computing device 102. In another of these embodiments, the filter 322 receives configuration settings from the agent 326 and stores the configuration settings in a filtering table.

The packet capture mechanism 365 may intercept any of the network traffic of the client 105, such as network packets associated with the application 338. In some embodiments, the packet capture mechanism 365 intercepts network traffic transparently to the application 338, the agent 326, the gateway 340, or to any portion of the network stack 310 of the client 105, such as any other driver or layer operating at a layer above or below the layer the packet capture mechanism 365 operates. In this manner, the present invention can be used with and support any of the techniques described herein and for any application and any protocol used by the application. In one embodiment, the packet capture mechanism 365 intercepts outbound packet traffic, such as any network traffic communicated via network 104 and/or gateway 340. The packet capture

mechanism 365 may forward the packets to the agent 325 or a frame monitor mechanism 360 of the agent 326. In some embodiments, the filter 322 communicates with the agent 326 via asynchronous I/O control messages. In one of these embodiments, the packet capture mechanism 365 may forward packets addressed to a private network behind a gateway 340 via asynchronous I/O control messages. In other embodiments, the filter 322 communicates with the agent 326 running in the user space 334 via UDP packets. In one embodiment, the filter 322 receives configuration settings from the agent 326 driver via asynchronous I/O control messages. The configuration settings may include information regarding which networks, protocols, or types of packets to filter. In one embodiment, the filter 322 stores the configuration settings in a filtering table. In another embodiment, the filter 322 receives a filtering table including the configuration settings.

In one embodiment, the filter 322 intercepts all outbound packets of the client 105 for inspection. For example, in some embodiments, the filter intercepts a packet generated by an application 338 executing in user-mode 332 for transmission by the client 105. If the packet satisfies a condition listed in the filtering table, the filter 322 may transmit the packet to the agent 326 and not to the original destination of the packet. The filter 322 may use an asynchronous I/O control message to forward the packet to the agent 326. The filter 322 may transmit the packet to the agent 326 in accordance with or responsive to a routing table .

In some embodiments, the agent 326 and the filter 322 communicate via an IOCTL application programming interface (API), such as any IOCTL libraries and function calls provided by the Microsoft Windows family of operating systems. In other embodiments, the IOCTL based interface between the agent 326 and the filter 322 may be provided by any portion of the operating system running on the client 105. Although discussed in terms of I/O control message and the IOCTL interface, the agent 326 and the filter 322 may communicate via any suitable mechanism and/or means.

The kernel 334 of client 105 may include an NDIS interface. In some embodiments, the NDIS interface includes a plurality of intermediate filters. In one embodiment, a packet passes through the NDIS interface and may be inspected by the plurality of intermediate filters. Although the filter 322 may be provided as an NDIS driver, the filter 322 may also be a process or other set or type of executable instructions executing in the kernel 334.

The agent 326 of the present invention may execute in the application space 332 or user-mode on the client 105. In other embodiments, the agent 326 operates in kernel-mode 334. In some embodiments, the agent 326 provides functionality for receiving packets from the filter 322. In other embodiments, the agent 326 provides functionality for applying a policy to a received packet. In still other embodiments, the agent 326 provides functionality for managing an SSL tunnel to the gateway 340. In yet other embodiments, the agent 326 provides functionality for encrypting and transmitting a packet to the gateway 340. The agent 326 may include frame monitor mechanism 360. The frame monitor 360 may include policies and logic for applying a policy to a received packet. The agent 326 may transmit a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.

In some embodiments, the frame monitor 360 may apply a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet. In other embodiments, the frame monitor 360 may identify an application 338 that generated the packet. In some of these embodiments, the frame monitor 360 may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application 338. In another embodiment, the frame monitor 360 may perform a checksum on the packet to verify that the identified application actually generated the packet.

In other embodiments, the packet capture mechanism 365 may be included in the agent 326 instead of or in addition to the filter 322. As such, the agent 326 may intercept network traffic. The packet capture mechanism 365 may use any hooking application programming interface (API) to intercept, hook, or otherwise obtain inbound and/or outbound packets of the client 105, such as the network traffic associated with application 338.

In one embodiment, a TCP connection is initiated by an application 338 executing on the client 105 for transmission of IP packets to a target computing device, such as computing device 102c of Figure 1B or the gateway 340 in Figure 1A. The remote access client 120 may intercept or capture the IP packets generated by the application 338. The remote access client 120 may send a TCP acknowledgement packet to the application 338 and terminate the TCP connection initiated by the application 338. Then, the remote access client 120 creates a second TCP connection to the second computing device 102c or the gateway 340 and transmits the captured IP

packets via the second TCP connection. In some embodiments, the remote access client 120 may store a captured IP packet in a buffer. In these embodiments, the remote access client 120 may transmit the buffered IP packets via the second TCP connection to the second computing device 102c. Storing the captured IP packets in a buffer enables preservation of the packets in the event of a disruption in the network connection.

In one embodiment, upon receipt of the captured IP packets, the gateway 340 may create a third TCP connection between the gateway 340 and the targeted computing device 102d, such as in Figure 1A. The gateway 340 may maintain a port-mapped Network Address Translation (NAT) table, enabling the gateway 340 to transmit response packets from the target computing device 102d to the port monitored by the application 338 that originally generated the IP packet on the client 105. Because the client 105 communicates only with a public network address of the gateway 3400, the client 105 is unaware of the network address of the target computing device 102d, increasing security to the network on which the target computing device 102d resides. Similarly, since the gateway 340 originates the TCP connection to the target computing device 102d, the target computing device 102d does not receive the address information of the client 105, protecting the client 105 and the network on which it resides. Additionally, since the gateway 340 receives the IP packets, the gateway 340 may make a determination responsive to a policy or security check as to whether or not to transmit the IP packets to the target computing device 102d, further increasing protection to the network on which the target computing device 102d resides.

In one embodiment, the present invention provides a method for securing a packet transmitted from a private, secured network behind a gateway 340 to a client 105 on an external network 104. The invention enables separation of the client 105 from the private network by providing network address translation (NAT) functionality on the gateway 340. A VPN gateway that uses NAT provides masquerading of IP addresses of a client 105 to shield the private network from direct layer-2 access by the client 105.

In one aspect, any portion of the remote access client 120, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365, or any portion thereof may comprise software, hardware, such as an ASIC or an FPGA, or any

combination of software and/or hardware. In some embodiments, portions of the remote access client 120 may be provided via one or more blades on the client 105.

Although the remote access client 120 is illustrated with multiple components, such as an agent 326 and a filter 322, one ordinarily skilled in the art will recognize and appreciate that the operations and functionality of the remote access client 120 described herein may be practiced in a single mechanism or single component. For example, in some embodiments, the operations and functionality of the remote access client 120 may be included within an application 338. In one embodiment for example, the functionality and operations of the remote access client 120 may be provided just as an agent 326, and in another embodiment, just as a network driver, such as the filter 322.

In some embodiments, the remote access client 120, or any portion thereof, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365 may comprise an application, module, service, computer program, software component, web service, web component, library, function, process, task, thread, or any other type and/or form of executable instruction which is designed to and capable of executing the functionality of the present invention as described herein, and which may operate in any portion or combination of user-mode 332 and/or kernel-mode 334.

As illustrated in Figures 1A-1C, the remote access client 120 of the present invention may be deployed and used in a variety of ways to communicate and provided remote access over a network to other computing devices, such as via a gateway 340 or directly between peer computing devices. In these variety of environments, the remote access client 120 may be used to practice one or more of the optimization techniques of the present invention as described in more detail below. For example, the remote access client 120 may be used for optimizing any real-time data communications, such as VoIP, desktop sharing, or web conferencing in any of the illustrative environments of Figures 1A-1C.

In the illustrative embodiments of Figures 1A-1C, the computing devices 102a-120n, such as for any of the clients 105, server, or the gateway 340, may be provided as any type and/or form of computing device such as a personal computer or computer server of the sort manufactured by the Hewlett-Packard Corporation of Palo Alto, California or the Dell Corporation of Round Rock, TX. Figures 1D and 1E depict block diagrams of a computing device 102 useful for practicing an embodiment of the present invention. As shown in Figures 1D and 1E, each computing device 102 includes a

central processing unit 102, and a main memory unit 104. As shown in Figure 1D, a typical computing device 102 may include a visual display device 124, a keyboard 126 and/or a pointing device 127, such as a mouse. Each computing device 102 may also include additional optional elements, such as one or more input/output devices 130a-130b (generally referred to using reference numeral 130), and a cache memory 140 in communication with the central processing unit 102.

The central processing unit 102 is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104. In many embodiments, the central processing unit is provided by a microprocessor unit, such as: the 8088, the 80286, the 80386, the 80486, the Pentium, Pentium Pro, the Pentium II, the Celeron, or the Xeon processor, all of which are manufactured by Intel Corporation of Mountain View, California; the 68000, the 68010, the 68020, the 68030, the 68040, the PowerPC 601, the PowerPC604, the PowerPC604e, the MPC603e, the MPC603ei, the MPC603ev, the MPC603r, the MPC603p, the MPC740, the MPC745, the MPC750, the MPC755, the MPC7400, the MPC7410, the MPC7441, the MPC7445, the MPC7447, the MPC7450, the MPC7451, the MPC7455, or the MPC7457 processor, all of which are manufactured by Motorola Corporation of Schaumburg, Illinois; the Crusoe TM5800, the Crusoe TM5600, the Crusoe TM5500, the Crusoe TM5400, the Efficeon TM8600, the Efficeon TM8300, or the Efficeon TM8620 processor, manufactured by Transmeta Corporation of Santa Clara, California; the RS/6000 processor, the RS64, the RS 64 II, the P2SC, the POWER3, the RS64 III, the POWER3-II, the RS 64 IV, the POWER4, the POWER4+, the POWER5, or the POWER6 processor, all of which are manufactured by International Business Machines of White Plains, New York; or the AMD Opteron, the AMD Athlon 64 FX, the AMD Athlon, or the AMD Duron processor, manufactured by Advanced Micro Devices of Sunnyvale, California. The computing device 102 may be based on any of the above described processors, or any other processor capable of operating as described herein.

Main memory unit 104 may be one or more memory chips capable of storing data and allowing any storage location to be directly accessed by the microprocessor 100, such as Static random access memory (SRAM), Burst SRAM or SynchBurst SRAM (BSRAM), Dynamic random access memory (DRAM), Fast Page Mode DRAM (FPM DRAM), Enhanced DRAM (EDRAM), Extended Data Output RAM (EDO RAM), Extended Data Output DRAM (EDO DRAM), Burst Extended Data Output

DRAM (BEDO DRAM), Enhanced DRAM (EDRAM), synchronous DRAM (SDRAM), JEDEC SRAM, PC100 SDRAM, Double Data Rate SDRAM (DDR SDRAM), Enhanced SDRAM (ESDRAM), SyncLink DRAM (SLDRAM), Direct Rambus DRAM (DRDRAM), or Ferroelectric RAM (FRAM). The main memory 104 may be based on any of the above described memory chips, or any other available memory chips capable of operating as described herein. In the embodiment shown in Figure 1E, the processor 100 communicates with main memory 104 via a system bus 150 (described in more detail below). Figure 1E depicts an embodiment of a computing device 102 in which the processor communicates directly with main memory 104 via a memory port 103. For example, in Figure 1E the main memory 104 may be DRDRAM.

Figures 1D and 1E depict embodiments in which the main processor 100 communicates directly with cache memory 140 via a secondary bus, sometimes referred to as a backside bus. In other embodiments, the main processor 100 communicates with cache memory 140 using the system bus 150. Cache memory 140 typically has a faster response time than main memory 104 and is typically provided by SRAM, BSRAM, or EDRAM.

In the embodiment shown in Figure 1D, the processor 100 communicates with various I/O devices 130 via a local system bus 150. Various busses may be used to connect the central processing unit 102 to any of the I/O devices 130, including a VESA VL bus, an ISA bus, an EISA bus, a MicroChannel Architecture (MCA) bus, a PCI bus, a PCI-X bus, a PCI-Express bus, or a NuBus. For embodiments in which the I/O device is a video display 124, the processor 100 may use an Advanced Graphics Port (AGP) to communicate with the display 124. Figure 1E depicts an embodiment of a computer 102 in which the main processor 100 communicates directly with I/O device 130b via HyperTransport, Rapid I/O, or InfiniBand. Figure 1E also depicts an embodiment in which local busses and direct communication are mixed: the processor 100 communicates with I/O device 130a using a local interconnect bus while communicating with I/O device 130b directly.

The computing device 102 may support any suitable installation device 116, such as a floppy disk drive for receiving floppy disks such as 3.5-inch, 5.25-inch disks or ZIP disks, a CD-ROM drive, a CD-R/RW drive, a DVD-ROM drive, tape drives of various formats, USB device, hard-drive or any other device suitable for installing software and programs such as the remote access client software 120 related to the present invention.

The computing device 102 may further comprise a storage device 128, such as one or more hard disk drives or redundant arrays of independent disks, for storing an operating system and other related software, and for storing application software programs such as any program related to the remote access client 120 of the present invention. Optionally, any of the installation devices 118 could also be used as the storage device 128. Additionally, the operating system and the proxy software 120 can be run from a bootable medium, for example, a bootable CD, such as KNOPPIX®, a bootable CD for GNU/Linux that is available as a GNU/Linux distribution from knoppix.net.

Furthermore, the computing device 102 may include a network interface 118 to interface to a Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (*e.g.*, 802.11, T1, T3, 56kb, X.25), broadband connections (*e.g.*, ISDN, Frame Relay, ATM), wireless connections, or some combination of any or all of the above. The network interface 118 may comprise a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 102 to any type of network capable of communication and performing the operations described herein.

A wide variety of I/O devices 130a-130n may be present in the computing device 102. Input devices include keyboards, mice, trackpads, trackballs, microphones, and drawing tablets. Output devices include video displays, speakers, inkjet printers, laser printers, and dye-sublimation printers. The I/O devices may be controlled by an I/O controller 123 as shown in Figure 1D. The I/O controller may control one or more I/O devices such as a keyboard 126 and a pointing device 127, e.g., a mouse or optical pen. Furthermore, an I/O device may also provide storage 128 and/or an installation medium 118 for the computing device 102. In still other embodiments, the computing device 102 may provide USB connections to receive handheld USB storage devices such as the USB Flash Drive line of devices manufactured by Twintech Industry, Inc. of Los Alamitos, California.

In further embodiments, an I/O device 130 may be a bridge 170 between the system bus 150 and an external communication bus, such as a USB bus, an Apple Desktop Bus, an RS-232 serial connection, a SCSI bus, a FireWire bus, a FireWire 800

bus, an Ethernet bus, an AppleTalk bus, a Gigabit Ethernet bus, an Asynchronous Transfer Mode bus, a HIPPI bus, a Super HIPPI bus, a SerialPlus bus, a SCI/LAMP bus, a FibreChannel bus, or a Serial Attached small computer system interface bus.

A computing device 102 of the sort depicted in Figures 1D and 1E typically operate under the control of operating systems, which control scheduling of tasks and access to system resources. The computing device 102 can be running any operating system such as any of the versions of the Microsoft® Windows operating systems, the different releases of the Unix and Linux operating systems, any version of the MacOS® for Macintosh computers, any embedded operating system, any real-time operating system, any open source operating system, any proprietary operating system, any operating systems for mobile computing devices, or any other operating system capable of running on the computing device and performing the operations described herein. Typical operating systems include: WINDOWS 3.x, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS NT 3.51, WINDOWS NT 4.0, WINDOWS CE, and WINDOWS XP, all of which are manufactured by Microsoft Corporation of Redmond, Washington; MacOS, manufactured by Apple Computer of Cupertino, California; OS/2, manufactured by International Business Machines of Armonk, New York; and Linux, a freely-available operating system distributed by Caldera Corp. of Salt Lake City, Utah, Java or Unix, among others.

In other embodiments, the computing device 102 may have different processors, operating systems, and input devices consistent with the device. For example, in one embodiment the computer 102 is a Zire 71 personal digital assistant manufactured by Palm, Inc. In this embodiment, the Zire 71 operated under the control of the PalmOS operating system and includes a stylus input device as well as a five-way navigator device.

Moreover, the computing device 102 can be any workstation, desktop computer, laptop or notebook computer, server, handheld computer, mobile telephone, any other computer, or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described herein.

In one aspect, the present invention is related to providing various techniques for optimizing communications between computing devices, such as depicted in any of the illustrative environments Figures 1A-1C. The present invention provides the following

techniques, which may be practiced stand-alone or in any combination: 1) peer-to-peer route optimization, 2) communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reducing network fragmentation by adjusting maximum transmission unit (MTU) adjustment to account for encryption, 4) client-side application-aware network communication prioritization, and 5) shielding a device from network disruption. The peer-to-peer route optimization technique will be discussed in conjunction with Figures 2A and 2B, techniques for communications via a lossless protocol of packets constructed for transmission via a lossy protocol are discussed in conjunction with Figures 3A and 3B, the MTU adjustment technique in conjunction with Figure 4, the client-side application-aware prioritization technique in conjunction with Figures 5A and 5B, and the network disruption shielding in conjunction with Figures 6A and 6B.

In one aspect, the present invention is related to providing a peer-to-peer route optimization technique between a first computing device accessing a second computing device via a gateway, such as the gateway 340 illustrated in Figure 1A. The peer-to-peer routing techniques provides a more optimal and direct communication between computing devices establishing or attempting to establish a communication session via a gateway. The illustrative method 260 of an embodiment of the present invention will be discussed in view of the illustrative environment 200 of Figure 2A. In brief overview, the environment 200 includes a gateway 340 providing remote access connectivity to a private network, such as a network with IP address ranges 10.10.10.XXX. The gateway 340 in association with the private network may have assigned an IP address of 10.10.10.2 for communications on the private network. This private network may include a server 102c. Also, the private network comprises a telecommunication device 210c, such as any type and/or form of VoIP telephone. The telecommunication device 210c is assigned IP address 10.10.10.100 on the private network.

In one embodiment, the server 102 comprises a signaling server, which may provide any type and/or form of signaling services for establishing a communication session between computing devices, such as a first computing device 102a and a second computing device 102b. In one embodiment, the server 102c supports a Session Initiation Protocol, SIP, which is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. In one embodiment, SIP works in the

application layer of the Open Systems Interconnection (OSI) communications model. In some embodiments, the first computing device 102a initiates a session via signaling, such as via the SIP protocol, to the signaling server 102c via signaling path 220. In one embodiment, the signaling server 102c in conjunction with the gateway 340 is used for establishing a media path 225 between the first computing device 102a and the second computing device 102b, such as for a VoIP telecommunication session between telephones 210a and 210b.

The first computing device 102a of environment 200 may be part of a network, private or public, accessing the gateway 340 via network 104 over the connection 341a and traversing the firewall 205a. The firewall 205a provides access to and traversal of a public network, and has assigned the IP address of 24.24.24.100. The first computing device 102a may be in communication with, or interfaced or coupled to a telecommunication device 210a, such as a VoIP communication device, or any other real-time data communication device. The second computing device 102b may be part of a private network and have assigned the IP address of 192.168.20.20. Additionally, the second computing device 102b may include a software based telecommunication device 210b, such as software-based VoIP telecommunication device or program. The second computing device 102b may access the gateway 340 via network 104 over connection 341b and traversing firewall 205b having a public network IP address of 216.216.10.10. The firewalls 205a and 205b may be any type and/or form of firewall as known to those ordinarily skilled in the art, such as a NAT firewall.

The first computing device 102a and second computing device 102b of Figure 2A includes and uses the remote access client 120 of the present invention to provide an ad-hoc peer-to-peer virtual network connectivity in the environment 200. In addition to maintaining a tunnel and virtual private connection, such as an SSL VPN connection, to the gateway 340, the remote access client 120 of the present invention also has logic, functionality, and operations to establish a direct ad-hoc connection, such as an SSL VPN connection, to a peer it is trying to reach. In view of Figure 2A, the illustrative method 260 of Figure 2B will be used to discuss how a peer-to-peer secure communication session is established for the media path 225 in one illustrative embodiment of the present invention. The peer-to-peer routing technique of the present invention as illustrated by method 260 provides better voice quality and reduces latency related to VoIP communications as well as other real-time data communications.

In brief overview of illustrative method 260, at step 262, the computing devices 102a and 102b establish tunneling sessions with the gateway 340. At step 264, the first computing device 102a initiates a session to second computing device 102b via gateway 340 using signaling protocol via the signaling path 220 to signaling server 102b. The session may be initiated by the telecommunication device 102a in communication with the first computing device 102a. At step 266, a signaling server 102c sets up the telecommunication session, and at step 268, provides the first computing device 102a with a first network identifier of the second computing device 102b. The first network identifier comprises the network address, such as a host name or IP address, of the second computing device 102b based on its IP address established via the tunnel 341b with the gateway 340. At step 270, the first computing device 102a communicates to the second computing device 102b using the first network identifier to establish a connection or communication session.

In further overview, at step 272, the gateway 340 intercepts the communications by the first computing device 102a and provides the first computing device 102a a second network identifier for the second computing device 102b. The second network identifier comprises an IP address or host name of the second computing device 102a directly or publicly accessible by the first computing device 102a, such as the last known public IP address of the second computing device 102b. At step 274, in one embodiment, the gateway 340 communicates to the second computing device 102b to request the second computing device 102b establish a swimmer session for first computing device 102a to connect to the second computing device 102b via firewall 205b. In some embodiments, the gateway 340, at step 276, may negotiate or otherwise provide encryptions keys for the first computing device 102a and second computing device 102b. At step 278, the first computing device 102a establishes a direct connection, communication session, or media path 225 to the second computing device 102b. In other embodiments, at step 280, the first computing device 102a and/or second computing device 102b match encryption keys received by the other computing device before allowing communications.

In some embodiments of illustrative step 262, the computing device 102a and 102b may establish a connection with the gateway 340 by any suitable means and/or mechanisms, such as by any type and/or form of tunneling or gateway protocol. In some embodiments, the connections 341a and 341b to the gateway 340 may form a virtual

private network connection, and in other embodiments, may use SSL or TLS to provide secure communications to the private network, such as the private network identified by the IP range 10.10.10.XXX in illustrative Figure 2A. In one embodiment, the computing devices 102a and 102b connect to the gateway 340 by traversing a firewall 205a-205b via a public network, while, in other embodiments, the computing devices 102a and 102b may connect to the gateway 340 via a private network, and may not traverse a firewall 205a-205b. One ordinarily skilled in the art will recognize and appreciate the variety of ways the computing devices 102a-102b may connect to and communicate with the gateway 340.

At illustrative step 264, in one embodiment, the telecommunication device 210a, such as a hard IP phone, initiates a telecommunication session, such as a telephone call, to the telecommunication device 210b, such as a soft IP phone. In some embodiments, the telecommunication device 210a initiates the telephone call by indicating the extension of the telecommunication device 210b. When the telecommunication device 210a initiates the telecommunication session, this initiation, indication, or request to establish a telecommunication session or media session may be sent to the signaling server 102a via SIP protocol, a proprietary signaling protocol, or any other type of protocol suitable for signaling. The signals are communicated via signaling path 220 via the tunneling session 341a to the gateway 230 and reach the signaling server 102c via the intranet routes of the private network behind the gateway 340.

Although the illustrative embodiment of method 260 is discussed in view of VoIP or telecommunication signaling and sessions, one ordinarily skilled in the art will recognize and appreciate that the present invention may be used for initiating any type and/or form of communication session, real-time or otherwise, such as an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. As such, the telecommunication devices 210a-210b, signaling/signal path 220, and signaling server 120a may accordingly and suitably comprise the type and/or form of device, signaling, protocols, and communications corresponding to the type and/or form of communication session.

In some embodiments of illustrative step 266, the signal server 102c may set up, negotiate, or establish any type and/or form of communication session, and in one embodiment the signaling server 102c sets up a telecommunication session, such as the VoIP telephone call initiated by the telecommunication device 210a. When setting up

the telecommunication or other media session, the signaling server 102c, at step 270, instructs, requests, signals or otherwise communicates to the initiating telecommunication device 210a and/or first computing device 102a to contact, signal, connect, or otherwise communicate to the peer telecommunication device 210b via a certain network address. In some embodiments, the network address provided by the signaling server 102c to the initiating telecommunication device 210a comprises the network address for the computing device 102b on the private network, i.e., 10.10.10.XXX, behind the gateway 340. In one embodiment, the network address for the peer telecommunication device 210b may comprise an enterprise private network address.

At this point, instead of contacting the peer telecommunication device 210b via its VPN private IP address, the illustrative method of 260, via the remote access client 120 facilities the telecommunication device 210a and/or the first computing device 102a to directly contact the peer or target telecommunication device 210b or the second computing device 102b. The techniques of the present invention is not specific to any VoIP protocol, and may be applied to any other protocols, such as any peer-to-peer protocol between computing devices. The techniques of the present invention makes decisions by way of the IP address of the resource a client is trying to connect with.

At step 270, when the telecommunication device 210a initiates a data connection to the telecommunication device 210b with the first network address provided by the signaling server 120c at step 268, such as the VPN private IP address of the soft IP phone, the gateway 340 intercepts the communication to provide the telecommunication device 210 and/or first computing device 102b with a second network address for contacting the telecommunication device 210b. In one embodiment, the gateway 340 intervenes and sends an out of band signal over the same established VPN tunnel 341a to the first computing device 102a that is facilitating traffic for the hard IP phone 210a. One ordinarily skilled in the art will recognize and appreciate that the gateway 340 may communicate to the telecommunication device 210 and/or computing device 102a that network address for contacting the computing device 102b and/or telecommunication device 210b directly by any suitable means and/or mechanisms. For example, the gateway 340 may communicate the second network address to the first computing device 102a via a second tunneling session.

In some embodiments, the gateway indicates to the first computing device 102a of the last known public IP address that the second computing device 102b which is running the soft IP phone 210b used to contact the gateway 340. In other embodiments, this public IP may not be the actual IP address of the second computing device but may be the IP address of the firewall 205b that the second computing device 102b is behind. If the computing device 210a contacts the public IP address of the firewall 205b directly, packets may be rejected by the firewall 205b. In these embodiments, the gateway 340 instructs the computing device 102b to establish what is known to those skilled in art as a swimmer session to the first computing device 102a. A forward hole is punched in the firewall 205b via which the first computing device 102a can traverse or get back in. In other embodiments, any suitable means and/or mechanism may be used to allow the first computing device 102a to traverse the firewall 205b to connect and communicate with the second computing device 102b.

Although illustrative method 260 is discussed in conjunction with environment 200 of Figure 2A having the second computing device 102n behind a firewall 205a, as one ordinarily skilled in the art will recognize and appreciate, the illustrative method 260 can be used in environments where the second computing device 102b is directly accessible without traversing a firewall 205a. As such, the illustrative method 260 may not need to at step 274 instruct the second computing device 102b to provide a swimmer session or other mechanism for the first computing device 102a to connect to the second computing device 102b.

In some embodiments, the gateway 340, at step 276, may negotiate a secret key between the computing devices 102a-103b for secure communications. The remote access client 120 on the computing devices 102a-102b may use this key for secure and encrypted communicates, and/or to authenticate or authorize the other computing device. In other embodiments, to ensure that malicious computing devices do not take advantage of this open hole, the gateway 340 at step 276 negotiates a secret key between the two computing devices 102a and 102b and the respective remote access clients 120 ensure that the keys match before allowing data communication. For example, in the embodiment of establishing a swimmer session, this key ensures that the packets coming in the open hole are from the computing device that the swimmer session was meant for.

In other embodiments, the gateway 340 does not perform step 276 to provide a secure mechanism of peer-to-peer communication sessions between the computing

devices 102a-102b. For example, the computing devices 102a-102b may be in the same private enterprise network and therefore, may be trusted. In further embodiments, instead of the gateway 340 negotiating a secret key, the computing devices 102a-102b use any suitable means and/or mechanism for authenticating and/or authorizing the other computing device for peer-to-peer communications. In some embodiments, the computing devices 102a-102b may authenticate and/or authorize via the gateway tunneling sessions, such as via path 341a, or at step 280, via the media path 225 established at step 278. For example, the remote access clients 120 of each computing device 102a-102b may check for matching keys over established media path 225 before allowing any data to be communication over the connection 225.

At step 278, the direct media path 224 for any type and/or form of communications is established between the computing devices 102a-102b without traversing the gateway 340, and, in some embodiments, not using the respective VPN assigned IP addresses of the computing devices 102a-102b but instead their public IP address or the IP address assigned to them by their resident network. Using the techniques of the present invention, the respective remote access client 120 of computing devices 102a-102b act as temporary peer-to-peer SSL gateways to each other, decrypting each other's SSL session directly without communicating via the gateway 340. The direct peer-to-peer communication session via path 225 avoids the extra-hop via the gateway 340. This will reduce any latency due to taking a longer route via the gateway 340, and will improve the quality, performance, and experience of real-time data communications, such as the VoIP communications illustrated in Figure 2A.

In some embodiments, the gateway 340 may be configured to automatically perform the techniques of illustrative method 260 every time a computing device 102 is trying to establish a peer-to-peer communication session or otherwise access a resource via the gateway 340. In other embodiments, the gateway 340 may be configured to automatically perform the techniques of the illustrative method 260 only for a certain IP address range either for a source IP address, a destination IP address, or any combinations thereof. In further embodiments, the gateway 340 may perform this technique based on the type of application and/or resource being accessed via the gateway 340. For example, in one embodiment, the gateway 340 may automatically perform this technique for any type of desktop or screen sharing application sharing screen data via the gateway 340. In other embodiments, the gateway 340 may determine

to perform this technique based on any type and/or form of business rules, access control policies, or other configuration, algorithm, and statistics. For example, the gateway 340 may perform this technique based on ping-based timing statistics between peer computing devices. If the peer computing devices are closer to each other than the gateway 340, the gateway performs the peer-to-peer routing technique. One ordinarily skilled in the art will recognize and appreciate the various ways the gateway of the present invention may be adapted or otherwise configured to perform the peer-to-peer routing technique of the present invention.

In one aspect, the present invention is related to allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol. In one technique illustrated in Figure 3B, the present invention use a false acknowledgement technique when communicating a lossy or unreliable protocol via a lossless or reliable protocol, such as, for example, communicating RTP over UDP via a TCP or SSL/TCP connection. In another technique illustrated in Figure 3C, the present invention uses payload shifting to communicate via a lossless protocol packets constructed for transmission via a lossy protocol. In some embodiments, these techniques of the present invention helps achieve Transport Layer Security (TLS) at a UDP level as one ordinarily skilled in the art will recognize and appreciate in view of the description below.

The illustrative method 360 of the embodiment of the present invention for practicing the false acknowledgement technique will be discussed in view of the illustrative environment 300 of Figure 3A and additionally in view of Figures 1A-1E. In brief overview, the environment 300 comprises a client 105a of computing device 102a in communications with a peer client 105b of computing device 102b or alternatively, the gateway 340 via network 104. In some embodiments, the client 105a may traverse IP routers 305a-305b or the network 104 may have IP routers 305a-305b. Although, in other embodiments, the computing devices 102a-102b and gateway 340 may be on the same network 104. Additionally, a telecommunication device 210a may be associated with client 105a and a second telecommunication device 210b may be associated with the peer client 105b or the gateway 340.

Client 105a may comprise a first network stack 310a, and the client 105 or gateway 340 may comprise a second network stack 310b. The network stacks 3201a-310a may comprise one or more network layers, such as any networks layers of Open Systems Interconnection (OSI) communications model. For example, as illustrated in

Figure 3A, the network stacks 310a-310b comprises a TCP/IP 343a-343 communication layer communication on top of the frame layer that is suitable as known to those skilled in art for a TCP/IP based network 104. The TCP layer 343a-343b comprises an illustrative embodiments of a reliable or lossless protocol. For example, in TCP 343a-343b as known to those ordinarily skilled in the art, the network stack 310a-310b or any drivers or mechanisms thereof, such as a TCP driver, may perform algorithms and operations, and comprise logic or functionality to provide one or more of the lossless or reliable characteristics of the protocol. For example, to support TCP 343a-343b, the network stack 310a-320b may perform packet ordering, packet retransmission, acknowledgements of receipt of packet, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm, and any other reliability related operations and algorithms as one ordinarily skilled in the art will recognize and appreciate in view of TCP 343a-343b or any other lossless protocol.

Additionally, the networks stacks 310a-310b may comprise an SSL 341a-341b layer for supporting SSL or SSL VPN communications. For example, the SSL layer 341a-341b may be used for a gateway or tunneling session between remote access clients 120 or between a remote access client 120 and a gateway 340. As illustrated in Figure 3A, the network stacks 310a-310b may also provides a layer for a lossy protocol 342a-342b, such as UDP, to be communicated over the lossless protocol 343a-343b, such as TCP. In some embodiments, the lossy or unreliable protocol 342a-342b may comprises Real Time Protocol (RTP) over UDP, and may comprise a payload have any type and/or form of real-time data, such any representation of voice or audio. In other embodiments, the lossy protocol 342a-342b may carry the VoIP over communications to and from the client 105a in an established VoIP session, such as a session established via illustrative method 260 discussed above in connection with Figures 2A and 2B. A lossless protocol, such as UDP 342a-342b may be chosen for real-time applications like voice, because it may be more important to get packets to the recipient, such as peer client 105b, on time rather than getting the packets in a reliable manner, such as via a lossless protocol.

The network stacks 310a-310b also include a shim 322a-322b of the remote access client 120 of the present invention. The shim 322a-322b may comprise any portion of the remote access client 120, and in some embodiments, comprises a network driver, network driver interface, or other network layer related mechanism for providing

the false acknowledgement technique of the present invention as described herein. The shim 322a-322b may comprise software, hardware, or any combination of software and hardware. In one embodiment, the shim 322a-322b may operate at the IP layer of the network stack prior to a network packet reaching the TCP layer 343a. In other embodiments, the shim 322a-322b may operate at the TCP layer 343a-343b. One ordinarily skilled in the art will recognize and appreciate that the shim 322a-322b may operate in any manner associated with the layer of operations of the lossless protocol in the network stack 310a-310b, including in or adjacent to the layer of the lossless protocol.

The false acknowledgement technique of the present invention as illustrated by method 360 of Figure 3B allows a lossy protocol, such as UDP 342a-343b, to be communicated via a lossless protocol, such as TCP 343a-343b. By the shim 322a-322b issuing a false acknowledgement of receipt of a TCP packet, the technique of the present inventions prevents or avoid the reliability mechanisms, operations and algorithms of the lossless protocol, such as in the example of TCP 343a-343b, any of the packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. As such, the lossy protocol 342a-342b can be communicated over a lossless protocol 343a-343b but maintain its lossy or unreliable characteristics which may be desired such as in real-time data communications. This technique also enables the lossy protocol to be communicated securely, or traverse a gateway via a tunneling protocol, or simply via TCP/IP while not applying the lossless characteristics of the lossless protocol to the lossy protocol communications.

In brief overview of illustrative method 360, at step 365, the computing devices 102a and 102b or the gateway 340 establish a lossless protocol based connection, such as a TCP connection, by which lossless protocol packets are communicated. At step 370, the remote access client 120 of the present invention may detect that the payload of a lossless protocol packet comprises a lossy protocol, such as RTP or UDP, or otherwise comprises real-time data. In one embodiment, at step 375, the illustrative method 360 may encrypt the payload with a key, such as a key provided via an out of band TLS or SSL session of step 367. At step 380, a false acknowledgement of receipt of the lossless protocol packet may be communicated or otherwise provided to the network stacks 310a-310b, such as by the shim 322a-322b. In response to the receipt of the false acknowledgement of receipt of the lossless protocol packet, at step 385, the respective

network stacks 310a-310b do not execute one or more, or all of the algorithms and operations that provide the reliable or lossless characteristics of the lossless protocol. At step 390, the lossless protocol packet with the lossy protocol payload is communicated between the network stacks 310a-310b.

At step 365 of illustrative method 360, the lossless protocol connection may be established via any suitable means and/or mechanisms using an type and/or form of lossless protocol. In one embodiment, the network stack 310a of a client 105a establishes a lossless protocol connection, such as TCP, to a peer client 105a having network stack 310b. In another embodiment, the network stack 310a of client 105a establishes a lossless protocol connection to a gateway 340 having network stack 310b. Additionally, the lossless protocol connection of step 365 may be established in a secured manner, such as SSL, or as a virtual private connection. Although the network stacks 310a-310b are illustrated as having the same network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks may have corresponding layers, which may be of different versions or associated with different operating systems and/or drivers, and that each network stack 310a-310b may have additional layers, less layers or different layers.

At illustrative step 360, in one embodiment, the remote access client 120 intercepts a network packet, such as via the packet capture mechanism 365, and inspects the network packet by any suitable means and/or mechanisms to determine the type of the protocol used in the payload of the network packet, or the type of contents in the payload of the network packet. In some embodiments, the shim 322a-322b of the remote access client 120 may be used for intercepting and inspecting the network packet. In one embodiment, the remote access client 120 may intercept a network packet and determine if the network packet comprises any lossless protocol or a specific lossless protocol, such as TCP. If the network packet is a lossless protocol, the remote access client 120 checks the payload to determine the type of protocol and/or the type of data. In one embodiment, the remote access client 120 may determine by any suitable fields of the payload of the network packet, such as any portion of header of the lossy protocol representing the payload, that the payload has a lossy protocol content. In another embodiment, the remote access client 120 may determine by any data of the payload, if the payload comprises a lossy protocol or comprises real-time data.

In one embodiment, the remote access client 120 determines that a TCP packet comprises a payload of RTP or UDP, and applies an encryption of the payload. The remote access client 120 may encrypt the payload of the network packet using any type and/or form of encryption with a key provided in any suitable manner. In some embodiments, the key or cipher is negotiated via an out of band TLS session between the clients 105a-105b or the client 105a and gateway as shown in Figure 3A as opposed to, in other embodiments, a traditional TLS session where the session is first negotiated and the same socket is used for data communication. In some embodiments, the encryption at step 375 is performed on a packet by packet basis. In another embodiment, encryption is performed on multiple packets at a time.

At step 380 of illustrative method 360 of the present invention, a false acknowledgment of receipt of the network packet, e.g., the lossless protocol packet, is issued, communicated, or otherwise provided to the network stacks 310a-310b comprising the respective sending and receiving computing devices 102a-120b, or gateway 340. The shim 322a-322b, any portion of the remote access client 120, or any portion of the network stack 310a-310b may issue the false acknowledgment of receipt of the network packet. In one aspect, the false acknowledgement of receipt of the network packet is false in the sense that it is communicated not to acknowledge the actual receipt of a network packet but in order to prevent the lossless and reliable mechanisms of the lossless protocol associated with the network stacks 310a-310b. As such, the false acknowledgement of receipt of the network packet may comprise the same form and/or type as an actual acknowledgement of receipt of the network packet.

In some embodiments, the false acknowledgement of receipt is issued to the network stacks 310a-310b prior to communicating the network packet or packets. In other embodiments, the false acknowledgement of receipt is issued after communicating the network packet(s) but at a time or in a manner such as to prevent the lossless protocol mechanisms of the receiving network stack 310a-310b from being applied to the transmitted network packet. In one embodiment, the false acknowledgment of receipt of the network packet is issued for each network packet, and in another embodiment, may be issued once per communication session or lossless protocol connection. Furthermore, one ordinarily skilled in the art will recognize and appreciate the false acknowledgement of receipt may be performed in different places in the network stack 310a-310b for different operating systems. For example, in one

embodiment, the acknowledgement of receipt may be issued at the Network Driver Interface Specification (NDIS) driver level in the Microsoft Family of Windows Operating Systems.

At step 385 of illustrative method 360, the network stack 310a-310b receiving the false acknowledgment of receipt of the network packet from step 380 may in response to such receipt, may not execute, stop executing, or prevent from executing any one or more algorithms and operations providing one or more lossless characteristics of the lossless protocol. For example, in the embodiment of TCP as the lossless protocol, the network stack 310a-310b may not execute any one or more of the following with respect to the network packet, or the TCP connection: packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. In some embodiments, the false acknowledgment of receipt must be received on a packet by packet basis to prevent the lossless layer of the network stack 310a-310b from employing reliability algorithms. As such, the sending network stack 310a-310b can determine on a packet by packet basis which packets to apply the false acknowledgment techniques of the present invention to. There may be some lossless protocol network packets comprising the lossy protocol for which the reliability algorithms of the lossless protocol should be applied. In other embodiments, the false acknowledgment of receipt of the network packet may be received once for the lossless protocol connection to prevent employing reliability algorithms for any subsequent packets received during the lossless protocol session or connection.

At step 390, the illustrative method 360 communicates the lossless protocol packet having the lossless protocol payload via the network stacks 310a-310b. In one embodiment, the lossless protocol packet is communicated after step 385, or in other embodiments, before step 385. So, although the lossless protocol packet becomes lost in the network, no attempt is made to reclaim the packet as one would expect for a lossy protocol packet.

Although the illustrative embodiment of method 360 is discussed using a false acknowledgment of receipt of the network packet such as in TCP, any type and/or form of indication, request, or instruction may be communicated to the network stacks 310a-310b to prevent employing any reliability or lossless algorithms of the lossless protocol. In some embodiments, the lossless protocol layer of the network stack 310a-310b may be adapted or configured to have a configuration, flag, or instruction to not use the

reliability algorithms either on a packet by packet basis, or a session or connection basis. For example, the lossless protocol may have fields, such in a header of a lossless protocol packet, that indicates whether reliability should be discarded or avoided for the packet.

Referring now to Figure 3C, another embodiment of steps taken to transmit packets constructed according to a lossy protocol via a lossless protocol is shown by illustrative method 345, which may also be referred to as a payload shifting technique. In brief overview of illustrative method 345, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device, such as client 105. At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. The first device 105 transmits the first TCP packet to the second device at step 352. At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, and at step 356, creates a second TCP packet including a second payload of the received second packet and the first TCP header information. At step 358, the first device transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

Still referring to Figure 3C, and now in more detail, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device 105. In some embodiments, the packet is intended to be transmitted using a lossy protocol of UDP. In further embodiments, the packet comprises RDP over UDP. In other embodiments, the first packet is generated by an application program 338 executing in user mode 332. In some embodiments, the packet is generated by an application 338 executing in kernel mode 334. In other embodiments, the first packet is received by the first device 105 for retransmission. In still other embodiments, the first packet is intercepted by a filter process 322 before it reaches the network stack 310a-310b. The filter process 322 may execute in user mode 332 or in kernel mode 334. In some embodiments, the filter 322 is a mini-driver. In other embodiments, the filter 322 is an NDIS driver. In other embodiments, the filter 322 process uses application hooking to intercept the first packet. In further embodiments, the application hooking is implemented via an application programming interface (API). In one embodiment, the hooking of network packets occurs at the network layer of the network stack 310a-310n.

At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. For example, the TCP connection may be established between the client 105 and a peer computing device 102b in one embodiment, and between the client 105 and the gateway 340 in another embodiment. In some embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by opening a specific TCP port. In other embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by setting a flag in the TCP header. The TCP header may include information regarding the source node, information regarding the destination node, or a sequence number particularly identifying the TCP packet.

At step 352, the first device 105 transmits the first TCP packet to the second device. In some embodiments, the second device may be a gateway 340. In other embodiments, the second device is a "peer" computing device 102b. The first TCP packet may be encrypted before transmission to the second device using, for example, SSL or TLS.

At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, such as UDP. The second packet may be received from the same application 338 that generated the first packet. At step 356, the first device 105 creates a second TCP packet including a second payload of the received second packet and the first TCP header information, as described above. At step 358, the first device 105 then transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device. In some embodiments, when an acknowledgment is received from the second device, the first device 105 updates the TCP header information before transmitting the packet. In other embodiments, the first device 105 creates a third TCP packet with updated TCP header information and having the second payload. The first device then transmits the third TCP packet.

Upon receipt of the TCP packet, the second device decrypts it, if necessary, and determines that the payload is one or more packets constructed to be transmitted using a lossy protocol. The second device may determine this based on the port on which the

packet was received or by a flag in the TCP header information. Once determined, the second device strips the TCP header from the payload and delivers the payload.

In another aspect, the present invention is related to adjusting the reported maximum transmission unit (MTU) parameter to optimize network communications by reducing packet fragmentation for encrypted network packets. This technique may be applied on one or both network stacks 310a-310b of illustrative environment 300 of Figure 3A. Encrypting a payload of a network packet, such as any network packet processed according to the illustrative method 360 described above, may increase the size of the payload. That is, the size of the network packet may increase to account for the change in size of the unencrypted original payload to the encrypted payload.

Still referring to Figure 3A, the network stacks 310a-310b may comprise a maximum transmission unit 402a-402b (MTU) parameter to indicate the size of the largest unit of data that can be sent over a type of physical medium in a network, such as an Ethernet based network. In the embodiment of TCP/IP, the MTU 402a-402b indicates the largest datagram or packet than can be transmitted by an Internet Protocol (IP) layer interface, without the interface needing to br4eak down or fragment the datagram into smaller units. An MTU parameter 402a-402b may be associated with a communications interface such as a network interface card. The default MTU size for Ethernet is 1,500 bytes, and IEEE 802.3 is 1,492 bytes. As one ordinarily skilled in the art will recognize and appreciate, the default MTU size will be based on the networking technologies such as Token Ring, FDDI, X.25, etc.

Referring now to Figure 4, a flow diagram depicts an illustrative embodiment of the MTU adjustment method 400 of the present invention. In brief overview, at step 405, a session between computing devices is established, such as between a first computing device 102a and a second computing device 102b. At step 410, one of the computing devices 102, such as the first computing device 102a, detects a network packet having an encrypted payload. At step 415, the computing device 102a-120b determines a setting for the MTU 402a-402b parameter of the network stack 310a-310b to account for the size of the encrypted portion of the payload. At step 420, the MTU 402a-402b parameter is decreased to account for the encrypted portion. If the MTU 402a-402b is requested or reported, the MTU 402a-402b will indicate a size smaller than the MTU size associated with the physical layer, such as 1,500 for Ethernet.

Using this technique, any device on the network 104 may communicate network packets to the network stack 310a-310b according to the decreased MTU size that can be encrypted along the route to the network stack 310a-310b and not be fragmented. If the network packet is encrypted it should still fit in the actual MTU size of the physical network layer medium, such as Ethernet. For example, the MTU parameter 402a-402b may be set to the default MTU size of 1,500 for Ethernet and in accordance with the illustrative method 400 decreased by a determined number of bytes, for example 100, to account for encryption overhead. A network packet may be transmitted from a server resource to the client comprising a size equal to the reported MTU 402a-402b size of 1,400. The network packet may traverse the gateway 340 and get encrypted via the SSL tunnel, which in turns increases the network packet size to 1,475. Since this size fits into the MTU size of the Ethernet physical medium, the network packet will not be fragmented.

At step 405 of illustrative method 400, any type and/or form of communication session between a first computing device 102a and a second computing device 102b, such as client 105b or gateway 340 of Figure 2A, may be established. In some embodiments, the session is established using the remote access client 120 on a first computing device. In one embodiment, the remote access client 120 establishes a session with the gateway 340, such as an SSL VPN session, or to another remote access client 120 on a peer computing device 102b.

In some embodiments of step 410, the remote access client 120 detects a network packet having an encrypted payload. In one embodiment, the packet capture mechanism 365 intercepts network packets and the agent 326 determines if the packet is encrypted. However, any other portion of the remote access client 120, such as the filter 322 or frame monitor 360 may determine if the packet is encrypted. In one embodiment, the entire payload of the network packet is encrypted, while in other embodiments, a portion of the payload is encrypted. The present invention may use any type and/or form of means or mechanism for determining if a packet has encryption. For example, in some cases, the remote access client 120 may check for a flag or field of the network packet indicating the payload is encrypted. In other embodiments, the remote access client 120 may check whether any portion of the payload is unintelligible, because it contains random data or noise from encryption. Additionally, the encrypted payload may be

encrypted in association with any layer of the network stack 310a-310b, such as layer 2, 3, 6 or 7 encryption.

In some embodiments of step 415, the illustrative method 400 of the present invention determines the adjustment to the reported MTU 402a-402b size on a packet by packet basis, or in other embodiments, on a connection or session basis, and at step 420 adjusts the MTU 402a-402b accordingly. In one embodiment, the MTU 402a-402b is decreased exactly by the amount of encryption overhead for the network packet. In some cases, the illustrative method 400 determines the MTU 402a-402b size adjustment once for the entire session or connection and decreases the size of the MTU 402a-402b to a value to account for encryption overhead for the entire session. For example, although network packets may have varying encryption overhead, the adjustment accounts for the largest encryption overhead. In further embodiments, the MTU 402a-402b may be adjusted to take into consideration encryption that may occur when the network packet leaves the network stack 310a-310b, such as encryption by a gateway 340 that may occur in the end-to-end network traversal of the network packet .

Additionally, the MTU 402a-402b size may be adjusted for other network performance factors in addition to the encryption overhead. In some embodiments, although the MTU 402a-402b is decreased due to encryption overhead, it may be further decreased to account for other overhead and factors related to network communication, as well as increased in other cases. For example, the MTU 402a-402b may have been previously adjusted for a factor not related to encryption and after using the techniques of the present invention the MTU 402a-402b is decreased to take into account encryption overhead. One ordinarily skilled in the art will recognize and appreciate that there may be other factors and considerations for adjusting the MTU besides or in addition to adjusting for encryption overhead in accordance with the techniques of the present invention.

Referring now to Figures 5A and 5B, the present invention, in an additional aspect, is related to client-side application-aware network communication prioritization techniques. The remote access client 120 of the present invention provides for the intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application. As depicted in the system 500 of Figure 5A, the remote access client 105 of computing device 102 is connected to network 104. The client 105 may execute one or more applications 338a-338n, which

access the network 104 via the agent 326 and filter 322 of the remote access client 120. In some embodiments, the applications 338a-338n provide one or more real-time data communications, such as VoIP. In other embodiments, one or more of the applications 338a-338 may provide email, collaboration, online meeting, and/or desktop sharing related services or functionality.

As illustrated in Figure 5A, the packet capture mechanism 365, 365' may be included in the filter 322 or the agent 326 of the remote access client 120, for intercepting network traffic of any of the applications 338a-338n of the client 105. The remote access client 120 may comprise any queues 540a-540n for queuing and prioritizing network communications of the client 105. In one embodiment, the queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322, and in other embodiments, may be included with or accessible by the agent 326. The queues 540a-540n may comprise any type and/or form of suitable means and/or mechanisms for storing and/or arranging network packets, such as network packets intercepted by the packet capture mechanism 365. In some embodiments, the queues 540a-540n may be associated with or assigned to network packets related to applications 338a-338n of the client 105. In other embodiments, the queues 540a-540n may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1...10. One ordinarily skilled in the art will recognize and appreciate that number of queues 540a-540n may be based on any desired granularity of prioritization, such as 3, 5 or 10 levels of priority. Additionally, some of the queues 540a-540n may be used for receiving and/or transmitting network packets prior to being placed into and/or taken out of a priority based queue 540a-540n.

The remote access client 120 may also have, access, or use a routing table 538 for determining how to route network packets of the client via the agent 326, such as onto the network 104 via a gateway 340. In one embodiment, the agent 326 establishes and maintains an SSL VPN connection to the gateway 340, such as illustrated in Figure 1A for example. In one embodiment, the routing table 538 comprise information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points. The routing table 538 may include a source IP address and source port, and an destination IP address and destination port to identify a communication path on the network 104. For example, the source IP address and source port may represent the IP

address of the client 105 and the port by which an application 338a-338n on the client 105 communicates on the network 105. The destination IP address may represent the IP address of a peer computing device to which the application 338a-338n communicates with via the destination port used by the peer device.

Additionally, the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application. These policies 520 may be specified by any suitable means and/or mechanisms. In some embodiments, the policies 520 may be specified by the name of the application 338a-338n and/or the type of application 338a-338n. In other embodiments, the policies 520 may be specified in accordance to the type of one or more protocols used by the applications 338a-338n and/or the size of the payload of the network packet. In another embodiment, the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105. In yet another embodiment, policies 520 may indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number. Additionally, the policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point. Furthermore, the policies 520 may be specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority. One ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.

The policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326. For example, the policies 520 may be provided by or downloaded via the gateway 340. The policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file. The policies 520 may be configurable by a user by any suitable means and/or mechanism. For example, the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.

In view of the system 500 of Figure 5A and Figures 1A-1C, the prioritization technique of the present invention illustrated by method 550 in Figure 5B will be described. In brief overview, at step 555 of the illustrative method 550, the client 105

intercepts one or more networks packets associated with an application 338a-338n on the client 105, and, at step 560, the network packets are stored to a queue 540a-540n. At step 565, a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application 338a-338n. At step 570, the determined priority is indicated for the network packets, and, at step 575, the network packets are communicated according to the determined priority. As such, the outbound network packets generated by an application 338a-338n on the client 105 are prioritized by the client 105 prior to transmission based on the type and/or priority of the application 338a-338n. For example, the application 338a may generate real-time data of VoIP communications, such as RTP over UDP via a TCP/IP session of an SSL connection to the gateway 340. The client 105, using the techniques of the present invention, may prioritize the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications. This technique may compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.

At step 555 of illustrative method 500, the client 105 may intercept network packets of one or more applications 338a-338n transparently to the application 338a-338n, the gateway 340, a peer computing device, and any of the network layers of a network stack. In this manner, the techniques of the present invention support any type of application 338a-338n on the client 105. In some embodiments, the network packets are intercepted by the packet capture mechanism 360 via agent 326 or filter 322. Any inbound and/or outbound network packets of an application 338a-338n may be intercepted by the remote access client 120 of the present invention.

At step 560, the network packets intercepted at step 555 may be stored in a queue 540a-540n. In one embodiment, the network packet is stored to a temporary queue 540a-540n prior to prioritizing the network packet at steps 565 and 570. In other embodiments, the network packet is stored to a determined priority queue 540a-540n or a queue 540a-540n associated with an application 338a-338n after the network packet is prioritized at steps 565 and/or step 570.

At step 565, the remote access client 120 of the present determines the association of network packets with applications 338a-338n in order to determine priorities and apply any priority based policies 520. The client 105, such as via agent 326, can associate network traffic with applications 338a-338n by any suitable means

and/or mechanisms. In some embodiments, the agent 326 identifies the network packet as generated from an application 338a-338n by any of the content of the network packet, such as any headers, fields, or the type and content of data in the payload of the network packet. In other embodiments, a network packet is associated with an application 338a-338n by matching information from the routing table 538, such as source and destination IP addresses and ports numbers with the IP addresses and ports numbers of the network packet. In some embodiments, the agent 326, such as via the frame monitor 360, may perform a checksum on the packet to verify that the identified application actually generated the packet.

Additionally, the remote access client 120 may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105. Furthermore, the remote access client 120 may determine any priorities, such as process task priority, assigned to the application 338a-338n by the operating system of the client 105. In other embodiments, the remote access client 120 may determine any other characteristics or statistics of the application 338a-338n such as size, memory usage, total execution time, and/or frequency of use. One ordinarily skilled in the art will recognize and appreciate the various characteristics of an application the present technique may use for providing client-side application-aware network communication prioritization.

At step 570, the remote access client 120 of the present invention indicates a priority for intercepted and queued network packets based on the application 338a-338n associated with the packet at step 565. In one embodiment, the agent 326 uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520. In some embodiments, the agent 326 may use characteristics of the application 338a-338n, such as running in the foreground or background, to indicate priority for a network packet of the application 338a-338n. In other embodiments, the agent 326 may use any combination of the policies 520 and characteristics of the application 338a-338n to indicate a priority for the network packets of the application 338a-338n.

In some embodiments, the agent 326 indicates the priority to the filter 322 for management of network packet queues 540a-540n to apply the indicated priorities. The agent 326 may communicate the priority of network packets to the filter 322 by any suitable means and/or mechanism such as via an application programming interface

(API), such an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art. In one embodiment, the filter 322 is not aware of the application 338a-338n by name but can associate priorities to network packets of applications 338a-338n via the routing table 538. An application 338a-338n corresponding to a network packet can be identified by any combination of source and destination identifiers, such as IP addresses and port numbers. As such, in some embodiments, the agent 326 indicates priorities to the filter 322 by routing information instead of application name. In other embodiments, the agent 326 provides to the filter 322 a mapping between applications 338a-338n, such as by application name or process id, to the routing information in a routing table 538.

Based on the indicated priorities for applications 338a-338n, in some embodiments, the filter 322 may place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities. In one embodiment, the filter 322 may move network packets from temporary queues 540a-540n or from memory or other storage to a queue 540a-540n associated with the application 338a-338n, a queue 540a-540n associated with a priority, or a queue 540a-540n associated with both an application and a priority. For example, in one embodiment, all high priority network traffic may be placed in a high priority queue 540a and arranged in order based on an order of priority of the application 338a-338n, such as real-time data applications 338a-338n prior to other applications 338a-338n. In some embodiments, the network packets may be arranged in order in a priority queue 540a-540n based on the time the network packet was intercepted by the packet capture mechanism 365, such as in a FIFO manner. In yet a further embodiment, one queue 540a-540n may be used for prioritization by the filter 322. Each network packet may be placed and arranged in a priority order respective to all other intercepted network packets to provide a packet by packet prioritization across all applications 338a-338n and intercepted network packets. One ordinarily skilled in the art will recognize and appreciate that the network packets may be arranged in various priority queues 540a-540n, such as high, medium, low, or by any other granularity, and be placed or arranged in the queue in any suitable manner in practicing the operations of the present invention described herein.

In one embodiment, all network packets for an application 338a-338n are placed in a queue 540a-540n associated with the application 540a-540n. For example, intercepted network packets for an application communicating to a first destination IP

address, and a first destination port may be placed in a first queue 540a. In another embodiment, all networks packets for a type of application 338a-338n, such as an email or voice application, or all network packets for a type of protocol used by the application 338a-338n, such as RTP or UDP, may be placed in a queue 540a-540n for prioritizing networks packets for one or more applications. For example, online collaboration related applications 338a-338n may be placed and prioritized in a first queue 540a for collaboration related applications. A second queue 540b may be used for email related applications 338a-338n. In another example, a queue 540a may be used for applications 338a-338n communicating real-time data or communicating using the RTP and/or UDP protocol. In a further example, a queue 540a may be used for applications 38a-338n communicating using a remote display protocol, such as ICA or RDP.

Within each application associated queue 540a-540n organized by specific application 338a-338n, type or category of application 338a-338n, or by protocol, the network packets may be further prioritized by the characteristic of the application 338a-338n generating them, e.g., a foreground application, the size of the network packet, or the time the network packet was intercepted. In some embodiments, one or more queues 540a-540n may be used for network packets intercepted but not prioritized because a policy 520 does not exist or apply to the network packet, or the policies 520 indicate to ignore or not process the network packet for prioritization. One ordinarily skilled in the art will recognize and appreciate the various ways network packets may be placed and arranged in a priority based manner in queues 540a-540n associated with the application 338a-338n, the type of application 338a-338n or the protocol used by the application 338a-338n, and that the priority may be based on the policies 520 specified for the client 105.

At step 575 of illustrative method 550, the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets. In some embodiments, the network packets are organized into priority queues 540a-540b so that the network packets of the highest priority queue 540a-540n are communicated first, and then the next highest priority queue 540a-540n second, and so on. In other embodiments, the queues 540a-540n are organized by application 338a-338n, and therefore, at step 575, the present invention communicates network packets from the queue 540a-540n based on the respective priorities of the applications 338a-338n. Regardless of the queue 540a-540n organization and management, one ordinarily

skilled in the art will recognize and appreciate that the remote access client of the present invention will communicate the network packets from the queues in a manner according to or consistent with the determined priorities, which in turn, may be based or derived from the policies 520 of the client.

In some embodiments, the remote access client 120 of the present invention considers other network factors in determining what network packets to communicate from what queue. For example, the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n. In another example, the remote access client 120 may recognize a high number of retransmits to a particular destination. As such, in some embodiments, the remote access client 120 may throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue 540a-540n. Thus, the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338a-338n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network.

In yet a further aspect and referring now to Figures 6A and 6B, the present invention is related to providing a network disruption shielding technique for persistent and reliable connectivity. Figure 6A illustrates environment 300 as discussed above in conjunction with Figure 3A. The environment 300 illustrates network stacks 310a and 310b, which may represent network stacks of computing devices 102a-120b or gateway 340, such as any of the computing devices 102 and the gateway 340 illustrated in Figures 1A-1C, 2A, or 5A. Each network stack 310a-310b may comprise one or more networks layers, such as a TCP/IP network layer on top of the frame network layer as one ordinarily skilled in the art will recognize and appreciate. Although the network stacks 310a-310b are illustrated in environment 300 of Figure 6A with a certain set of network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks 310a-310b may have any type and/or form of network layers, in any suitable combination, and each of the network stacks 310a-310b may have different forms of each layer in relation to the other network stack.

The network stacks 310a-310b may be considered to have a first portion 605a-605b of the network stack, and a second portion 610a-610b of the network stack. As

illustrated in the example network stacks 310a-310b of Figure 6A, the first portion 605a-605b of the network stack comprises the network layers at and below the TCP network layer. The second portion 610a-610b may comprise those network layers above the TCP network layer, such as a UDP over SSL protocol layer. Although the first portion 605a-605b and the second portion 610a-610b are shown as portioned, segmented, or otherwise divided at the TCP layer, the first portion and second portion may be formed at a higher or lower dividing layer in practicing the network disruption shielding technique of the present invention as one ordinarily skilled in the art will recognize and appreciate.

The network stacks 310a-310b illustrated in Figure 6A may represent an application 338a-338n on client 105, such as the client depicted in Figure 5A, establishing a peer-to-peer SSL VPN connection to a second computing device 102b or, alternatively, a gateway 340. The client 105 may be a mobile client, such as a notebook, personal digital assistant (PDA), a smart phone, or any type of mobile computing or telecommunication device. The client 105 may communicate real-time data such as VoIP communication via the UDP protocol or RTP over UDP via the SSL session established to the peer device 102b or gateway 340. In one embodiment, the agent 326 of the remote access client 120 establishes and maintains the SSL or SSL VPN session to the gateway 340 or to peer computing device 102b. The agent 326 may operate in user-mode 332, and may handle any network layer and protocol processing related to the second portion 610a-610b of the network stack 310a-310b, along with any application layer protocols. As a TCP/IP based network 104, the UDP over SSL session of the second portion 610a-610b of the network stack 310a-310b may be communicated over a TCP/IP stack forming the first portion 605a-605b of the network stack 310a-310b. In view of the remote access client 120 of the present invention, such as illustrated in Figure 1A or 5A, the filter 322 may be a network driver operating in kernel-mode 332 within the first portion 605a-605b of the network stack 310a-310b.

The present invention uses a network disruption shielding technique as depicted by illustrative method 650 in Figure 6B to maintain the second portion 610a-610b of the network stack 310a-310b through a network level connection interruption, such as any type and/or form of network disruption to the first portion 605a-605b of the network stack 310a-310b. The network disruption shielding technique of the present invention may be performed transparently to an application 338a-338n of the client 105, a user of the client 105, any one or more network layers above the first portion

605a-605b, and the gateway 340 or peer computing device 102b, and any portion of their respective network stacks 310a-310b. In one embodiment, the network disruption is shielded without notification to the user of the client that the network was disrupted or a session was interrupted.

In brief overview of illustrative method 650, at step 665, a client 105 establishes a session via at least a first protocol over a network connection between the client and another device, such as a peer computing device or gateway. As such, a network stack 310a-310b is established or used on the client 105. The network stack 310a-310b has a first portion 605a-605b and a second portion 610a-610b. At step 660, a disruption in the network connection is detected causing the first portion 605a-605b of the network stack 310a-310b to be disestablished, or otherwise disrupted from being used or continued to be used. At step 665, the present invention maintains the second portion 610a-610b of the network stack 310a-310b during the disruption and maintaining a session, or sessions, associated with the network layers of the second portion 610a-610b.

During the disruption, at step 670, any network packets related to the second portion 610a-610b of the network stack 310a-310b may be queued. At step 675, the first portion 605a-605b of the network stack 310a-301b is reestablished or otherwise received from the network disruption. While the first portion 605a-605b of the network stack 310a-301b is reestablished, the present invention maintains the second portion 610a-610b, and sessions thereof, allowing at step 680, to continue with the session by linking or re-associating the second portion 610a-610b with the first portion 605a-605b of the network stack 310a-310b. The network connection and/or the session may automatically be re-authenticated at step 680. At step 685, the illustrative method may communicate any queued network packets and continue with the session transparently as if the network disruption did not occur.

In an embodiment of illustrative step 655, a first computing device 102a may establish a network connection with a second device, such as a peer computing device 102b or a gateway 340, by any suitable means and/or mechanism and using any type and/or form of connection based protocol. For example, the network connection may be established via a TCP connection on a TCP/IP network or by an SPX connection on an IPX/SPX network. In some embodiments, the network connection may be initiated by any of the applications 338a-338n on the client, such as any application illustrated in

Figure 5A. For example, a remote display client, such as an ICA client of Citrix Systems, Inc. or a Remote Display Client of Microsoft Corporation may initiate or establish the network connection. In other embodiments, the network connection of illustrative step 665 may be initiated and/or established via the agent 326, filter 322, or any other portion of the remote access client 120. In one embodiment, the establishing of the network connection forms the first portion 605a-605b of the network stack 310a-310b. In other embodiments, the first portion 605a-605b of the network stack 310a-310b, or portion thereof, is established via connection to a network 104 upon startup of the client 105.

In some embodiments, the second portion 610a-610b of the network stack 310a-310b is formed by establishing one more sessions, such as an SSL session, via any type and/or form of protocol over the network connection, such as a remote display protocol of ICA or RDP. The session may be established via any application 338a-338n or the remote access client 120 of the client. In one embodiment, the session may correspond to a tunneling or gateway session with a peer computing device 102b or a gateway 340. In another embodiment, the session may be any type of interactive session such as a media session established via a signaling protocol, SIP for example. For example, the session of the second portion 610a-610b of the network stack 310a-310b may comprise a VoIP communication session, such as one established by illustrative method 260 of Figure 2B. Additionally, there may be multiple sessions associated with the second portion 610a-610b of the network stack 310a-310b. For example, an SSL or SSL VPN session may form one session, while a second session, such as media session via RTP over UDP may form a second session. Additionally, at any application layer of the network stack 310a-310b one or more applications 338a-338n on the client 105 may establish an application level session with a peer computing device 102b. In one embodiment, the agent 326 of the remote access client 120 is responsible for establishing and maintaining the second portion 610a-610b of the network stack 310a-310b and one or more of the associated sessions.

At step 660 of the illustrative method 650 of the present invention, a disruption is network connection is detected. In one embodiment, the network disruption may be caused by a mobile client 105 roaming between networks and networks segments, which, in some embodiments, causes the client 105 to obtain a new network IP address and/or host name. In some embodiments, the disruption disrupts the first portion 605a-

605b of the network stack 310a-310b, such as, for example, causing a TCP or SPX connection to be disconnected. In one aspect, the disruption causes the first portion 605a-605b, or any portion thereof, of the network stack 310a-310b to be disestablished, or otherwise needing to be re-established, reconnected, reconfigured or rebuilt. For example, in some embodiments, the IP layer of the network stack may maintain intact while the TCP layer is reestablished. In one embodiment, any TCP related drivers may need to be re-started. In other embodiments, the TCP/IP layer be intact even though the network connection is disrupted, and only a new TCP connection needs to be established. In other embodiments, the TCP/IP layer is intact but needs to reconfigure itself for a new network or network segment, such as changing the IP address of the client 105. One ordinarily skilled in the art will recognize and appreciate the various ways a network connection may be disrupted and impact or affect a first portion of the network stack.

In some embodiments, the agent 326, or any other portion of the remote access client 120 may detect the network disruption by any suitable means and/or mechanisms. In one embodiment, the agent 326 may determine a network disruption by receiving an error message or failure upon calling or executing an API call to the first portion 605a-605b of the network stack 310a-310b. For example, the SSL session maintained by the agent 326 for the second portion 610a-610b relies or depends on the TCP connection of the first portion 605a-605b of the network stack 310a-310b. As the agent 326 transacts via the SSL session, the agent 326 may receive an error or failure message indicating a problem with the TCP connection. In other embodiments, the agent 326 may receive an event or message from any network layer of the first portion 605a-605b of the network stack 310a-310b indicating a network disruption. One ordinarily skilled in the art will recognize and appreciate the various ways the network disruption may be detected.

At illustrative step 665, in some embodiments, upon detection of the network disruption, the agent 326 or any other portion of the remote access client 120 of the present invention maintains the second portion 610a-601b of the network stack 310a-310b during the disruption. For example, although the SSL based session maintained by the agent 326 depends on an underlying TCP connection, the agent 326 keeps the SSL session open or active through the disruption to the TCP connection. As there may multiple sessions associated with one or more layers of the second portion 610a-610b of the network stack, the agent 326, in some embodiments, keeps one or more, or all, of the

multiple sessions open or active although the first portion 605a-605b of the network stack 310a-310b is disrupted.

At step 670 of illustrative method 650, the remote access client 120 of the present invention, in some embodiments, queues one or more network packets of any of the protocols related to the second portion 610a-610b of the network stack 310a-310b during the network disruption. The remote access client 120 may use any type and/or form of queuing mechanisms, such as any of the queues 540a-540n illustrated in Figure 5A. In other embodiments, the remote access client 120 may discard network packets during the disruption, such any packets related to a lossy protocol, such as RTP over UDP for voice communications. In some cases, it may be desirable to discard packets, such as UDP packets, to reduce latency and quality issues, such as in voice communications. In further embodiments, the remote access client 120 may queue some network packets and discard other network packets. In an additional embodiment, the remote access client 120 may queue the network packets, and discard some or all of the network packets after a predetermined period of time. The remote access client 120 may use the policies 520 to determine which network packets to queue and/or discard. For example, a network packet of a first application 338a may be queued while a network packet of a second application 338n is discarded. In other embodiments, the remote access client 120 may use any network statistics or any network traffic inspection techniques, for example stateful inspection, as known to those skilled in the art to determine whether to queue and/or discard network packets during the disruption.

At step 675 of illustrative method 650, the first portion 605a-605b of the network stack 310a-310b is reestablished while the second portion 610a-610b of the network stack 310a-310b is maintained along with maintaining any desired session or sessions of the second portion 610a-610b of the network stack 310a-310b. The first portion 605a-605b of the network stack 310a-310b may be reestablished by any suitable means and/or mechanisms. For example, the client 105 may reestablish the TCP/IP connection to the network 104, such as by logging into a new network for a roaming mobile client 105. In other embodiments, the remote access client 120, such as via the agent 326 or the filter 322, reestablishes the first portion 605a-605b of the network stack 310a-310b. For example, the agent 326 may initiate and establish a new TCP connection. Upon reestablishing the first portion 605a-605b, the second portion 610a-610b of the network stack 310a-310b is linked with, re-associated with or starts to use or continue to use the

first portion 605a-605b to reestablish the network stack 310a-310b. In some embodiments, the agent 326 may be notified by an event of any network layer that the first portion 605a-605b has been reestablished or in other embodiments, may poll by any predetermined frequency to determine the first portion 605a-605b is reestablished. For example, the agent 326 may check if the TCP connection is active or can be reconnected.

In some embodiments, at step 680, the remote access client 120, such as the agent 326, may automatically re-authenticate the client 105 or a user of the client 105 for the network connection, such as a TCP connection for the first portion 605a-605b of the network stack 610a-610b. For example, the remote access client 120 may automatically re-authenticate the client 105 to a network 104 using any network related credentials of a user of the client 105. Additionally, the remote access client 120 may automatically re-authenticate the client 105 or a user of the client 105 for any session associated with the second portion 610a-610b of the network stack 310a-310b. For example, the SSL session between the agent 326 and the gateway 340 or peer computing device 102c may be re-authenticated.

In another example, an application 338a may be accessing a host service, web server, or application server that uses authentication credentials for access. The agent 326 may automatically re-authenticate the application 338a to the corresponding service or server using application related authentication credentials. In some embodiments, the remote access client 120 may re-authenticate the client and/or user of the client 105 at multiple levels, such as for network access and/or TCP connection, SSL or SSL VPN session, and/or any application level sessions, such as a media interactive user session, for example, a VoIP telephone session. Furthermore, the remote access client 120 may re-authenticate at any time prior to step 685, during step 685, for example, after communicating queued network packets but before continuing other communications, or after step 865, in response to a request to authenticate from a peer computing device, such as a server or the gateway 340.

At step 685 of illustrative method 650, the remote access client 120 of the present invention continues to use the session or sessions of the second portion 610a-610b of the network stack. If any network packets have been queued or remain queued at step 670, the remote access client 120 communicates the queued network packets and continues communicating any network packets of the client 105, such as network

packets generated by or sent to the one more applications 338a-338n of the client 105. As such, the network disruption shielding technique of the present invention provides a seamless and transparent solution to nomadic mobile computing solutions and for generally providing reliable and persistent network connectivity and access.

In the example of a VoIP communications, the illustrative method 650 of the present invention will reduce the number of telephone call drops due to network disruptions and improve the usage of and experience with VoIP. A VoIP user will not need to reconnect the telephone call due to temporary network disruptions in network availability as the remote access client 120 of the present invention will automatically maintain the session and reconnect to the network. Additionally, the remote access client 120 of the present invention will automatically re-authenticate the connection and sessions for providing security after the network disruption. Furthermore, the network shielding technique of the present invention is useful for 1) continuing transactions, commands, or operations automatically through the network disruption, 2) maintaining session related context and cache through the network disruption, and 3) automatically handling change in network address of the client due to changes in the network.

By providing a reliable and persistent connection, the present invention also avoids interruptions to transactions, commands or operations as part of the functionality exercised between the a first computing device 102a and a second computing device 102b, such as client 105a and 105b in Figures 1C. For example, a file copy operation using Windows Explorer has not been designed to continue working after there is a disruption in a network connection. A user on the client 105 may use the file copy feature of Windows Explorer to copy a file from the client 105 to a server 102c. Because of the size of the file or files, this operation may take a relatively extended period of time to complete. If during the middle of the operation of the copy of the file to the server, there is an interruption in the network connection between the client 105 and the server, the file copy will fail. Once the network connection is re-established, the user will need to start another file copy operation from Windows Explorer to copy the file from the client 105 to the server. Under the present invention, the user would not need to start another file copy operation. The network connection would be re-established in accordance with the network disruption shielding technique of the present invention as illustrated in Figure 6B. As such, the file copy of Windows Explorer would not get notified of the interruption in the network connection and therefore, would not

fail. The remote access client 120 would re-establish any connections and transmits any queued data so that operation can continue without failure. The remote access client 120 would maintain a queue of the data related to the file copy operations that has not been transferred to the server because of the interruption in the network connection. Once the network connection is re-established, the remote access client 120 can transmit the queued data and then continue on with transferring the data related to the file copy operation in due course.

Although this aspect of the invention is described in terms of a file copy operation example, one ordinarily skilled in the art will recognize that any operation, transaction, command, function call, etc. transacted between a first computing device 102a and a second computing device 102b, can be maintained and continued without failure from the network connection disruption, and, furthermore, without the client 105 or user of the client 105 recognizing there was a disruption or having notice of the disruption. Additionally, the transaction or operation can be maintained and continued transparently to the application 338, the gateway 340, second computing device 102c, and any part of the second portion 610a-610b of the network stack 310a-310b.

By providing the client 105 with a reliable and persistent connection to a peer computing device 102b or gateway 340, the present invention avoids the process of opening a new user session with an application 338 on the peer, such as a host service on server, by maintaining the user session through network connection interruptions. For each user session between peer computing device, each computing device may maintain session specific context and caches, and other application specific mechanisms related to that instance of the user session. For each new user session established, these session specific context and caches need to be re-populated or re-established to reflect the new user session. For example, a user on the client 105 may have an http session with a server 102c having a web server or web application. The server 102c may keep context specific to providing this instance of the http session with the client 105. The context may be stored in the memory of the server, in files of the server, a database or other component related to providing the functionality of the server 102c. Also, the client 105 may have local context specific to the instance of the http session, such as a mechanism for keeping track of an outstanding request to the web server. This context may be stored in memory of the client 105, in files on the client 105, or other software component interfaced with the client 105. If the connection between the client 105 and

the server 102c is not persistent, then a new user session needs to be established with new session specific context on the server 102c and the client 105. The present invention maintains the session so that a new session, and therefore new specific session context, does not need to be re-established.

The present invention maintains the user session through network level connection interruptions and without notification to the user of the client that the session was interrupted. In operation of this aspect of the invention, the client 105 establishes the connection to the peer computing devices. Via the connection, a session between the client 105 and the server is established. The remote access client 120 can store and maintain any session related information such as authentication credentials, and client 105 and host server 102c context for the established session. Upon detection of a disruption in network connection, the remote access client 120 can re-establish the first portion 605a-605b of the network stack 310a-301b while maintaining the second portion 610a-610b of the network stack. The network connection disruption may cause an interruption to the underlying TCP/IP connection used by the session between the client 105 and the server 102c. However, since the second portion 610a-610b of the network stack 310a-310b is maintained, the session can be re-established and/or continued after the network connection is re-established without the user on the client 105 having notification that the session was interrupted. Thus, the interruption of the session caused by the network connection disruption is effectively hidden from the user using the network disruption shielding techniques of the present invention.

Furthermore, by providing a reliable and persistent connection, the present invention also enables a client 105 to traverse through different network topologies without re-starting a session or an application 338 on the client 105. For example, the client 105 may be a computer notebook with a wireless network connection. As the client 105 moves from a first wireless network to a second wireless network, the client's network connection may be temporarily disrupted from the first wireless network as a network connection is established with the second wireless network. The second wireless network may assign a new network identifier, such as a host name or internet protocol address, to the client 105. This new network identifier may be different than the network identifier assigned to the client 105 by the first wireless network. In another example, the client 105 may be physically connected through an Ethernet cable to a port on the network. The physical connection may be unplugged and the client 105 moved to

another location to plug into a different port on the network. This would cause a disruption into the network connection and possibly a change in the assigned network identifier. Without the present invention, any sessions between peer computing devices may need to be restarted due to the change in the network topology, the disruption to the network connection, and/or the change in the assigned network identifier. By the method and systems described herein, the remote access client 120 of the present invention maintains the network connection for the client and automatically re-established the client's 105 network connection including handling changes in the network topology and network identifier. The client 105, and any applications or sessions on the client 105, can continue to operate as if there was not a network connection disruption or a change in the network identifier. Furthermore, the user on the client 105 may not recognize there were any interruptions or changes, and the client 105 may not receive any notice of such interruptions.

In an additional aspect, any of the techniques of the present invention, such as the illustrative methods of Figures 2B, 3B, 3C, 4, 5B and 6B, can be practiced in one or more combinations with each other. In one embodiment, the peer-to-peer routing technique may be practiced with the false acknowledgement and/or MTU adjustment techniques. This would provide a client communicating real-time data, such as VoIP, to connect to the peer via a more optimal and direct route and to communicate the real-time data via UDP over a secure SSL/TCP/IP connection, while avoiding any latency due to any reliability mechanism of TCP and reduce fragmentation due to the encryption overhead. Additionally, this embodiment may be further combined with the client-side application-aware prioritization technique and/or the network disruption shielding technique. As such, the secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP. The network disruption technique would allow a mobile VoIP phone, such as a soft phone of a notebook, roam between network access points and automatically continue with the session.

The techniques of the present invention are complimentary to each other for network communication optimizations, such as for example in VoIP communications over a SSL VPN gateway. As such, each of the 1) peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and 5) the network

disruption shielding technique of the present invention may be practiced with one or more of the following techniques and optimization of the present invention: 1) the peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and/or 5) the network disruption shielding technique.

In one further illustrative example of the present invention, an online meeting, collaboration and/or desktop sharing service, such as the hosted service of GoToMeeting.com, WebEx.com,or LiveMeeting.com may use the techniques of the present invention in one or more combinations. The host service may use a gateway 340, and the techniques of illustrative method 260 to facilitate a peer-to-peer connection between a first computing device of a meeting presenter and a second computing device of a meeting attendee. The computing devices of the meeting presenter and attendees may download via the host service the remote access client 120, or any portions thereof. Once the meeting presenter and the meeting attendee establish a peer-to-peer connection, the peer computing devices may use any of the optimization techniques of the present invention to optimize their communications, such as the MTU adjustment technique, client-side application aware technique, or the network disruption shielding technique. Along with the peer-to-peer routing, the optimization techniques of the present invention, will improve the performance, efficiency and user experience of the online meeting, collaboration, or desktop sharing.

In yet a further aspect and in view of Figure 2A, for example, the remote access client 120 of the present invention can distribute Dynamic Host Configuration Protocol (DHCP) IP addresses of the client 105 or the publicly visible IP addresses to the telecommunication device 210a-210b, such as either a hardware or software based VoIP telephone. The gateway 340 of the present invention facilitates the discovery of the public IP addresses of the client, such as client 105b illustrated in Figure 2A. As such, the techniques of the present invention enables protocols that communicate their IP address over the protocol to continue to function.

Many alterations and modifications may be made by those having ordinary skill in the art without departing from the spirit and scope of the invention. Therefore, it must be expressly understood that the illustrated embodiments have been shown only for the purposes of example and should not be taken as limiting the invention, which is defined by the following claims. These claims are to be read as including what they set forth

literally and also those equivalent elements which are insubstantially different, even though not identical in other respects to what is shown and described in the above illustrations.

We claim:

1. A method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device;

(b) initiating, by the first computing device, a communication session to the second computing device via the third computing device;

(c) receiving, by a server, a signal to establish the communication session;

(d) communicating, by the server, to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) communicating, by the first computing device, a request to initiate a connection with the second computing device using the first network address;

(f) intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating, by the third computing device, a request to the second computing device to allow a connection from the first computing device using the second network address.

2. The method of claim 1, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network

3. The method of claim 1, wherein the third computing device comprises a remote access gateway.

4. The method of claim 1, wherein the second computing device is located behind a firewall associated with the second network address.

5. The method of claim 1, comprising providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

6. The method of claim 1, comprising providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

7. The method of claim 1, comprising communicating, by the third computing device, a key to the first computing device and the second computing device.

8. The method of claim 7, comprising communicating, by the first computing device, the key to the second computing device.

9. The method of claim 8, comprising checking, by the first computing device, that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

10. The method of claim 7, comprising communicating, by the second computing device, the key to the first computing device.

11. The method of claim 10, comprising checking, by the second computing device, that the key received from the first computing device matches the key of the second computing device before transmitting data to the second computing device.

12. The method of claim 1, associating a first telecommunication device with the first computing device, and associating a second telecommunication device with the second computing device.

13. The method of claim 12, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

14. The method of claim 12, comprising establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection.

15. The method of claim 15, comprising communicating between the first telecommunication device and the second telecommunication device over the telecommunication session without traversing the to the first computing device

16. The method of claim 1, comprising communicating a remote display protocol via the connection between the first computing device and the second computing device.

17. The method of claim 16, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

18. The method of claim 1, comprising sharing a screen view of the first computing device with the second computing device via the connection.

19. In a gateway, a method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing a first tunneling session with the first computing device on a first network;

(b) establishing a second tunneling session with the second computing device on the second network;

(c) receiving a request by the first computing device to initiate a communication session with the second computing device;

(d) providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

(f) intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

20. The method of claim 19, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

21. The method of claim 19, wherein the second computing device is located behind a firewall associated with the second network address.

22. The method of claim 19, comprising providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

23. The method of claim 19, comprising communicating a key to the first computing device.

24. The method of claim 19, comprising communicating a key to the second computing device.

25. A system for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device, the first network disconnected from and not routable to the second network, the system comprising:

a first computing device on the first network;

a second computing device on the second network;

a third computing device establishing a first tunneling session with the first computing device and a second tunneling session with the second computing device;

a server accessible via the third computing device;

wherein:

the server communicates via the third computing device to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

the first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address;

the third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

the third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

26. The system of claim 25, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

27. The system of claim 25, wherein the third computing device comprises a remote access gateway.

28. The system of claim 25, wherein the second computing device is located behind a firewall associated with the second network address.

29. The system of claim 25, wherein the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session.

30. The system of claim 25, wherein the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

31. The system of claim 25, wherein the third computing device communicates a key to the first computing device and the second computing device.

32. The system of claim 31, wherein the first computing device communicates the key to the second computing device.

33. The system of claim 32, wherein the first computing device checks that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

34. The system of claim 31, wherein the second computing device communicates the key to the first computing device.

35. The system of claim 34, wherein the second computing device checks that the key received from the first computing devices matches the key of the second computing device before transmitting data to the second computing device.

36. The system of claim 25, comprising a first telecommunication device associated with the first computing device, and a second telecommunication associated with the second computing device.

37. The system of claim 36, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

38. The system of claim 37, wherein the first telecommunication device establishes a telecommunication session with the second telecommunication device via the connection.

39. The system of claim 38, wherein the first telecommunication device communicates with the second telecommunication device over the telecommunication session without traversing the third computing device.

40. The system of claim 25, wherein the first computing device and the second computing device communicate a remote display protocol via the connection.

41. The system of claim 25, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

42. The system of claim 25, wherein the first computing device shares a screen view with the second computing device via the connection.

43. A gateway for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the gateway comprising:

a means for establishing a first tunneling session with the first computing device on a first network;

a means for establishing a second tunneling session with the second computing device on the second network;

a means for receiving a request by the first computing device to initiate a communication session with the second computing device;

a means for providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

a means for receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

a means for intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

a means for communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

44. The system of claim 43, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

45. The system of claim 43, wherein the second computing device is located behind a firewall associated with the second network address.

46. The system of claim 43, comprising a means for providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

47. The system of claim 43, comprising a means for communicating a key to the first computing device.

48. The system of claim 43, comprising a means for communicating a key to the second computing device.

49. A method for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the method comprising the steps of:

(a) establishing a connection between a first computing device and a second computing device via a lossless protocol;

(b) detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

(c) communicating, by the first computing device, a false acknowledgement of receipt of
the lossless protocol packet to one of the first computing device or the second computing device; and

(d) communicating, by the first computing device, the lossless protocol packet to the second computing device.

50. The method of claim 49, comprising encrypting, by the first computing device, the one or more packets using a key.

51. The method of claim 50, comprising providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

52. The method of claim 49, comprising encrypting the one or more packets on a packet by packet basis.

53. The method of claim 49, further comprising performing step (c) before step (d).

54. The method of claim 49, wherein the second computing device is a gateway.

55. The method of claim 49, comprising, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

56. The method of claim 49, wherein the lossless protocol comprises a transport control protocol.

57. The method of claim 56, comprising preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, a flow control algorithm, a naple's algorithm, and a sliding window algorithm.

58. The method of claim 49, wherein the lossy protocol comprises a user datagram protocol.

59. The method of claim 49, comprising communicating, by the first computing device, the
lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to
the second computing device.

60. The method of claim 49, wherein the one or more packets comprises a real-time protocol.

61. The method of claim 49, comprising communicating by the first computing device one of
real-time voice, audio, or data to the second computing device via the one or more packets.

62. A system for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the system comprising:

a means for establishing a connection between a first computing device and a second computing device via a lossless protocol;

a means for detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

a means for communicating, by the first computing device, a false acknowledgement of receipt of the lossless protocol packet to one of the first computing device or the second computing device; and

a means for communicating, by the first computing device, the lossless protocol packet to the second computing device.

63. The system of claim 62, comprising a means for encrypting, by the first computing device, the one or more packets using a key.

64. The system of claim 63, comprising a means for providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

65. The system of claim 63, comprising a means for encrypting the one or more protocol packets on a packet by packet basis.

66. The system of claim 62, further comprising a means for communicating the false acknowledgement of receipt of the lossless protocol packet before communicating the

lossless protocol packet.

67. The system of claim 62, wherein the second computing device is a gateway.

68. The system of claim 62, comprising a means, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, for preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

69. The system of claim 62, wherein the lossless protocol comprises a transport control protocol.

70. The system of claim 69, comprising a means for preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, and a flow control algorithm.

71. The system of claim 62, wherein the lossy protocol comprises a user datagram protocol.

72. The system of claim 62, comprising a means for communicating, by the first computing device, the lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to the second computing device.

73. The system of claim 62, wherein the one or more packets comprises a real-time protocol.

74. The system of claim 62, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

75. A method for transmitting packets from an application using an unreliable

transport protocol over a TCP connection, comprising:

receiving, at a first device, a first packet to be transmitted using an unreliable transport protocol;

creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device;

transmitting, by the first device, the first TCP packet to the second device;

receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol;

creating a second TCP packet including a second payload of the received second packet and the first TCP header information; and

transmitting, by the first device, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

76. The method of claim 75, comprising establishing the TCP connection with a port number associated with the unreliable transport protocol.

77. The method of claim 75, comprising dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol.

78. The method of claim 75, wherein the unreliable transport protocol is UDP.

79. The method of claim 75, comprising further:

receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism.

80. The method of claim 75, comprising establishing, by the first device, the TCP connection with a VPN gateway device.

81. The method of claim 75, comprising establishing peer-to-peer communications between the first device and the second device via the TCP connection.

82. The method of claim 75, comprising encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

83. A method for transmitting packets from an application using an unreliable transport protocol over a TCP connection, comprising:

intercepting, at a second device, a first TCP packet created on a first device and received on the second device, the first TCP packet including a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device, the intercepting occurring before the first TCP packet is provides to a TCP stack on the second device;

identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable transport protocol;

stripping the TCP header of information from the first TCP packet; and

forwarding the first payload to an application using the unreliable data protocol.

84. The method of claim 83, wherein the unreliable protocol is UDP.

85. The method of claim 83, wherein the step of identifying comprises identifying the TCP header information includes a port number associated with the unreliable transport protocol.

86. The method of claim 83, comprising further:

intercepting, by the second device, the first TCP packet using a packet capture driver.

87. The method of claim 83, wherein the first device is a client device and the

second device is a VPN gateway.

88. The method of claim 87, comprising further:
performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

89. A system for transmitting packets from an application using an unreliable transport protocol over a TCP connection, the system comprising:
a first device, the first device comprising:
an application generating a first and second packet, the first and second packet intended to be transmitted using an unreliable transport protocol;
a filter process, the filter process intercepting the first and second packets from the application and forwarding the intercepted packets to a tunnel process; and
a tunnel process, the tunnel process requesting the opening of a TCP connection between the first device and a second device, the request to open the TCP connection indicating to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol, the tunnel process forwarding the first and second packets as payloads in a first and second TCP packet to the second device, the tunnel process sending the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet ; and
a second device in communication with the first device, the second device comprising:
a second tunnel process opening the TCP connection requested by the first device, the second tunnel process identifying and forwarding the source address of the TCP connection to a second filter process; and
the second filter process, the second filter process intercepting packets from the application received at the second device with the TCP connection source address in a header, the second filter process stripping the TCP header from the received packets and forwarding the stripped packets,

circumventing the TCP/IP stack on the second device, to an intended destination.

90. The system of claim 89, wherein the filter process on the first device comprises a packet capture driver.

91. The system of claim 89, wherein the second filter process on the second device comprises a packet capture driver.

92. The system of claim 89, wherein the first device is a client device and the second device is a VPN gateway device.

93. The system of claim 89, further comprising:
a third device to which the stripped packets are transmitted.

94. The system of claim 93, wherein the second device comprises further:
a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to a third device.

95. The system of claim 89, wherein the unreliable data protocol is UDP.

96. A method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the method comprising the steps of:

(a) establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

(b) detecting, by the first computing device, a network packet having an encrypted payload;

(c) determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

(d) altering the maximum transmission unit parameter of the first network stack to the determined setting.

97. The method of claim 96, comprising communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

98. The method of claim 96, wherein the payload comprises a real-time protocol.

99. The method of claim 96, further comprising altering the maximum transmission unit parameter via a network driver interface specification level mechanism of the first network stack

100. The method of claim 96, further comprising determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

101. The method of claim 96, comprising establishing the session between the first computing device and the second computing device via a gateway.

102. The method of claim 96, communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

103. The method of claim 96, comprising communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

104. The method of claim 96, further comprising establishing the session between the first computing device and the second computing device via an agent of the first computing device.

105. The method of claim 104, comprising communicating, by the agent, via an IOCTL application programming interface to the first network stack to alter the

maximum transmission unit parameter to the determined setting.

106. A system for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the system comprising:

a means for establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

a means for detecting, by the first computing device, a network packet having an encrypted payload;

a means for determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

a means for altering the maximum transmission unit parameter of the first network stack to the determined setting.

107. The system of claim 106, comprising a means for communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

108. The system of claim 106, wherein the payload comprises a real-time protocol.

109. The system of claim 106, wherein the payload comprises a representation of one of real-time voice, audio, or data.

110. The system of claim 106, further comprising a means for altering the maximum transmission unit parameter of the first computing device via a network driver interface specification level mechanism of the first network stack

111. The system of claim 106, further comprising a means for determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

112. The system of claim 106, comprising a means for establishing the session

between the first computing device and the second computing device via a gateway.

113. The system of claim 106, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

114. The system of claim 106, comprising a means for communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

115. The system of claim 106, wherein the network packet comprises a lossless protocol packet.

116. The system of claim 115, wherein the lossless protocol packet comprises a transport control protocol.

117. The system of claim 106, wherein the payload comprises a lossy protocol packet.

118. The system of claim 117, wherein the lossy protocol packet comprises a user datagram protocol.

119. The system of claim 106, comprising an agent of the first computing device for establishing the session between the first computing device and the second computing device.

120. The system of claim 119, wherein the agent communicates via an IOCTL application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

121. A method for a client to prioritize network communications of the client associated with an application of the client, the method comprising the steps of:

(a) intercepting, by the client, one or more network packets associated with one or more applications of the client;

(b) storing, by the client, the one or more network packets to a queue;

(c) determining, by the client, the queued one or more network packets is associated with a first application of the client;

(d) indicating, by the client, a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client; and

(e) providing the prioritized one or more network packets for communications via a network stack of the client.

122. The method of claim 121, wherein the step of determining, by the client, further comprises determining the queued one or more networks packets of the first application comprises real-time data.

123. The method of claim 122, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

124. The method of claim 121, comprising preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

125. The method of claim 121, comprising holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

126. The method of claim 121, comprising intercepting, by the client, the one or more network packets transparently to the one or more applications on the client.

127. The method of claim 121, comprising running the first application in the foreground, and the second application in the background.

128. The method of claim 121, comprising associating a priority with the first

application higher than a priority associated with the second application.

129. The method of claim 128, comprising specifying, by a user, the priority of one of the first application or the second application.

130. The method of claim 121, comprising receiving, by the client, the one or more network packets from a computing device.

131. The method of claim 121, comprising providing, by the one or more applications, the one or more network packets for communicating from the client to a computing device.

132. A client for prioritizing network communications of the client associated with an application of the client, the client comprising:

a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client, and

a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client; and

an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

133. The client of claim 132, wherein the agent determines the one or more networks packets of the first application comprises real-time data.

134. The client of claim 132, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

135. The client of claim 132, wherein one of the agent or the network driver prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

136. The client of claim 132, wherein the network driver holds in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

137. The client of claim 132, wherein the mechanism intercepts the one or more network packets transparently to the one or more applications on the client.

138. The client of claim 132, wherein the first application is running in the foreground, and the second application is running in the background.

139. The client of claim 132, wherein the first application has a priority higher than the second application of the client.

140. The client of claim 132, comprising a configuration mechanism for a user to specify the priority.

141. The client of claim 132, wherein the client receives the one or more network packets from a computing device.

142. The client of claim 132, wherein the one or more applications provides the one or more network packets for communicating from the client to a computing device.

143. The client of claim 132, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

144. The client of claim 132, wherein the network driver operates in kernel-mode of an operating system of the client.

145. The client of claim 132, wherein the agent operates in user-mode of an operating system of the client.

146. The client of claim 132, wherein one of the agent or the network driver comprises the mechanism for intercepting one or more network packets of the client.

147. A method for shielding from a network disruption a session established via a first protocol, the method comprising the steps of:

(a) establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device, the network connection associated with a network stack, a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol;

(b) detecting a disruption in the network connection causing the first portion of the network stack to be disestablished;

(c) maintaining, by the agent, the session and the second portion of the network stack during the disruption; and

(d) re-establishing the second portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

148. The method of claim 147, comprising the step of:

(e) continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

149. The method of claim 147, comprising the step of

(e) dropping, by the second portion of the network stack, any network packets received

during the disruption.

150. The method of claim 147, wherein the device comprises one of a remote access gateway or a computing device.

151. The method of claim 147, further comprising establishing the session via the first protocol of one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

152. The method of claim 147, comprising communicating, by the agent, real-time data via the session between the client and the device.

153. The method of claim 152, wherein the real-time data comprises a real-time protocol.

154. The method of claim 152, wherein the real-time data comprises a representation of one of voice or audio.

155. The method of claim 147, comprising operating the agent in user-mode of an operating system of the client.

156. The method of claim 147, wherein the first portion of the network comprises one of a transport control protocol or an internet protocol.

157. The method of claim 147, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

158. The method of claim 147, comprising the client communicating with the device via a remote display protocol.

159. The method of claim 158, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

160. The method of claim 147, comprising performing one of steps (b), (c) and (d) transparently to an application of the client communicating via the network connection.

161. The method of claim 147, comprising intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application.

162. The method of claim 147, comprising intercepting, by a network driver

associated with the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

163. A system for shielding from a network disruption a session established via a first protocol, the system comprising

an agent of a client establishing a session between the client and a device over a network connection via a first protocol;

a network stack having a first portion and a second portion, the first portion of the network stack comprising one or more layers of the network stack below the layer of the first protocol, and the second portion of the network stack comprising a layer for the first protocol and one or more layers of the network stack above the first protocol; and

a detector for detecting a disruption in the network connection causing the second portion of the network stack to be disestablished;

wherein:

upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption; and

the client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

164. The system of claim 163, wherein the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

165. The system of claim 163, wherein one of the first portion or the second portion of the network stack drops any network packets received during the disruption.

166. The system of claim 163, wherein the device comprises one of a remote access gateway or a computing device.

167. The system of claim 163, wherein the first protocol comprises one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

168. The system of claim 163, wherein the agent communicates real-time data via the session between the client and the device.

169. The system of claim 168, wherein the real-time data comprises one of a real-time protocol.

170. The system of claim 168, wherein the real-time data comprises a representation of one of voice or audio.

171. The system of claim 163, wherein the agent operates in user-mode of an operating system of the client.

172. The system of claim 163, wherein the first portion of the network stack comprises one of a transport control protocol or an internet protocol.

173. The system of claim 163, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

174. The system of claim 163, wherein the first protocol comprises a remote display protocol.

175. The system of claim 174, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

176. The system of claim 163, wherein the agent intercepts one or more network packets of an application of the client transparently to the application.

177. The system of claim 163, comprising a network driver associated with the second portion of the network stack, the network driver intercepts one or more network packets of an application of the client transparently to the application, and provides the one or more packets to the agent to communicate via the session.

178. The system of claim 177, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

179. The system of claim 177, wherein the network driver operates in kernel-mode of an operating system of the client.

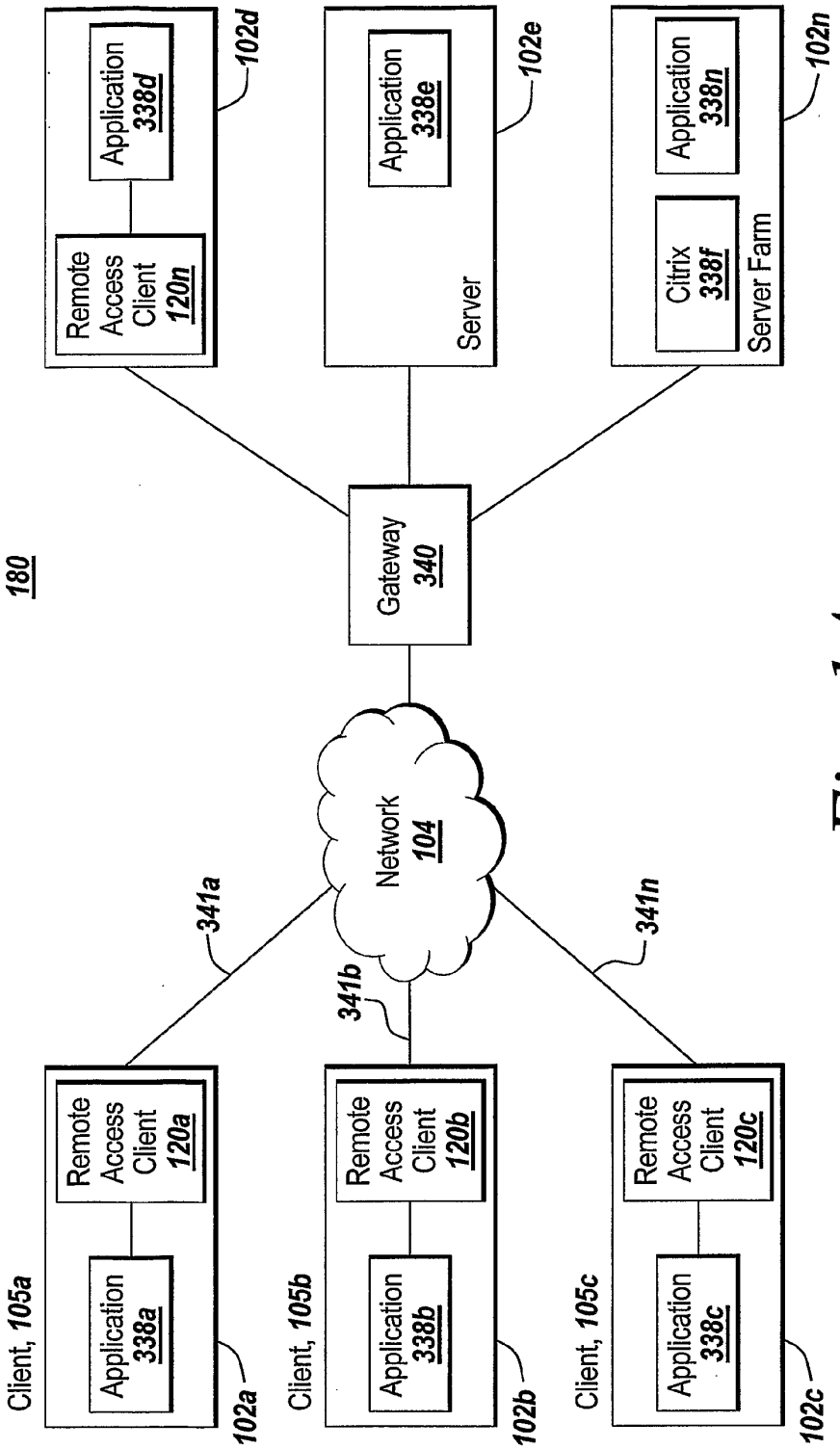

180
Client, 105a
Application 338a
Remote Access Client 120a
102a
Client, 105b
Application 338b
Remote Access Client 120b
102b
Client, 105c
Application 338c
Remote Access Client 120c
102c
341a
341b
341n
Network 104
Gateway 340
Application 338d
Remote Access Client 120n
102d
Application 338e
Server
102e
Application 338n
Citrix 338f
Server Farm
102n

Fig. 1A

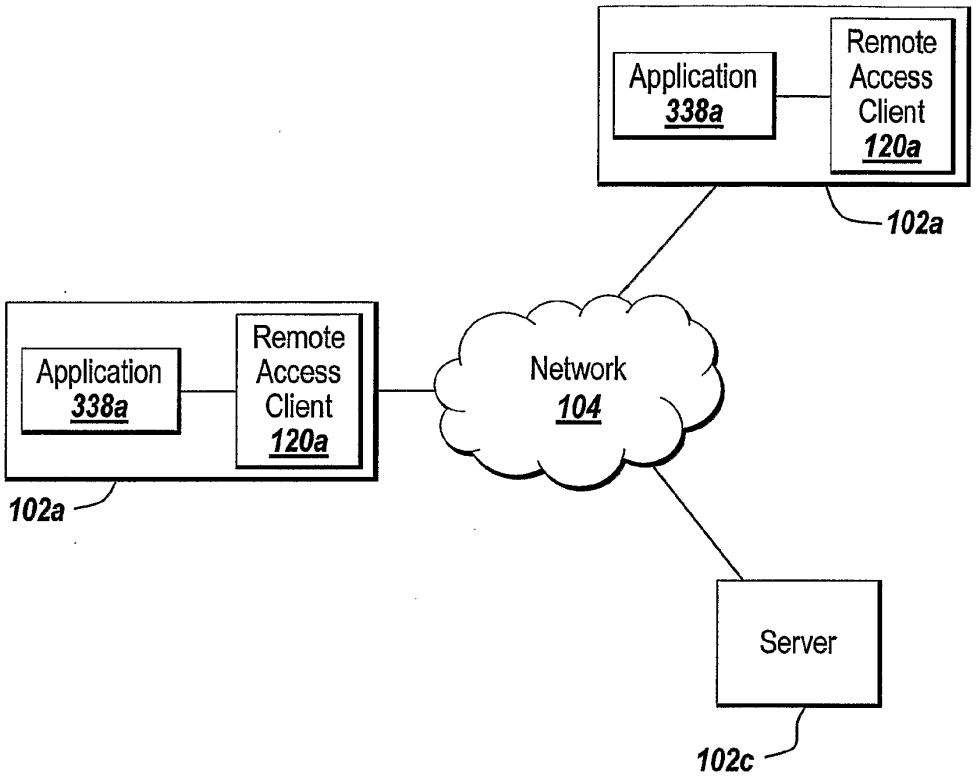

Application
338a
Remote
Access
Client
120a
102a
Application
338a
Remote
Access
Client
120a
102a
Network
104
Server
102c

Fig. 1B

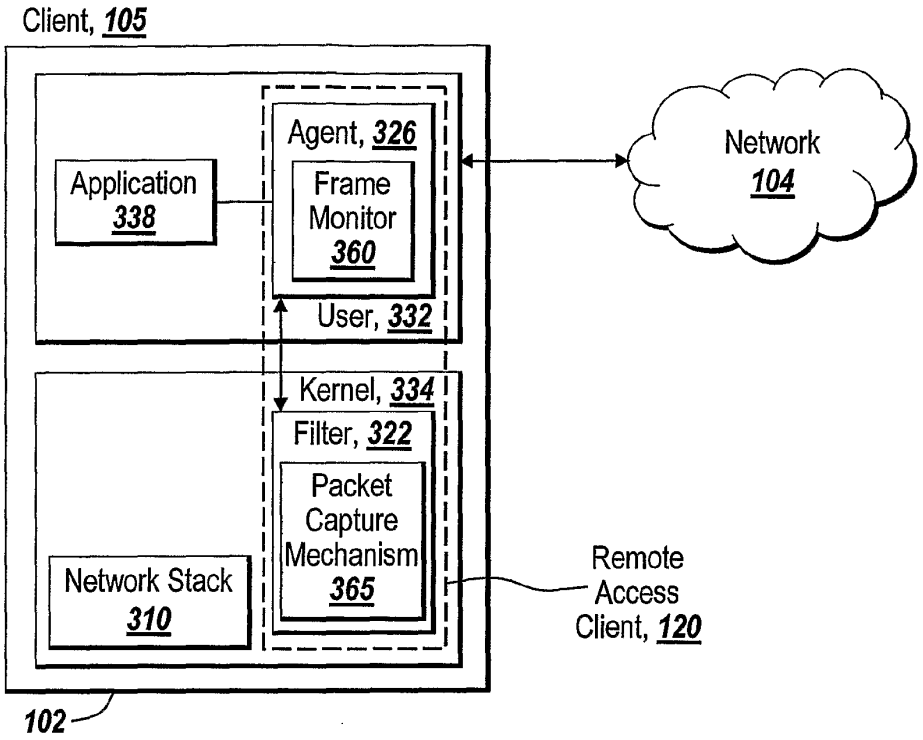

Client, 105
Agent, 326
Application 338
Frame Monitor 360
User, 332
Kernel, 334
Filter, 322
Packet Capture Mechanism 365
Network Stack 310
Network 104
Remote Access Client, 120
102

Fig. 1C

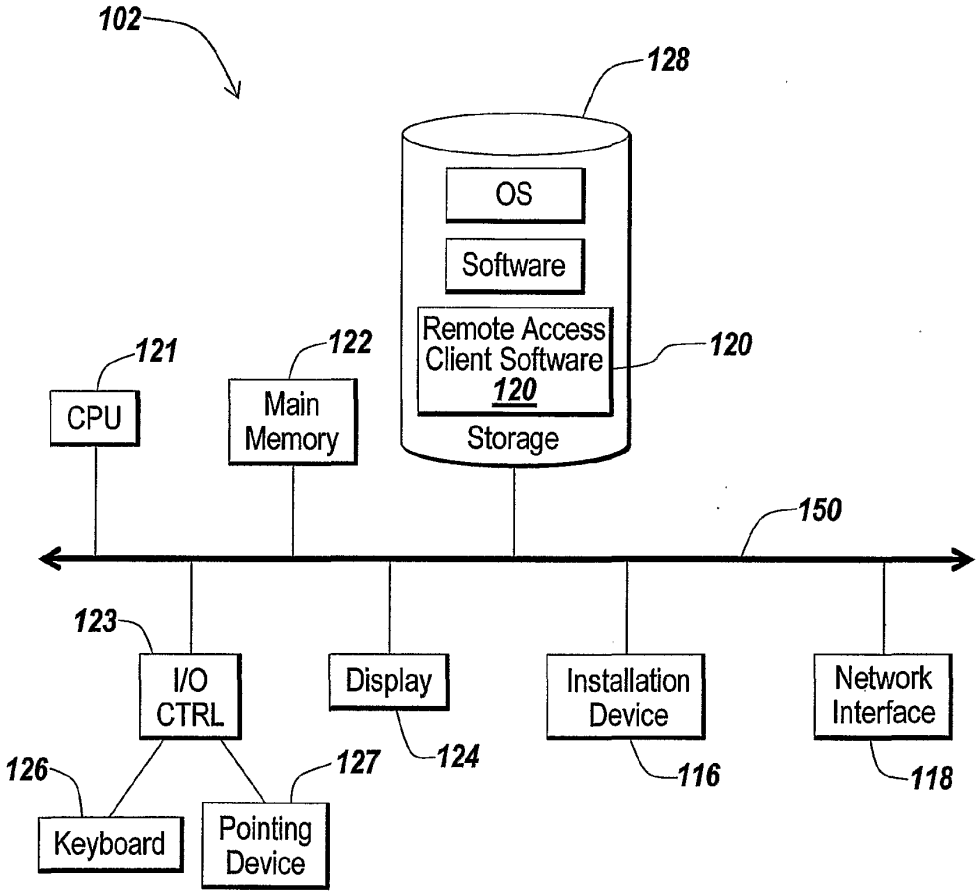

102
128
OS
Software
Remote Access Client Software
120
120
Storage
121
CPU
122
Main Memory
150
123
I/O CTRL
Display
124
Installation Device
116
Network Interface
118
126
Keyboard
127
Pointing Device

Fig. 1D

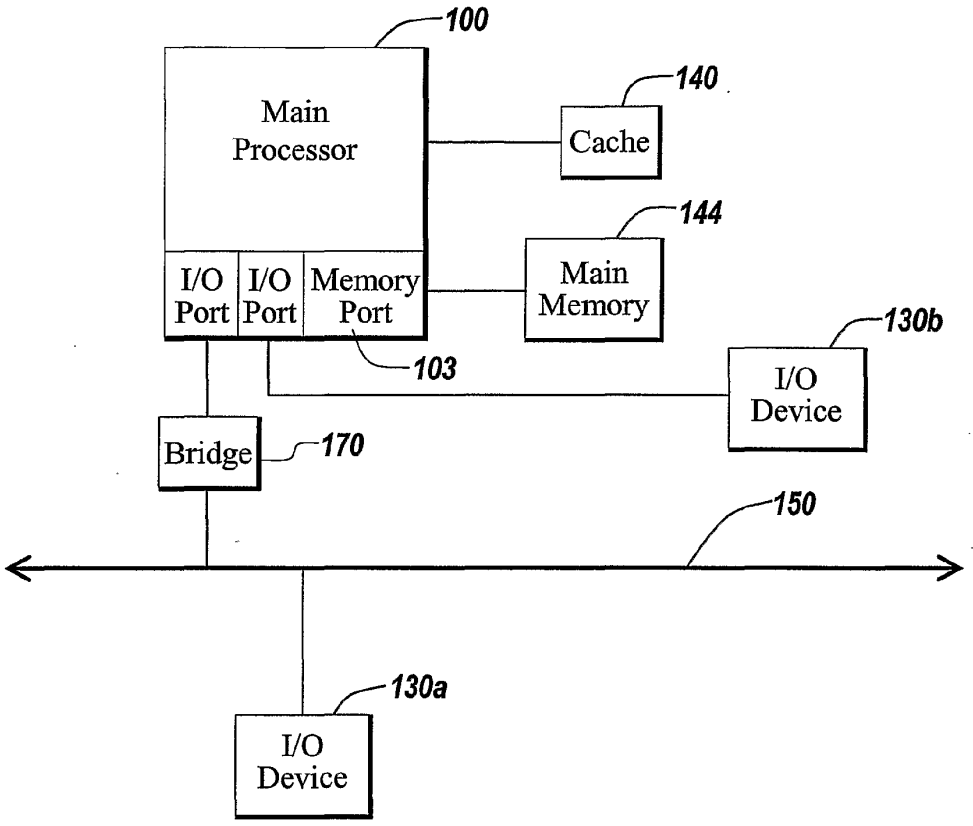

100
Main Processor
140
Cache
144
Main Memory
I/O Port
I/O Port
Memory Port
103
130b
I/O Device
Bridge
170
150
130a
I/O Device

Fig. 1E

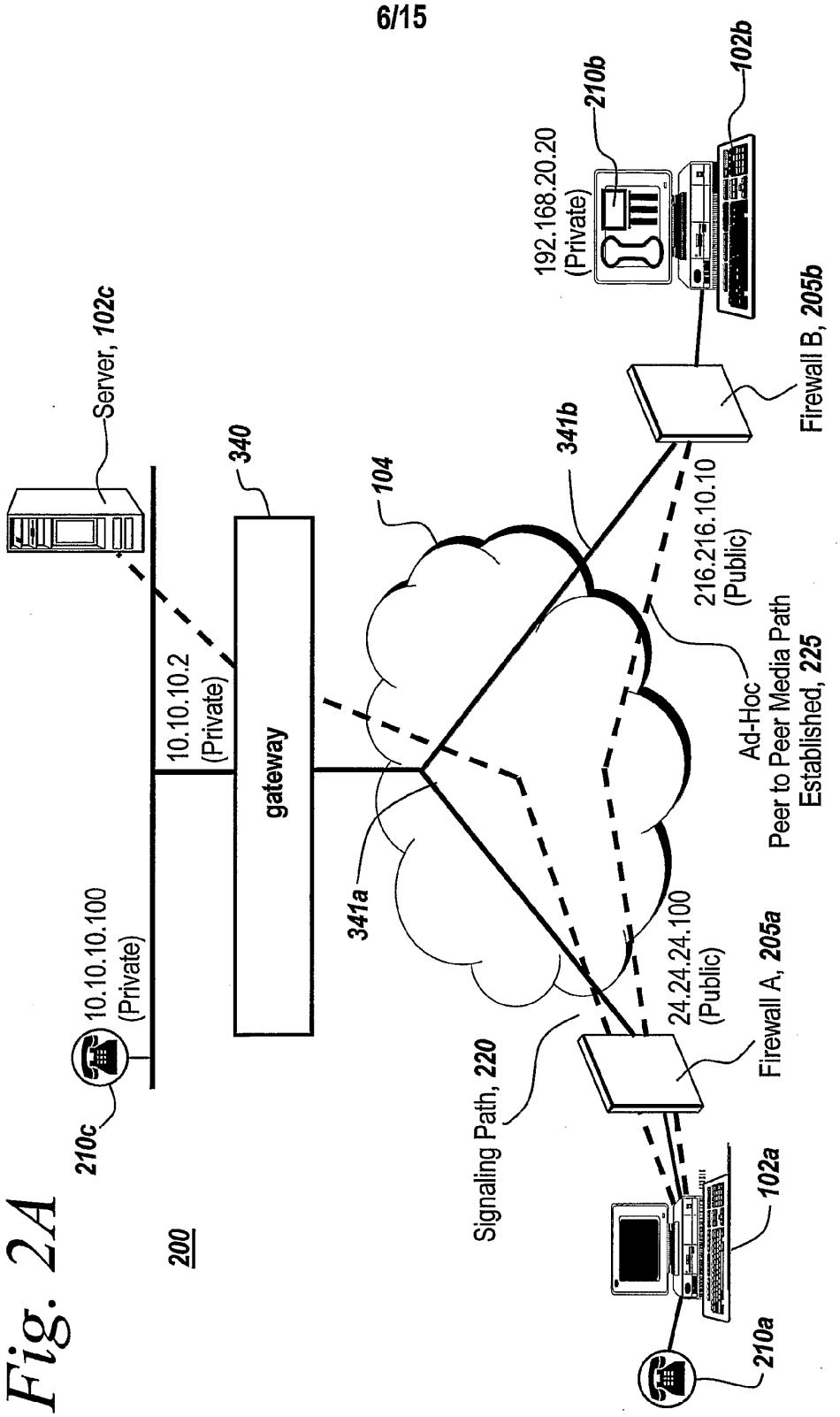

Server, 102c
340
104
341b
210b
102b
192.168.20.20
(Private)
10.10.10.2
(Private)
gateway
216.216.10.10
(Public)
Ad-Hoc
Peer to Peer Media Path
Established, 225
Firewall B, 205b
10.10.10.100
(Private)
341a
24.24.24.100
(Public)
Signaling Path, 220
Firewall A, 205a
210c
200
102a
210a

Fig. 2A

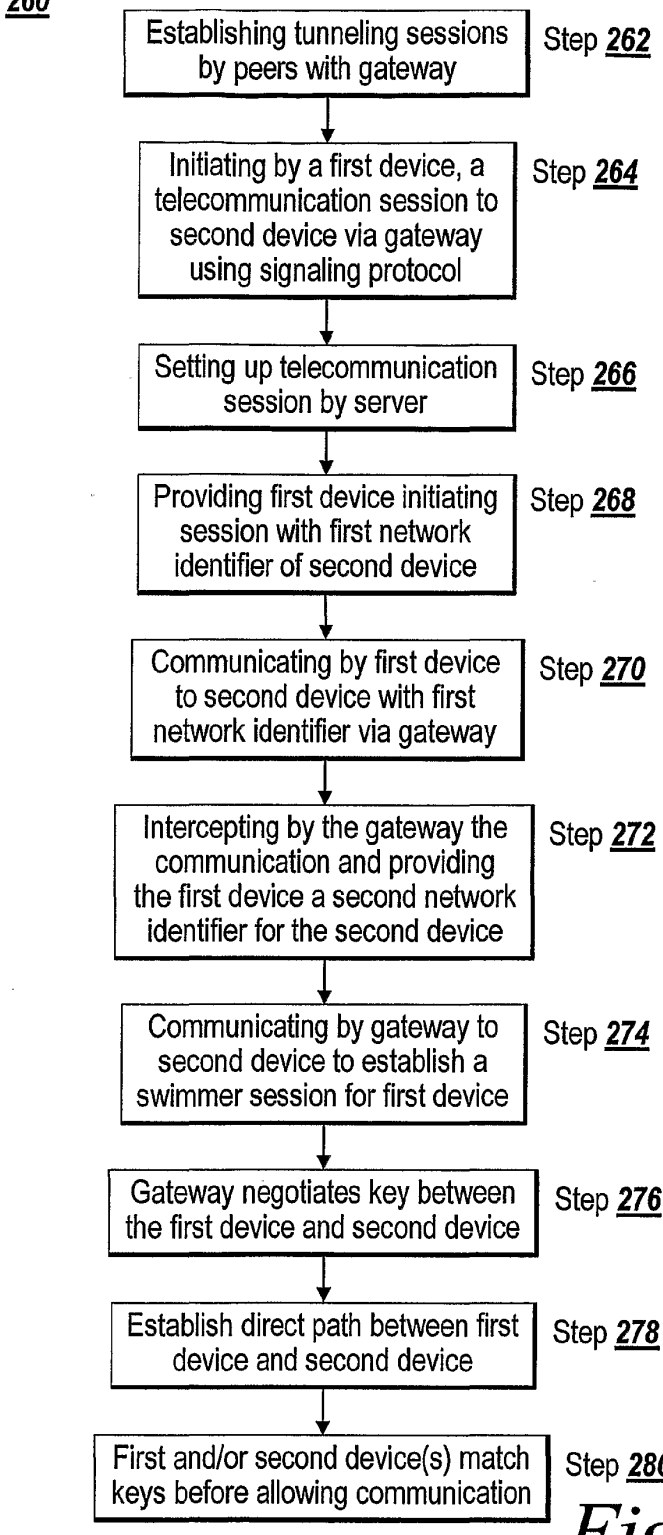

260
Establishing tunneling sessions by peers with gateway
Step 262
Initiating by a first device, a telecommunication session to second device via gateway using signaling protocol
Step 264
Setting up telecommunication session by server
Step 266
Providing first device initiating session with first network identifier of second device
Step 268
Communicating by first device to second device with first network identifier via gateway
Step 270
Intercepting by the gateway the communication and providing the first device a second network identifier for the second device
Step 272
Communicating by gateway to second device to establish a swimmer session for first device
Step 274
Gateway negotiates key between the first device and second device
Step 276
Establish direct path between first device and second device
Step 278
First and/or second device(s) match keys before allowing communication
Step 280

Fig. 2B

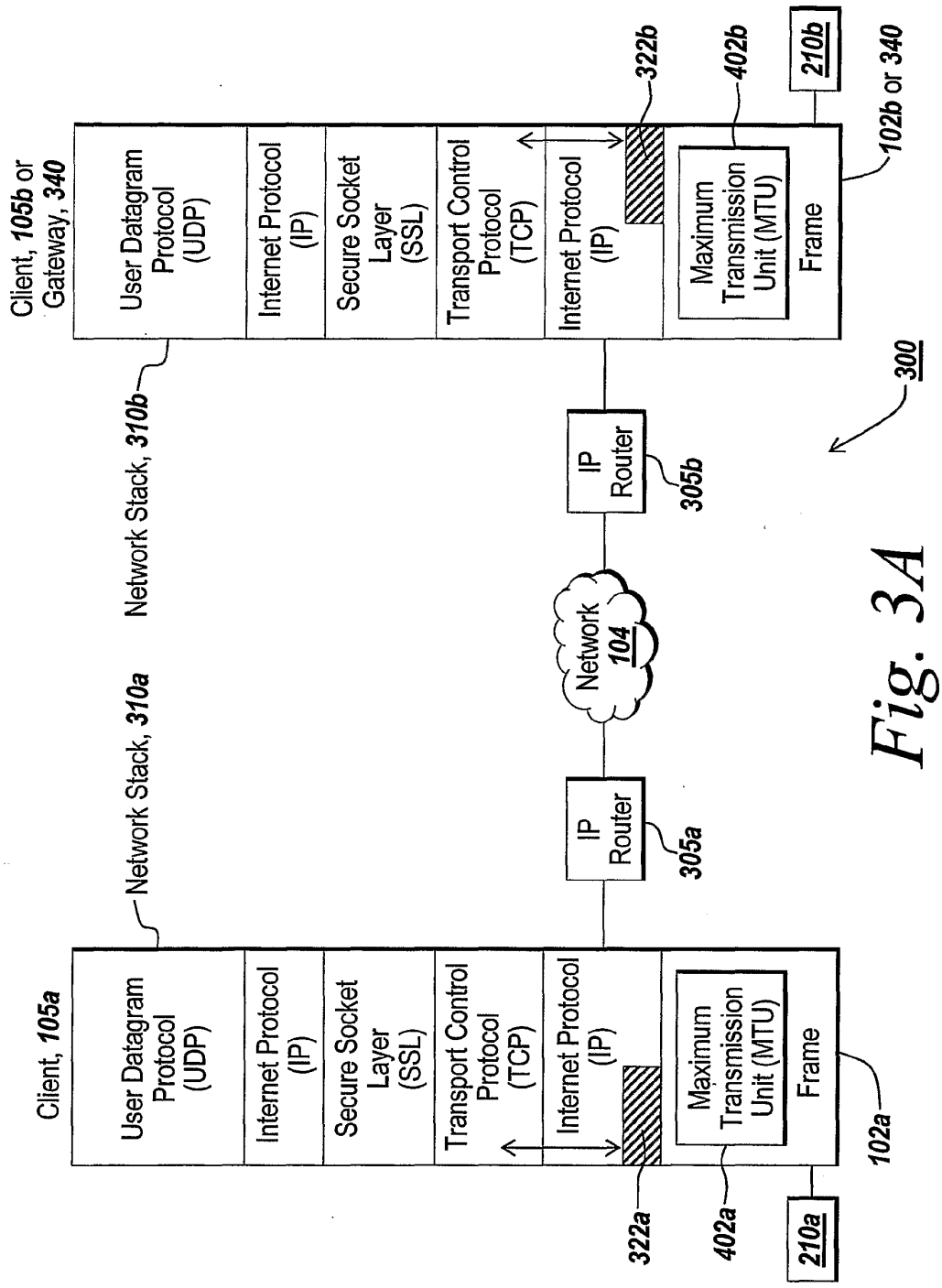

Client, 105a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
102a
322a
402a
210a
Network Stack, 310a
IP Router
305a
Network 104
IP Router
305b
Network Stack, 310b
Client, 105b or Gateway, 340
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
102b or 340
322b
402b
210b
300

Fig. 3A

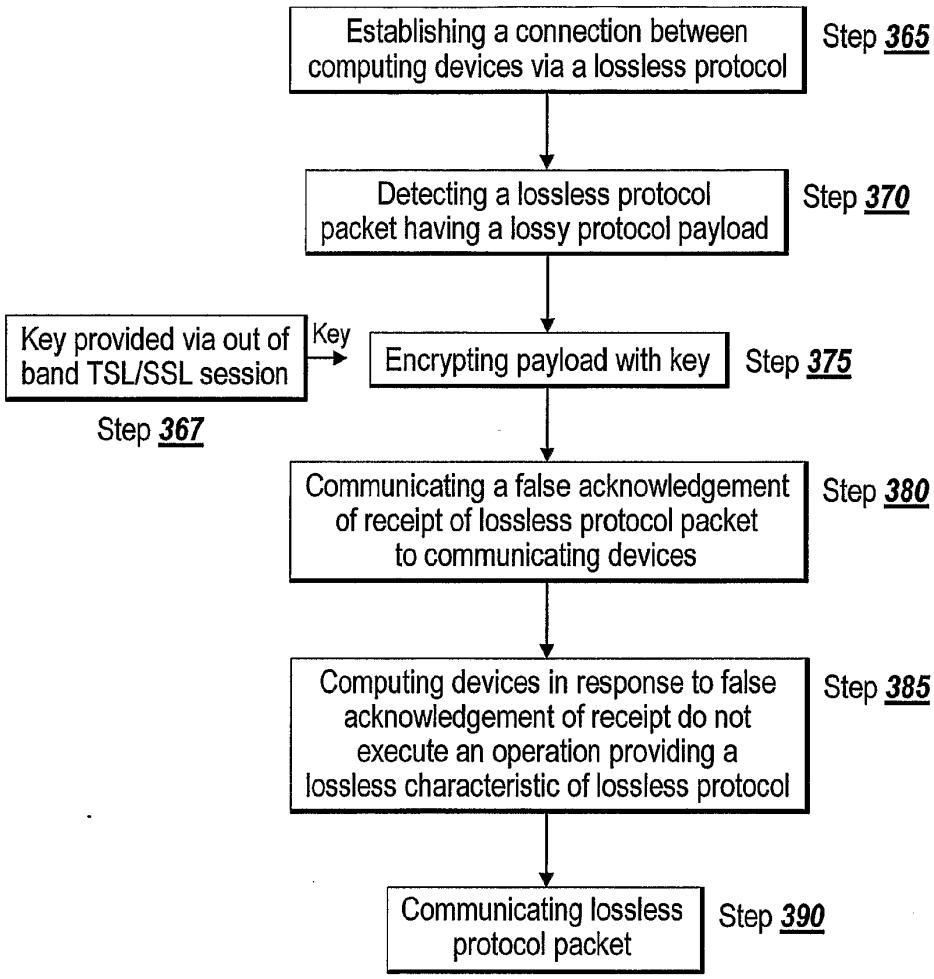

Establishing a connection between computing devices via a lossless protocol
Step 365
Detecting a lossless protocol packet having a lossy protocol payload
Step 370
Key provided via out of band TSL/SSL session
Key
Encrypting payload with key
Step 375
Step 367
Communicating a false acknowledgement of receipt of lossless protocol packet to communicating devices
Step 380
Computing devices in response to false acknowledgement of receipt do not execute an operation providing a lossless characteristic of lossless protocol
Step 385
Communicating lossless protocol packet
Step 390

Fig. 3B

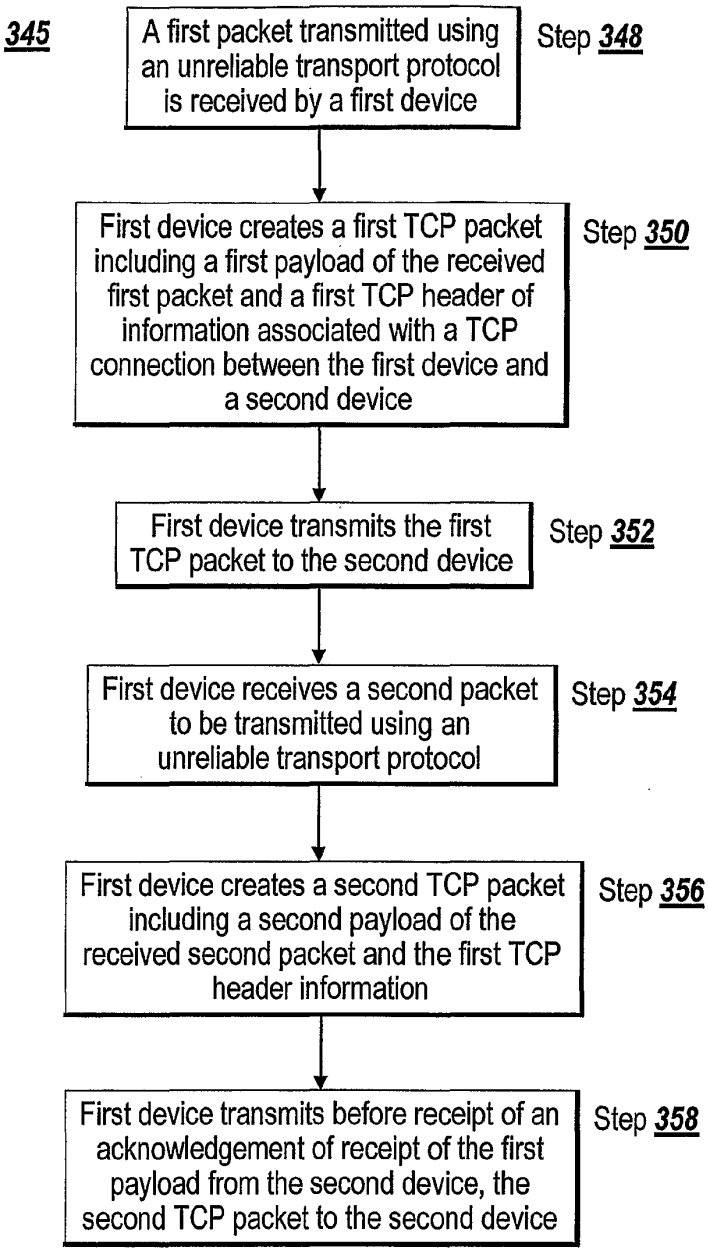

345
A first packet transmitted using an unreliable transport protocol is received by a first device
Step 348
First device creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection between the first device and a second device
Step 350
First device transmits the first TCP packet to the second device
Step 352
First device receives a second packet to be transmitted using an unreliable transport protocol
Step 354
First device creates a second TCP packet including a second payload of the received second packet and the first TCP header information
Step 356
First device transmits before receipt of an acknowledgement of receipt of the first payload from the second device, the second TCP packet to the second device
Step 358

Fig. 3C

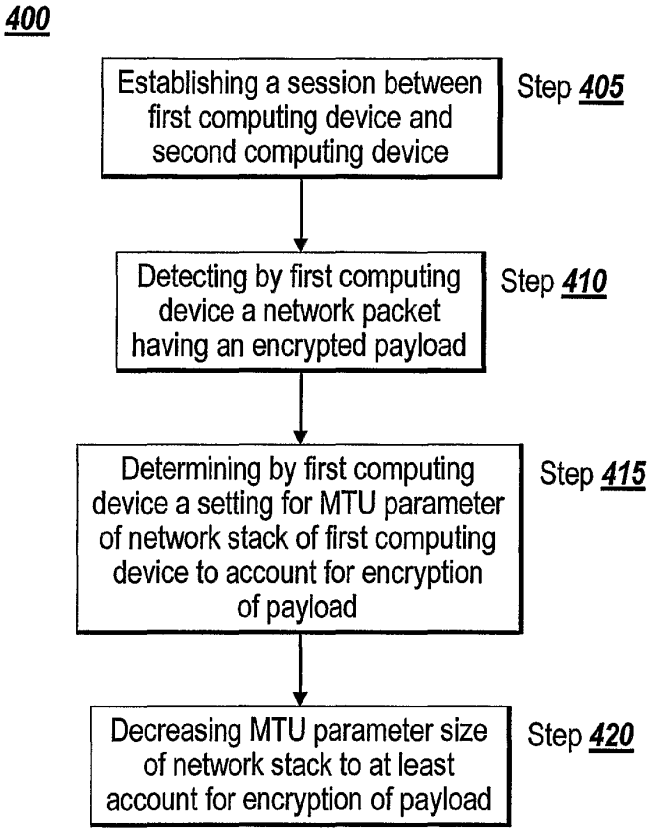

400
Establishing a session between first computing device and second computing device
Step 405
Detecting by first computing device a network packet having an encrypted payload
Step 410
Determining by first computing device a setting for MTU parameter of network stack of first computing device to account for encryption of payload
Step 415
Decreasing MTU parameter size of network stack to at least account for encryption of payload
Step 420

Fig. 4

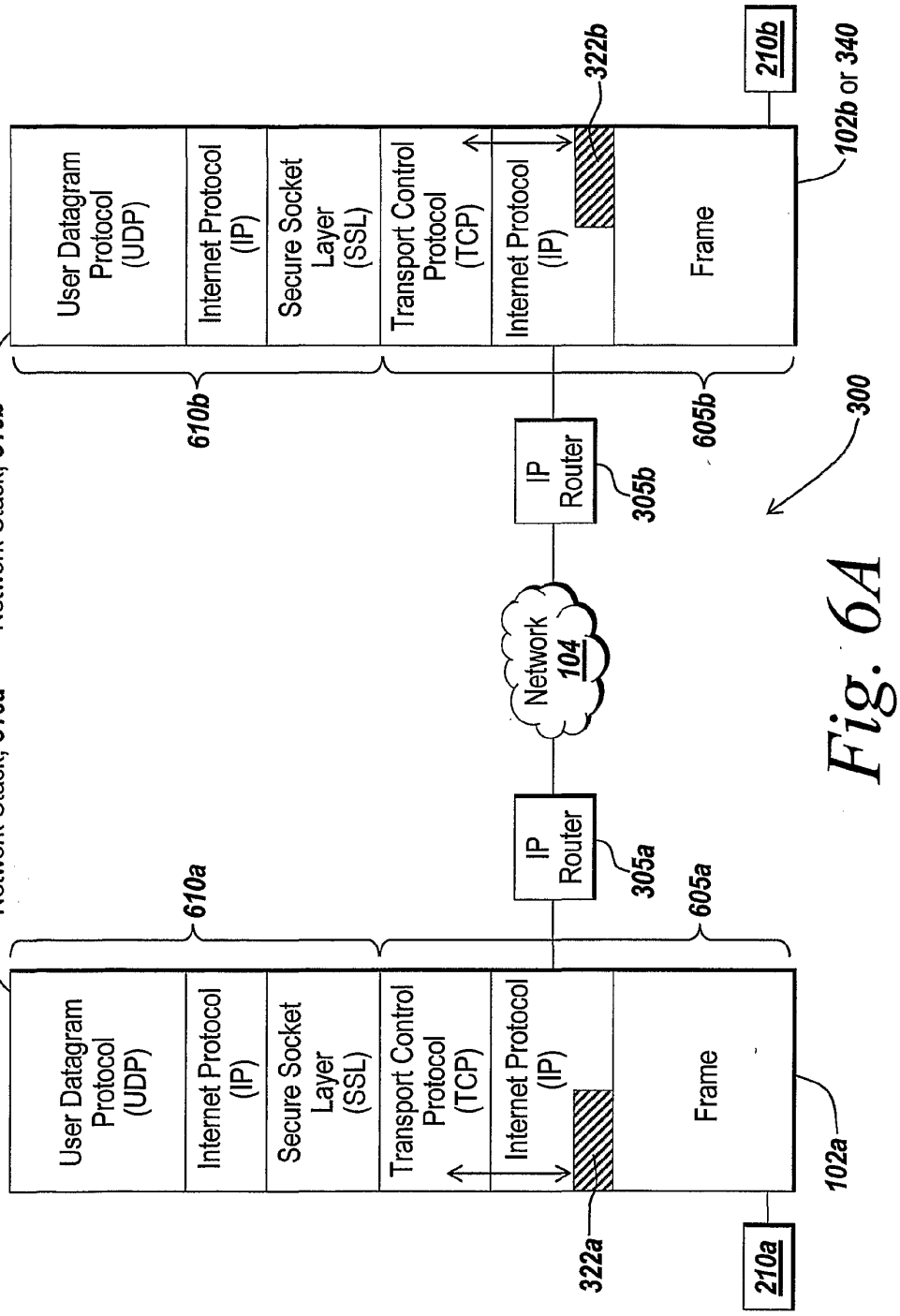

Network Stack, 310b
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Frame
322b
210b
102b or 340
610b
605b
300
IP Router
305b
Network 104
IP Router
305a
Network Stack, 310a
610a
605a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Frame
322a
210a
102a

Fig. 6A

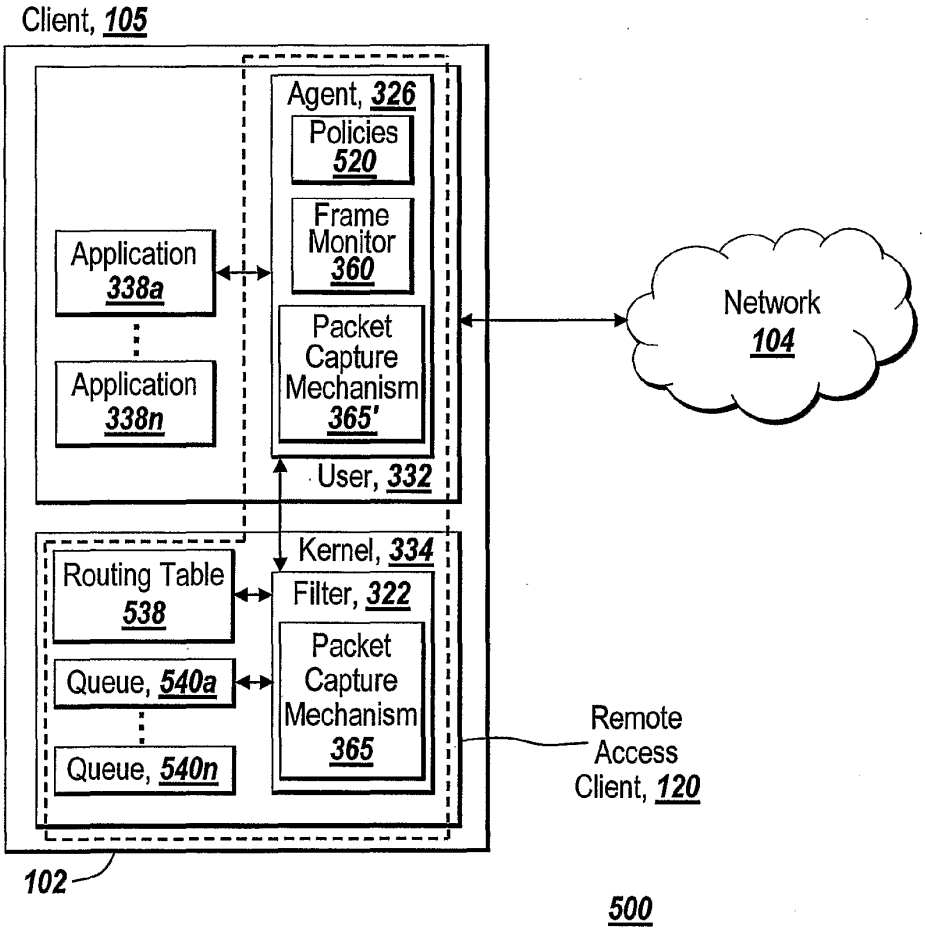

Client, 105
Agent, 326
Policies 520
Frame Monitor 360
Application 338a
Application 338n
Packet Capture Mechanism 365'
Network 104
User, 332
Kernel, 334
Routing Table 538
Filter, 322
Queue, 540a
Queue, 540n
Packet Capture Mechanism 365
Remote Access Client, 120
102
500

Fig. 5A

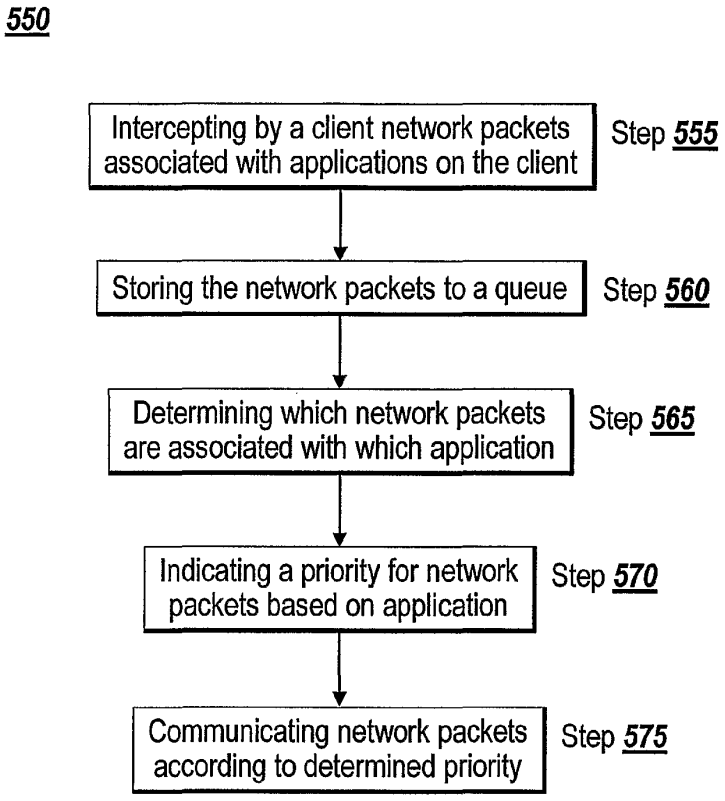

550
Intercepting by a client network packets associated with applications on the client
Step 555
Storing the network packets to a queue
Step 560
Determining which network packets are associated with which application
Step 565
Indicating a priority for network packets based on application
Step 570
Communicating network packets according to determined priority
Step 575

Fig. 5B

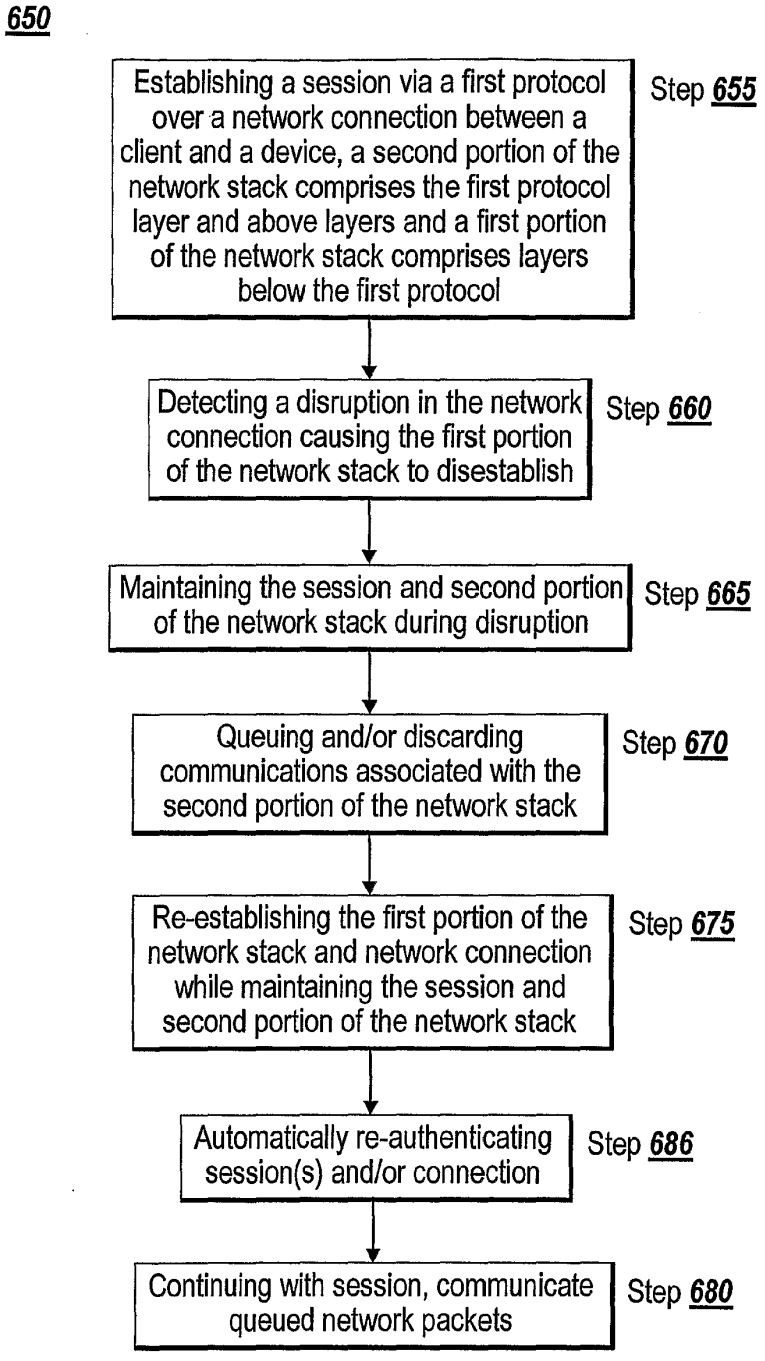

650
Establishing a session via a first protocol over a network connection between a client and a device, a second portion of the network stack comprises the first protocol layer and above layers and a first portion of the network stack comprises layers below the first protocol
Step 655
Detecting a disruption in the network connection causing the first portion of the network stack to disestablish
Step 660
Maintaining the session and second portion of the network stack during disruption
Step 665
Queuing and/or discarding communications associated with the second portion of the network stack
Step 670
Re-establishing the first portion of the network stack and network connection while maintaining the session and second portion of the network stack
Step 675
Automatically re-authenticating session(s) and/or connection
Step 686
Continuing with session, communicate queued network packets
Step 680

Fig. 6B

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 02156671.2

[43] 公开日 2004 年 6 月 30 日

[11] 公开号 CN 1508734A

[22] 申请日 2002.12.13 [21] 申请号 02156671.2

[71] 申请人 华人创意股份有限公司
地址 台湾省台北市
[72] 发明人 温世仁 吴鸿祺

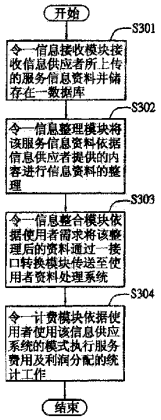
[74] 专利代理机构 北京三幸商标专利事务所
代理人 刘激扬

权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 用以支持中小企业营运发展的信息供应方法以及系统

[57] 摘要

一种用以支持中小企业营运发展的信息供应方法以及系统，令一信息接收模块接收信息供应者上传的服务信息资料并储存在数据库中；令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行相关资料的整理；令一信息整合模块依据使用者输入的需求将该整理后且符合该需求的资料，通过一接口转换模块传送至使用者数据处理系统；最后，令一计费模块依据使用者使用系统的模式，执行服务费用的统计工作。 通过该使用本发明，能够提供个人工作室、住家办公室及中小企业的经营者及其从业人员使用者通过单一网站即可获得所需的信息服务。



ISSN1008-4274

知识产权出版社出版

1. 一种用以支持中小企业营运发展的信息供应方法，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应方法包括：

令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；

令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；

令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及

令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

2. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式所提供的网络协议地址及统一资源寻址器地址资料其中的一种。

3. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的一种。

4. 如权利要求 1 所述的方法，其特征在于，该信息资料的整理步骤还包括将同一信息供应者及不同信息供应者其中任一者提供的相同、相似及不同信息的其中任一种信息，加以分类、归纳及结合的数据处理过程。

5. 如权利要求 1 所述的方法，其特征在于，该信息整合形式可以是数据库信息的搜寻、信息服务提供者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

6. 如权利要求 1 所述的方法，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

7. 如权利要求 1 所述的方法，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

8. 如权利要求 1 所述的方法，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、

个人数字助理以及移动电话中的任一种。

9. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

10. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

11. 如权利要求 1 所述的方法，其特征在于，该数据库是一关系型数据库。

12. 如权利要求 1 所述的方法，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

13. 如权利要求 1 所述的方法，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

14. 一种用以支持中小企业营运发展的信息供应系统，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应系统包括：

一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；

一信息接收模块，用以接收信息提供者通过网络通讯系统提供的信息；

一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；

一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；

一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及

一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

15. 如权利要求 14 所述的系统，其特征在于，该信息供应者提供的信息可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式提供的网络协议地址及统一资源寻址器地址资料中的任一种。

16. 如权利要求 14 所述的系统，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的任一种。

17. 如权利要求 14 所述的系统，其特征在于，该信息整理模块是将同一信息供应者及不同信息供应者中任一者提供的相同、相似及不同的信息中的任一种信息，加以分类、归纳及结合的数据处理过程。

18. 如权利要求 14 所述的系统，其特征在于，该信息整合模块的整合形式可以是数据库信息的搜寻、信息服务者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

19. 如权利要求 14 所述的系统，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

20. 如权利要求 14 所述的系统，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

21. 如权利要求 14 所述的系统，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、个人数字助理以及移动电话中的任一种。

22. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

23. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

24. 如权利要求 14 所述的系统，其特征在于，该数据库是一关系型数据库。

25. 如权利要求 14 所述的系统，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

26. 如权利要求 14 所述的系统，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

用以支持中小企业营运发展的信息供应方法以及系统

技术领域

本发明是关于一种用以支持中小企业营运发展的信息供应方法以及系统，特别是关于一种整合信息以提供使用者通过单一网站获取该整合信息的信息供应方法与系统。

背景技术

随着电子信息科技的蓬勃发展，诸如个人计算机、笔记本型计算机、平板计算机、掌上型计算机、个人数字助理乃至移动电话等具有数据处理功能的电子装置或系统，其在功能上愈来愈强大，除单纯进行数据处理外，这些设备已经能够提供使用者上网浏览、信息的上传或下载、听音乐、编辑、播放影像信息等多元化的多媒体服务，来获取所需要的信息。另一方面由于有线及无线网络通讯技术的日益成熟，再加上这些电子装置或系统的体积愈来愈轻薄短小，便于使用者在行动中进行信息的取得。基于上述种种客观环境，使用者主观上也更乐意通过该具有网络连接与数据传输功能的电子装置或系统进行信息的搜寻及取得。

但是当愈来愈多的使用者不再通过报纸、杂志，甚至广播电视等传统的媒体来取得信息，而是选择通过具有实时性的网络通讯系统来取得所需的信息时，网络信息供应商势必要考虑如何能够充分利用网络通讯系统的特性，提供有别于传统媒体所能够提供的信息。

现有通过网络通讯系统提供使用者信息的方法不一般是以下方法：由使用者通过浏览器联接门户网站，输入要搜寻信息的关键词等搜寻条件，通过该门户网站提供的搜寻引擎进行与该关键词相符及/或近似的网页资料，由使用者通过输入网址或借由超级链接的方式与该网址进行联接，通过浏览器进行资料的浏览或传输。

这种现有的信息搜寻方法，对于缺乏网络搜寻经验或是搜寻条件等相关信息不是十分充分的使用者而言，信息的寻找、取得有时就如同大海捞针。此外，若使用者要同时搜寻许多具有实质关联性、却不具有形式关联性的网站时，上述的搜寻方式恐怕无法有效解决使用者的需要。此时，使用者仍须通过一次次的搜寻才有可能找到所需要的

信息。即令使用者已经搜寻到所有的相关信息，但若缺乏有效率的资料筛选，则所搜集到的信息对于使用者而言不但无法有效的解决自身的需要，有时反而会成为庞大的负担。

另一方面，使用者在通过付费网站获取信息方面，通常所采用的方法有固定费率制，也就是缴纳一定的费用取得在一定期间内无限次的使用权；储值制，也就是购买一定的点数，再从所使用的信息对应的点数中加以扣除。除上述两种以外，再一种方法就是依据服务提供商所开列的价格，通过信用卡或转帐的方式支付费用。上述服务费用的支付方法均是依据固定的服务价目表收费，并不能够将使用者登录或连接的等级、范围甚或是服务内容作为服务费率调整的依据。

综上所述，如何能够为使用者提供一套具有整合多元信息、并能够更合理地保证信息服务提供商与信息需求方利益的方法，是亟需解决的问题。

发明内容

为克服现有技术的缺点，本发明的主要目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一信息供应网站，让信息供应者通过该信息供应网站提供信息服务。

本发明的另一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率。

本发明的又一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易。

本发明的再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算。

本发明的又再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一接口转换机制，用以提供客户端的使用者可以借由不同类型的数据处理系统通过本发明获得信息服务。

为达成上述目的，本发明之用以支持中小企业营运发展的信息供应系统包括：一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；一信息接收模块，用

以接收信息提供者通过网络通讯系统提供的信息；一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

通过该用以支持中小企业营运发展的信息供应系统，进行信息供应的方法是：令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

与传统的信息供应方法以及系统比较，本发明通过整合信息供应者提供的信息机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息供应者通过该信息供应网站提供信息服务，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率；同时能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易，它所提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算及收取。本发明提供的接口转换机制，能够让客户端的使用者可以借由不同类型的数据处理系统通过本发明获得其所需的信息服务。

附图说明

图 1 为一应用架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的应用架构；

图 2 为一系统架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的系统架构；以及

图 3 为流程图，用以显示本发明之用以支持中小企业营运发展的信息供应方法的流程步骤。

具体实施方式

实施例

在以下实施例中，本发明用以支持中小企业营运发展的信息供应方法以及系统中所提供的信息包括文字资料、图像数据、影音资料以及其它无法由人类通过感官直接辨识的电磁记录资料，实际上能够通过本发明的用以支持中小企业营运发展的信息供应方法以及系统提供信息供应服务的，均适用于本发明的用以支持中小企业营运发展的信息供应方法以及系统。

请参阅图 1，如图所示，在本实施例中，本发明的用以支持中小企业营运发展的信息供应系统 100，是应用在现有的主从架构网络通讯系统 200 中，又该用以支持中小企业营运发展的信息供应系统 100 是建构在该网络通讯系统 200 的伺服端，用以提供具有网络连接功能的网络终端装置 300 及网络终端装置 400 的客户端使用者，借由一浏览器应用程序通过该网络通讯系统 200，与建构在该伺服端的用以支持中小企业营运发展的信息供应系统 100 相互连接，进行包括程序或资料的上传或下载、资料储存及数据管理等工作。其中，该网络通讯系统 200 可以是一国际互联网(Internet)、企业内部互联网(Intranet)或企业间互联网(Extranet)；该网络终端装置 300 及网络终端装置 400 可以是个人计算机(PC)、笔记本型计算机(NB)、工作站(Workstation)或其它具有数据处理功能的装置或系统；该浏览器应用程序可以是微软的网络探险家(Internet Explorer)或是网景的领航员(Netscape Navigator)等。上述的主从架构网络通讯系统 200、该网络终端装置及该浏览器应用程序均为现有的软、硬件架构，故在此不重复说明。

请参阅图 2，它显示了本发明的用以支持中小企业营运发展的信息供应系统 100 的系统架构，如图所示，该用以支持中小企业营运发展的信息供应系统 100 搭配至一网络服务器 210，该网络服务器 210 是提供该用以支持中小企业营运发展的信息供应系统 100，通过该网络通讯系统 200 与网络终端装置 300 及网络终端装置 400 相互连接，并提供该网络终端装置 300 及网络终端装置 400 响应使用者的指令或其它需求以进行资料存取之用。在本实施例中，该网络终端装置 300 及网络终端装置 400，是利用各该网络终端装置上的网络浏览器应用程序，如上述的微软的 IE 或是网景的 Navigator，通过网络通讯系统 200 经由该网络服务器 210，与该用以支持中小企业营运发展的信息供应系统 100 相互连接，以进行档案管理相关的工作。需特别说明的是，该用以支持中小企业营运发展的信息供应系统 100 还可以与一防火墙(Firewall)系统联接(未图标)，用以保护该用以支持中小企业营运发展的信息供应

系统 100。该用以支持中小企业营运发展的信息供应系统 100 包括：一数据库 220、一信息接收模块 230、一信息整理模块 240、一信息整合模块 250、一接口转换模块 260 以及一计费模块 270。

该数据库 220 是用来储存至少包括信息提供者所提供的信息、信息整合的相关资料、信息需求者的信息资料、信息需求者及信息供应者之间信息服务整合的资料以及服务费用等资料表。在本实施例中，为增加资料查询及检索的效率，该数据库 220 可以是一关系型数据库。其中，该信息提供者所提供的信息资料表，用来储存至少包括信息提供者所提供的文字资料、图像数据、影音资料以及其它能够以储存在该数据库的任何形式的资料等数据区位；该信息整合的相关资料表，用以储存至少包括信息类别资料、信息内容相互关系资料以及信息整合资料等数据区位；该信息需求者的信息资料表，用以储存至少包括使用者基本身分、使用者使用信息的权限以及使用者使用资源的记录等数据区位；该信息需求者及信息供应者之间信息服务整合的资料表，用以储存至少包括有信息服务整合类别资料以及信息服务整合历史记录资料等数据区位；该服务费用资料表，则用以储存至少包括信息供应者的收费模式、信息供应者所提供的信息被使用的计量以及信息供应者与该用以支持中小企业营运发展的信息供应系统管理者之间利润分配基础等数据区位。

通过这种关系型数据库的建立，当使用者输入上述任一种资料时，该用以支持中小企业营运发展的信息供应系统 100 即可快速的寻找到其对应的资料。需特别说明的是，上述的各该数据区位及其所属的资料表仅为举例而已，在实际情况下，其内容应更为明确详细。此外，各该数据区位的内容也有可能包括有其它的数据区位或是资料表，只是由于篇幅所限，以及为陈述上的简洁，仅显示与本发明的用以支持中小企业营运发展的信息供应方法以及系统有关的部分资料。另一方面，该关系型数据库的系统架构也有多种，应视使用者的需要加以建构，故也不再重复说明。

该信息接收模块 230 是用来接收信息提供者通过网络通讯系统 200 所提供的信息。在本实施例中，信息提供者可以是顾问咨询服务、专业规划服务、生活增值服务、知识增值服务、业务连接服务，甚至包括法人组织或政府机关的行政单位或对外服务窗口等任何自然人或法人构成的信息提供主体。该信息提供者可借由该网络终端装置通过该网络通讯系统 200，将提供的信息服务内容上传至该网络服务器 210，该信息接收模块 230 随即将接收到的信息服务相关资料加以储存至该

EX1060 - Page 929

数据库 220 中。

需特别说明的是，信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间应建立一资料传送的协议，如以特定的识别号码或文字定义的特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息相关资料时，则应依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段。

该信息整理模块 240 是对该信息接收模块 230 接受该信息提供者提供的信息内容，按照一定的规则进行整理。在本实施例中，由于信息提供者所提供的信息内容包罗万象，内容可能包括各个领域中不同层次的内容，可能是民间企业或是政府机关。但是通常一种业务的处理流程可能包括许多不同的信息供应者才能完成。如专利的申请，其流程可能包括寻找专业的专利事务所讨论专利申请的相关信息，委托其办理如专利说明书的撰写或专利申请程序的代办，当完成专利说明书的撰写后，还必须送交专利局进行专利审查，最后再经由相关的作业程序才能确定是否获得专利权。

该信息整理模块 240 能够将与专利申请相关的信息服务内容作一整理，当使用者欲搜寻与专利申请相关的信息服务时，即可获取一连串有用且相关的信息服务。在整理手段上，可以通过上述由信息供应者与用以支持中小企业营运发展的信息供应系统管理者之间的协议，借由特定的识别号码或文字加以分类，以将前阶段由民间专利事务所提供的服务，与后阶段由政府机关的专利局提供的行政程序服务等加以连接。也就是当信息供应者提供的信息通过该信息接收模块 230 储存至该数据库 220 时，该信息整理模块 240 能够将该特定相关的信息加以整理，并以特定的关键内容如“专利申请”等储存至该数据库 220 中的特定数据区位中，以供该用以支持中小企业营运发展的信息供应系统 100 进行资料的存取。

该信息整合模块 250 用来将该信息整理模块 240 所整理出的信息与使用者所提出的信息需求作一个连接互通。在本实施例中，当使用者借由网络终端装置通过该网络通讯系统 200，与建构有该用以支持中小企业营运发展的信息供应系统 100 的网站相互连接时，该网站会提供一信息服务相关的搜寻机制，如请求使用者输入使用者基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需的信息服务与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的相关信息服务相互结合。其结合方式包括提

EX1060 - Page 930

供使用者以超级链接的方式与该信息供应者相互连接、以提供如统一资源寻址器(URL)等网络资源的连接及/或提供如线上实时视频会议(Net-Meeting)等线上实时的信息请求及响应。

该接口转换模块 260 会依据不同客户端的网络终端装置提供符合该系统资料传送存取的资料规格。在本实施例中，该网络终端装置 300 及 400 并不限定为现有的个人计算机或笔记本型计算机，还可包括任何能够通过网络通讯系统 200 连接至架构有该用以支持中小企业营运发展的信息供应系统 100 网站的系统或装置，如移动电话所适用的无线应用软件协议(WAP)等其它网页浏览格式。该接口转换模块 260 是为使用不同资料浏览或存取协议的系统或装置提供转换接口，使其均可连接到架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，供使用不同浏览或存取协议的网络终端装置进行信息的搜寻或接受信息供应者所提供各种形式的信息服务。

该计费模块 270 是用以依据使用者使用资源服务的模式，计算其所应支付的服务费用。在本实施例中，该计费模块 270 除了依据信息供应者或该用以支持中小企业营运发展的信息供应系统 100 的管理者所确定的信息服务价目表，计算使用者所使用的信息服务内容所应支付的总服务费用外。还能够依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式及其历史记录，作为计算服务费用的标准。以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式、并加以记录，若该使用者与其中一家具有专利代理经验的信息供应者相互联系，并且双方进行了如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间服务与被服务的信息，若使用者再通过该网站与专利局进行信息需求与供应的服务时，该计费模块 270 仍会记录他们之间的有关信息。通过上述追踪记录使用者的行为模式、并加以记录的方式，能够以依据使用者利用该网站的不同层次(Level)作为计算服务费用的标准。

请参阅图 3，它显示通过上述的用以支持中小企业营运发展的信息供应系统 100，在实施该用以支持中小企业营运发展的信息供应方法的步骤是。

在步骤 S301 中，令该信息接收模块 230 接收信息供应者上传的服务信息资料并储存在该数据库 220 中。通过该信息接收模块 230 能够接收资料供应者所传送的信息资料，以超级链接的方式所提供的网络

EX1060 - Page 931

协议地址及／或统一资源寻址器地址等资料。

承前所述，该信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间得建立一资料传送的协议，如以特定的识别号码或文字定义特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息等相关资料时，则能够依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段中。

在本实施例中，若一专利事务所欲通过该用以支持中小企业营运发展的信息供应系统 100 作为一专利信息供应者，则其能够借由网络终端装置通过该网络通讯系统 200，将其所能提供的信息资料传送至该网络服务器 210，其中该传送的资料包括文字或影像信息资料，以超级链接方式所提供的网络协议地址及／或统一资源寻址器地址等资料。此外，还包括特定的识别号码或文字，如“0001”与“专利服务”等，该信息接收模块 230 在该网络服务器 210 接收到上述的资料时，随即将该资料储存至该数据库 220 中符合该识别号码“0001”与识别文字“专利服务”的数据区位中，接着进行步骤 S302。

在步骤 S302 中，令该信息整理模块 240 将该服务信息资料依据信息供应者所提供的内容进行相关资料的归纳、整理。其过程包括将同一信息供应者或不同信息供应者所提供的相同、相似或不同的信息加以分类、归纳或结合等。

承前所述，除该专利服务的信息供应者能够传送相关信息资料外，设架构有该用以支持中小企业营运发展的信息供应系统 100 的网站还能够与政府机关、如上述的专利局等相互合作，提供诸如线上专利申请或咨询等服务。由于一专利的申请流程可能需通过包括专利事务所与专利局等信息服务提供者的协助才能顺利完成。则该信息整理模块 240 则应将专利事务所及专利局所提供的信息服务作一信息归类，当使用者登录架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，且欲请求该网站提供“专利申请”的信息服务时，则能够轻易的搜寻到上述经归纳后的该专利事务所及专利局所提供的信息服务，接着进行步骤 S303。

在步骤 S303 中，令一信息整合模块 250 依据使用者输入的需求，将该整理后且符合该需求的资料通过一接口转换模块 260 传送至客户端网络终端装置。其整合的模式包括数据库 220 信息的搜寻、信息服务提供者网络资源的连接及/或提供线上实时的信息请求及响应等。

承前所述，当有“专利服务”信息需求的使用者登录该网站后，该网站能够提供使用者一输入该使用者相关信息的功能，如要输入使

EX1060 - Page 932

用者的基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字，如识别号码“0001”与识别文字“专利服务”等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需要的“专利服务”的相关信息服务，与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的、经整合后的该专利事务所及专利局所提供的信息服务相互结合。

在本实施例中，使用者进行数据库 220 中相关资料的搜寻、与该专利事务所进行网络视频会议及上述假设的专利局线上的专利申请作业流程等信息服务，接着进行步骤 S304。

在步骤 S304 中，令一计费模块 270 依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式，执行服务费用的统计工作。它是依据使用者使用信息的模式，计算所需支付的费用以及信息供应者之间的利润分配。

承前所述，在使用者通过上述的信息整合模块 250 取得该用以支持中小企业营运发展的信息供应系统 100 所提供的服务信息的过程中，该计费模块 270 会记录使用者与该信息供应者整合的信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其信息。

在本实施例中，以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式并加以记录，若该使用者与其中一具有专利代理经验的信息供应者相互联系，双方进行如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间的相关信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其有关信息。通过上述的信息记录，该计费模块 270 能够依据所记录该使用者连接该网站的层次、连接的时间及/或信息服务的内容等，计算出相对应的服务费用，其中，该服务费用的计算基准应视实际情况加以制定。此外，该计费模块 270 还能够依据信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者对于信息提供的利润分配基准，进行利润分配的计算。

综上所述，本发明之用以支持中小企业营运发展的信息供应方法以及系统，能够通过整合信息服务供应者所提供的信息服务供应机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息服务供应者通过该信息供应网站提供信息服务。

本发明的用以支持中小企业营运发展的信息供应方法以及系统能够协助个人工作室、住家办公室及中小企业的经营者及其从业人员，在接取订单、增创营收、善用外部资源、进行委外服务、增加经营弹性、减少聘雇人员及办公室空间的需求、节省营运成本、降低创业门槛等方面提供帮助，进而达到解决失业问题及调整产业结构的目的。

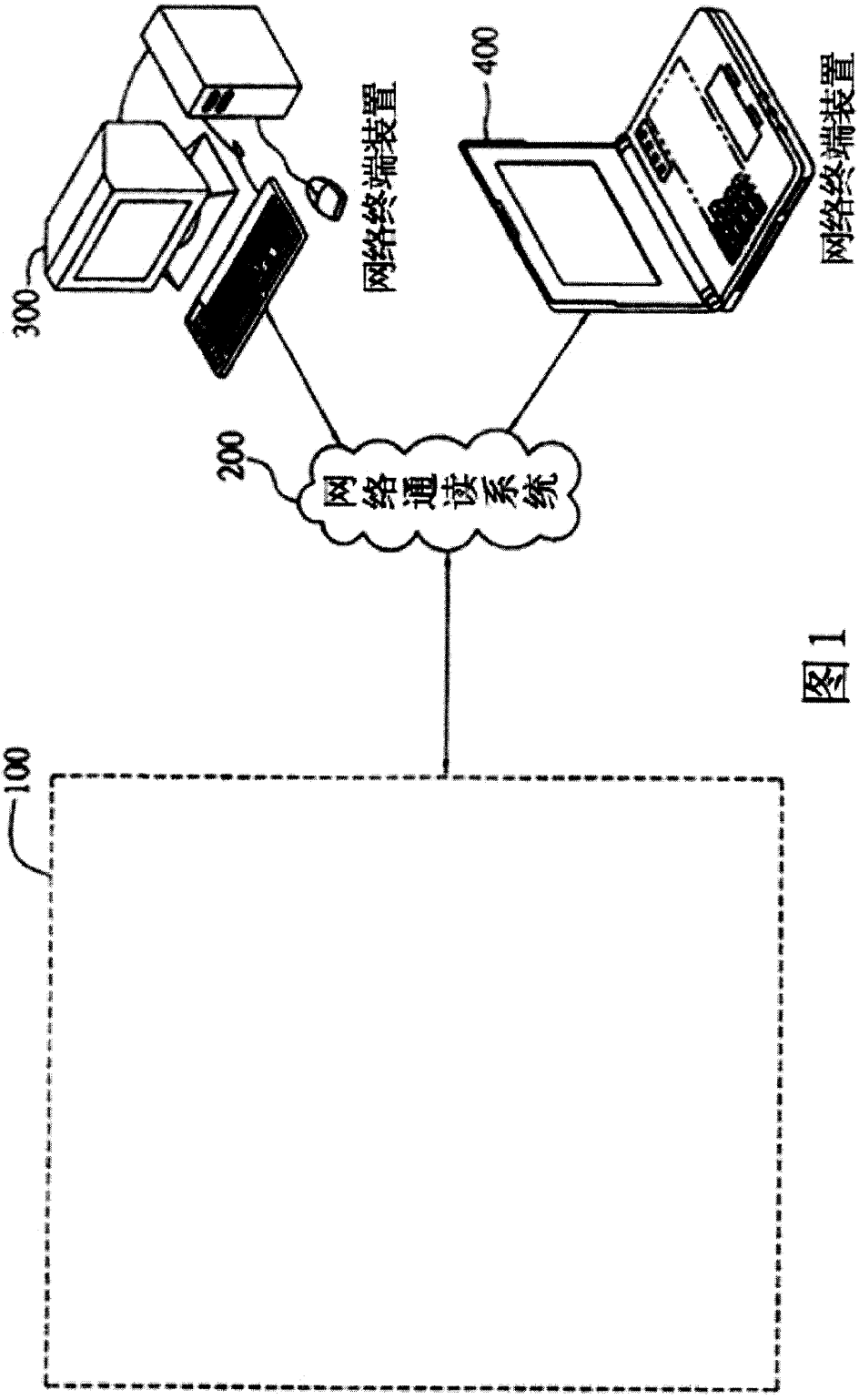


图 1

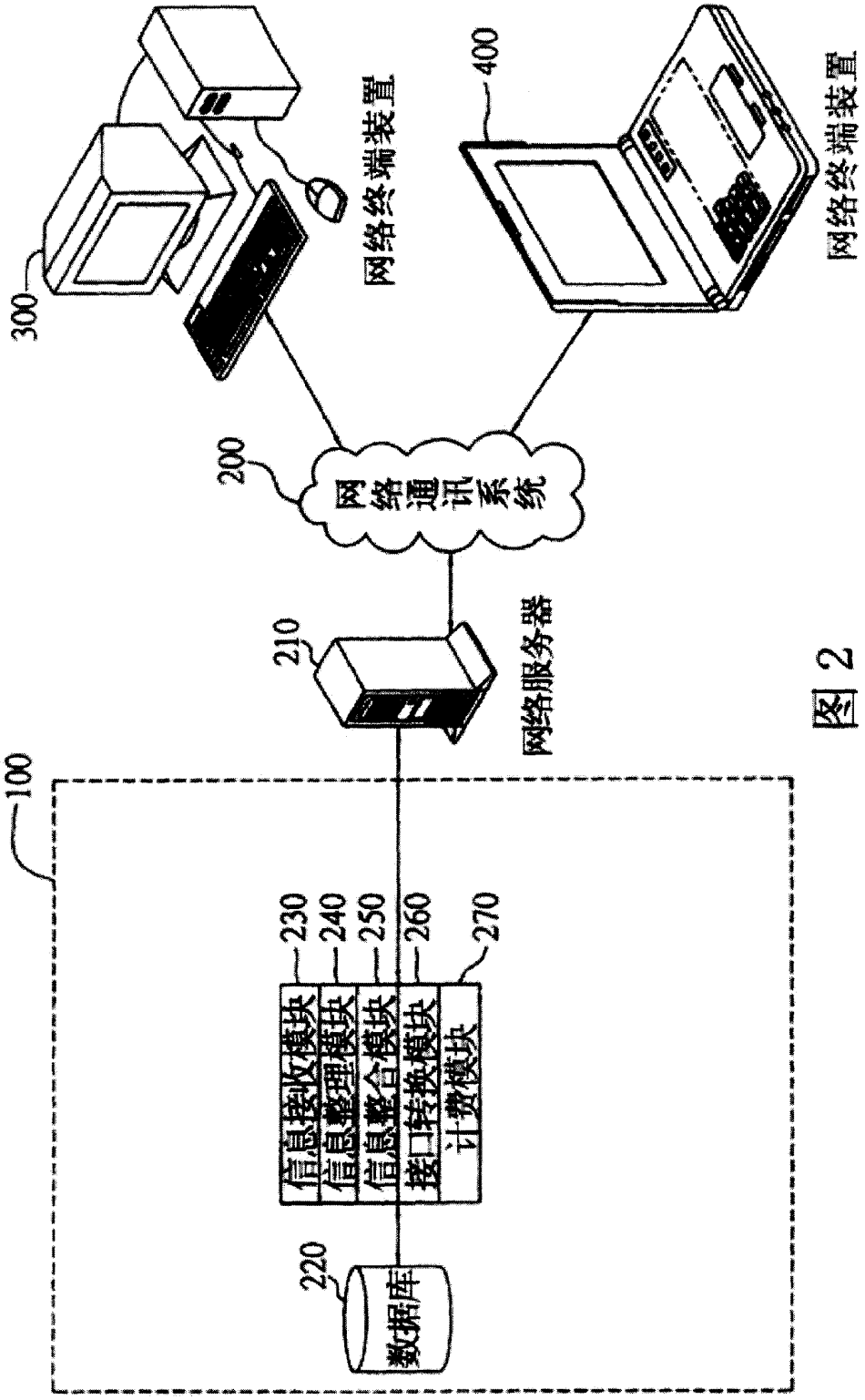

300
网络终端装置
400
网络终端装置
200
网络通讯系统
210
网络服务器
100
230
240
250
260
270
信息接收模块
信息整理模块
信息整合模块
接口转换模块
计费模块
220
数据库

图 2

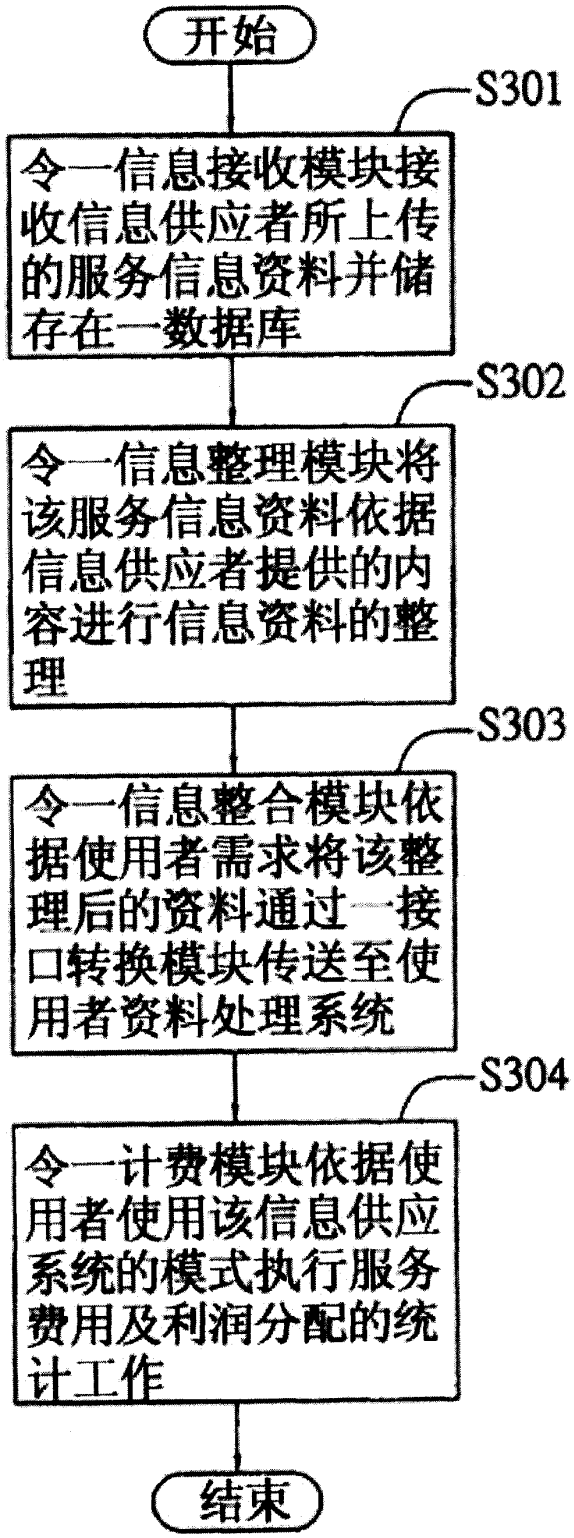

开始
S301
令一信息接收模块接收信息供应者所上传的服务信息资料并储存在一数据库
S302
令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行信息资料的整理
S303
令一信息整合模块依据使用者需求将该整理后的资料通过一接口转换模块传送至使用者资料处理系统
S304
令一计费模块依据使用者使用该信息供应系统的模式执行服务费用及利润分配的统计工作
结束

图 3

Apple

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Method and system for providing information for supporting operation development of small-medium enterprises

CN 1508734 A

Publication number	CN1508734 A
Publication type	Application
Application number	CN 02156671
Publication date	Jun 30, 2004
Filing date	Dec 13, 2002
Priority date	Dec 13, 2002
Inventors	温世仁, 吴鸿琪
Applicant	华人创意股份有限公司
Export Citation	BiBTeX, EndNote, RefMan

Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention is a kind of information supplying method and the system for supporting small and medium-sided enterprise development. A information receiving model receives the service information data uploaded by supplier and stores them in the databank; a information arranging model carries on the arrangement of relative data according to the content supplied by the supplier; a information integrating model transmits the proper data to the user data processing system through a interface converting model, finally, a charge calculating model calculates the charge according to the mode used by the user.

DESCRIPTION translated from Chinese

Supply methods to support the development of SMEs as well as operating system

Technical Field

The present invention relates to an operation to support the development of SMEs information provision method and system, especially with regard to an integrated information to provide users to access information through a single Web site that integrated information provision method and system.

Background

With the rapid development of electronic information technology, such as personal computers, notebook computers, tablet computers, palmtop computers, personal digital assistants and even mobile phones and other electronic devices or systems having a data processing function, its increasingly powerful in function, In addition to simple data processing, these devices have been able to provide users with Internet browsing, upload or download information, music, editing and playback of multimedia video information and other diversified services to get the information they need. On the other hand due to the wired and wireless network communications technologies become more sophisticated, the volume plus these electronic devices or systems increasingly compact size, ease of access to information in the user performs actions. Based on all these objective circumstances, users are more willing subjective electronic device or system that has a network connection and data transmission capabilities to search and access to information.

But when more and more users are no longer to obtain information through traditional media, newspapers, magazines and even radio and television, choosing instead to obtain the necessary information through the network communication system with real-time, online information provider bound to consider how to take full advantage of the characteristics of the network communications system, providing different from traditional media to provide information.

Existing methods provide user information through the network communication system is not generally the following methods: by the user through a browser connection portal, enter search keywords and other search criteria information

CLAIMS (26) translated from Chinese

An information provision method to support SME Business Development, to provide users with a data processing system by means of the information required to obtain services through a network communication system, wherein the means for support of the SME Business Supply method development include: make an information receiving module receives the information service provider information uploaded and stored in a database; make an information consolidation module based on the content of the service information provided by the information provider of information materials finishing; make an information integration module based on the needs of the user input, the finishing and meet the needs of data through a user interface conversion module is transferred to the data processing system; and to make a billing module according to the user to use the use to support the development of SMEs operating mode of information supply system, the implementation of service fees and profit distribution statistics work.

2. The method according to claim 1, characterized in that the information service provider information may be uploaded text data, image data, audio data, image data, network protocol address provided by hyperlinks and unified address information resource addressing one of them.

3. The method according to claim 1, characterized in that the service information This information can be uploaded provider of business intelligence, business opportunities, professional services, professional planning, business connections, administrative procedures and value-added services in one .

4. The method according to claim 1, characterized in that the finishing step also includes the same information will be different from the same information provider and wherein any one of the information provider provides, any of which is similar to and different information information, classify, summarize and combine the data processing.

5. The method according to claim 1, characterized in that the integration of information and forms can be connected to provide search and information services provider of database information online real-time network resource information request and response in

provided through the portal, and the search engine Keywords consistent and / or similar web information input by the user through the website or by way of hyperlinks connecting with the site, browse or transfer data through the browser.

This existing information search method, for lack of experience, or search Web search and related information is not very full of users, the information search, obtain sometimes like needle in a haystack. In addition, if the user to simultaneously search a number of substantive relevance, is not associated with a form of site, said search means could not be effectively addressed the needs of users. In this case, the user must still search through time and time again possible to find the information they need. And even if the user has to find all the relevant information, but if the lack of effective screening information, then the information gathered for the user not only can not effectively solve their own needs, sometimes it will become a huge burden.

On the other hand, users get to information through pay sites, typically used a fixed rate system, which is to pay a fee to obtain unlimited times within a certain period the right to use; stored value system, which is to buy a certain points, and then be deducted from the corresponding point information used in the. In addition to the two outside, then one approach is based on the service provider listed price, pay by credit card or debit way. The method of payment of the above services are based on a fixed fee service price list, the user is not able to log on or connect the level, the scope of services or even service rates as the basis for the adjustment.

In summary, how can we provide users with a set of integrated pluralistic information and the ability to more reasonable assurance that the information service provider and information needs of Fangli Yi approach is needed to solve problems.

DISCLOSURE

To overcome the disadvantages of the prior art, the main object of the present invention is to provide a support operation for the development of SMEs information provision method and system capable of providing an information provider website information provider to provide information so that the information supplied by website services.

Another object of the present invention is to provide a support operation for the development of SMEs information provision method and system that can provide information on the information provider for effective integration, improve the efficiency of users to find the information.

A further object of the present invention is to provide a support for the development of the SME Business information provision method and system, which can provide a user through an information service integration mechanisms and information provider of information services deals.

A further object of the present invention is to provide a support operation for the development of SMEs information provision method and system, which can provide an accounting mechanism to allow information providers to use information service based on user model to calculate the cost of services .

Again object of the present invention is to provide an operation to support the development of SMEs information provision method and system, which can provide an interface conversion mechanism for providing client user can borrow from the different types of data processing systems The present invention is to obtain information services.

To achieve the above objects, the present invention in order to support the development of SMEs operating information supply system comprising: a database for storing information providers including at least the information provided, the relevant data and information collated, the information needs of those information, information and data as well as those who need services cost any one.

The method according to claim 6, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

7. The method according to claim 1, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

8. The method according to claim 1, characterized in that the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

9. The method according to claim 1, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

10. The method according to claim 1, characterized in that the network communication system may be a wired communication systems and wireless communication system of any one.

11. The method according to claim 1, characterized in that the database is a relational database.

12. The method according to claim 1, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

13. The method according to claim 1, characterized in that the user may be operators and their employees personal studio, home office and SME any one.

14. A method for supporting the development of the SME Business information supply system to provide users with borrowed by a data processing system to obtain the required information and services through a network communication system, wherein the means for support of the SME Business development of information supply system comprising: a database for storing at least include the information provided by those who provide information, relevant data and information collated, the information needs of those information, information needs and information providers who integrate data and information services Service cost information; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module receives information about the content of the information provided by the provider; an information integration module to the information needs of information consolidation module collated information submitted by the user to make a connection interworking; an interface converter module for different clients according to the data processing system to provide data transmission in line with the system, access specifications; and a billing module for computing services they need to pay the costs, as well as information provider and distribution of profits to support the development of SMEs operating information providing system administrators use of resources based on user-service model.

15. The system according to claim 14, characterized in that the information provider provides information may be text data, image data, audio data, image data, addresses in hyperlinks network protocol and provide uniform resource addressing address data in either.

16. The system of claim 14, wherein the service information provider uploaded the information may be business intelligence, business

data integration between information provider of information services; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module an information integration module to the information needs of information consolidation module collated information and user make a connection the proposed exchange;; an interface converter module for different customers based on the content of the information provided by the information provider end data processing system provides data transmission in line with the system specifications access; and a billing module for computing services they need to pay the costs, as well as information service providers based on user patterns and the use of resources to support SME Business Development Supply system administrator profit distribution.

The method by which to support the development of SMEs operating information supply system for the supply of information is: make an information receiving module receives information on the service provider information uploaded and stored in a database; an information consolidation module makes the service information provided in accordance with the content of the information provider to collate information; and make an information integration module based on the needs of the user input, the finishing and meet the needs of data transmission via an interface conversion module to the user data processing systems; and to make a billing module according to the user to use the development of SMEs to support operations information supply system mode, performing a service fee of statistical work and the distribution of profits.

Compared with the traditional supply methods and information systems, information mechanism of the present invention to provide by integrating information provider, the information service integration mechanisms, billing mechanism and interface conversion mechanism, through information supplied by a website to provide information by the information provider Supply website provides information services, information providers can provide information for effective integration, improve the efficiency of users to find the information required; at the same time be able to provide users with information and services through an integrated mechanism and information provider of information services transaction, it provides a billing mechanism, so that information providers use information service based on user patterns, calculate and charge for the services. Interface conversion mechanism of the present invention provides, allows the client user can borrow from the different types of data processing systems and services to get the information they need by the present invention.

Brief Description

Figure 1 is a block diagram of the application architecture, application architecture to show support for the operation of the present invention the development of SMEs information supply system; Figure 2 is a block diagram of the system architecture, the present invention is used to show support for SMEs operation and development of information systems architecture supply system; and Figure 3 is a flow chart, the process steps for information provision method of the present invention to support the development of SMEs operating display.

opportunities, professional services, professional planning, business connections, administrative procedures and any value-added services species.

17. The system according to claim 14, characterized in that the module is the same as information of the same sort of information providers and different information provider provided by any one, any one of similar and different information in the information, classify, summarize and combine the data processing.

18. The system according to claim 14, characterized in that the form of the integration of information integration module may search a database of information, and providing on-line information services connected by network resources and real-time information request in response to any one of species.

19. The system of claim 14, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

20. The system of claim 14, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

21. The system of claim 14, wherein the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

22. The system of claim 14 claim, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

23. The system of claim 14 claim, wherein the network communication system may be wired communication systems and wireless communications systems in any one.

24. The system according to claim 14, characterized in that the database is a relational database.

25. The system according to claim 14, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

26. The system of claim 14 claim, characterized in that the user may be operators and their employees personal studio, home office and small and medium enterprises of any kind.

DETAILED DESCRIPTION

Example In the following examples, the present invention is to support the development of SMEs operating information supply method and an information system is provided including text data, image data, audio and video data as well as by other human senses can not be recorded by the direct identification of electromagnetic data actually able to provide information supply services through information provision method and system to support the operation and development of SMEs in the present invention are useful in the present invention, an information provision method and system to support the operation and development of SMEs.

See Figure 1, as shown in this embodiment, in order to support the operation and development of SMEs in the information supply system 100 of the invention, is used in the existing master-slave architecture network communication system 200, versus a to support the operation and development of SMEs in the information supply system 100 is constructed on the

servo end of the network communication system 200 for providing network terminal device has a network connection function client user network terminal device 300 and 400, made by a browser application 200, 100 interconnected with the construction of the servo end to support the operation and development of SMEs in the information supply system via the network communication system for including a program or data upload or download, data storage and data management. Wherein the network communication system 200 may be a Internet (Internet), intranet (Intranet) or enterprises Internet (Extranet); the network terminal device 300 and a network terminal device 400 may be a personal computer (PC), notebook computer (NB), workstation (Workstation) or other device or system with data processing capabilities; the browser application may be Microsoft's Internet Explorer (Internet Explorer) or Netscape Navigator (Netscape Navigator) and so on. Said main are existing software and hardware architecture from architecture network communication system 200, the network terminal device and the browser application, so this will not be repeated.

See Figure 2, which shows the operation to support the development of SMEs information systems architecture supply system 100 of the invention, as shown in the operation to support the development of SMEs with information supply system 100 to a network server 210, the network server 210 is provided to support the operation and development of SMEs in the information supply system 100 through the network communication system 200 and the network terminal device 300 and a network terminal device 400 connected to each other, and to provide the network terminal device 300 and network the terminal apparatus 400 in response to user commands or other requirements for use of data access. In this embodiment, the network terminal device 300 and a network terminal device 400 is using a web browser application on each of the network terminal device, such as Microsoft's IE or Netscape Navigator as described above, through the network communication system 200 210, 100 connected to each other via the network server to support the development of SMEs operating information supply system for records management-related work. In particular, and it noted that the operation to support the development of SMEs information supply system 100 also may be a firewall (Firewall) system connections (not shown) to protect the operation to support the development of SMEs information supply system 100 . The operation to support the development of SMEs information supply system 100 includes: a database 220, an information receiving module 230, an information consolidation module 240, an information integration module 250, an interface conversion module 260, and a billing module 270.

The database is used to store at least 220, including information provided by the information provided, the information related to the integration of data, information, information needs of those, who between information needs and information providers of information services and integrated information service expense sheet . In the present embodiment, in order to increase the efficiency of data query and retrieval, the database 220 may be a relational database. Among them, the information sheet provided by the information provider, used to store text data including at least provided information provider, image data, video and audio information and other data can be stored in any form of the databases and other data area bits; information integration related information table for storing information including at least category, information content and information integration relationship information data such as location information; the information needs of those information table for storing includes at least the basic user identity, user permission to use information and recording user data such as resource use location; the information needs of persons between information providers and information services to integrate the data sheet, including an information service for storing at least types of information integration and data information services into history data such as location; the service cost data tables, including at least information provider to store the charging mode, metering and information provider information provider the information provided is used to support the operation and development of SMEs Supply Profit distribution between basic data such as location system administrator.

Through this relationship database when a user enters any of the above information, which is used to support 100 to quickly find the information corresponding to its SME Business Development Supply System. In particular, and it noted that all the data and information on the location of the above table belongs only way of example only, in reality, its contents should be more clearly detailed. In addition, the contents of each bit of the data area may also include other data or information table location, but due to limited space, as well as a succinct statement on the show only to the present invention supports SME Business Development Supply methods and some of the information system related. On the other hand, the relational database system architecture also has many, depending on the needs of users should be construction, it is also not repeated.

The message receiving module 230 is used to receive network information provider through the communication system 200 to provide information. In this embodiment, the information provider may be consulting services, professional planning services, life value-added services, value-added knowledge services, business connectivity services, and even any natural or legal person or legal entity government administrative units or foreign service window, etc. Information provided constituted body. This information is provided by the network may, by the terminal device 200 via the network communication system, the information services to be provided to upload to the network server 210, the information receiving module 230 then the received information service related information to be saved to the database 220.

Need of special note is the establishment between information providers and managers to support the operation and development of the SME information supply system 100 a data transfer protocol, the particular type of information, such as specific identification number or text definition When 230 receives information related information having the identification

number or character of the information receiving module should be based on the identification number or text to the relevant information stored in the database 220 corresponding information storage field.

This information consolidation module 240 is receiving module 230 accepts the information content of the information providers, in accordance with certain rules finishing. In this embodiment, since the information content provided by the information provider all-inclusive, the content may include various fields at different levels of content, may be private companies or government agencies. But usually a business process flow may include a number of different information provider to complete. As a patent application, the process may include professional patent search firm to discuss patent applications related information for the execution of programs written or patent application as the patent specification of the charge d'affaires, after the completion of drafting patent specification must also be sent to the Patent patent examination Board, and finally by the relevant operating procedures in order to determine whether the franchise.

This information consolidation module 240 can be related applications and patent information services as a consolidation, when the user wants to search and patent applications related to information services, you can get a series of useful and related information services. On finishing means, said by agreement by the information provider and to support the development of SMEs operating information supply system between managers, to be borrowed by a particular identification number or text classification, to the front stage by private patent matters services provided, to be connected with the later stages of the administrative service provided by government agencies and other offices. That is when the information provider of information provided by the information receiving module 230 to 220 stored in the database, the information sorting module 240 can be related to the specific information received, and in particular the key elements as "patent application" and storage to the database 220 of location-specific data in order for the operation to support the development of SMEs information supply system 100 access data.

The information integration module 250 to the information needs of information consolidation module 240 to sort out information and users are asked to make a connection exchange. In this embodiment, when the user by the network terminal device 200 via the network communication systems, and construction has to support the operation and development of SMEs in the information supply system 100 is connected to each other at the site, the site will provide an information service relevant search mechanism, such as requesting the user to enter a personal identification data basic user identity, user permission to use the information, as well as specific information search key identification number, or text and so on, through the information integration module search function 250, that can The information requirements are needed for information services and related information services to support the operation and development of the SME information supply system 100 can offer combined with each other. Its combination of methods include providing users with hyperlinks connected to each other and the information provider to provide a unified resource addressing connector device (URL) and other network resources, and / or provide such as on-line real-time video conferencing (Net-Meeting) and other online real-time information requests and responses.

The interface conversion module 260 will be based on network unit to provide different clients in line with the specifications of the information system data transmission access. In this embodiment, the network terminal device 300 and 400 is not limited to existing personal computer or notebook computer, it may also include any communication system 200 connected via a network to have the infrastructure to support SME Business Development system or device information supply system 100 sites, such as mobile phones applies wireless applications protocol (WAP) and other browser formats. The interface conversion module 260 is to use a different browser or system or device data access protocol conversion interface is provided, it can be connected to architecture has to support the operation and development of SMEs in the information supply system 100 sites for different use Browse or access protocol network terminal devices to search for information or receive information providers are providing various forms of information services.

The billing module 270 is for the use of resources based on user mode services, computing services, they should pay the costs. In this embodiment, the billing module 270, in conformity with the information provider or manager to support the development of SMEs operating information providing system 100 of the determined price list information services, information services used to calculate the user Total service charges to be paid outside. It can also be based on the user to use the operation to support the development of SMEs information supply system model and its history of 100, as a standard computing service costs. In the aforementioned "patent application" process, for example, when a user from searching for relevant patent office or patent offices of information, the billing module 270 begins recording the user to use the site of use, click on the number or download files The amount of data and other behavior patterns, and recorded, if the user with one of the information provider has experienced patent agents interrelated, and both sides were as real-time online information and consulting service, the billing module 270 immediately recorded use between those and the information provider services and information to be served, if the user then the demand and supply of information services through the site with the Patent Office, the billing module 270 will still record information between them. It is recorded by the above-mentioned track record of user behavior patterns and the way the user can take advantage of different levels according to the website (Level) as a standard to calculate the cost of services.

See Figure 3, which shows through the above-mentioned operation to support the development of SMEs information supply system 100, the procedures described in the information supply method to support the operation and development

of SMEs in yes.

In step S301, so that the information service information receiving module 230 receives information provider uploaded and stored in the database 220. Information received by the information provider module 230 is capable of receiving data transmitted, the network protocol address provided by way of hyperlinks and / or uniform resource addressing address and other information.

Cheng said before, the information provider to support the operation and development of SMEs in the information supply system was set up a data transfer protocol between the 100 managers, such as a specific identification number or text to define specific types of information, when The information receiving module 230 receives the information and other related information with that identification number or text, it is possible according to the identification numbers or letters to the relevant information stored in the database 220 corresponding information storage field.

In this embodiment, if a patent office by the desire to support the operation and development of SMEs in the information supply system 100 as a provider of patent information, it can borrow from the network terminal device 200 via the network communication system, which It can provide information sent to the network server 210, wherein the transmission of data, including text or image information, network protocol addresses to hyperlinks provided and / or uniform resource addressing address and other information. Moreover, further comprising a specific identification number or text, such as "0001" and "Patent services", the information receiving module 230 at the network server 210 receives the information, then the information stored in the database 220 to meet the The identification number "0001" and recognized character "Patent Services" data location, followed by step S302.

In step S302, so that the information received from the service module 240 on the basis of information provided by the content information provider summarize the relevant information and organize. The process includes the same information the same provider or different information provided by suppliers, similar or different information to be classified, or a combination of induction and the like.

Cheng said before, in addition to the patent information service providers can communicate the relevant information, provided the architecture has to support the development of SMEs operating site information providing system 100 also with government agencies, such as the above-mentioned patent offices and other mutual cooperate in providing such as online and other patent applications or consulting services. Because of a patent application process may include assistance and other needs by the patent office and patent office information service providers in order to successfully complete. Then this information should be finishing module 240 information services Patent Office and the Patent Office provided information to make a classification, when the user logs architecture has to support the operation and development of the SME information supply system 100 sites, and wants When requesting the site to provide "patent application" of information services, it is possible to easily find the information and services that the patent office and summarized by the Patent Office after the above offer, followed by step S303.

In step S303, so that an information integration module 250 in accordance with the needs of the user input, the finishing and meet the needs of data through an interface conversion module 260 is transmitted to the client network terminal devices. Its integrated model includes a connection search, information services provider database 220 information network resources and / or provide real-time online information request and response and so on.

Before the bearing, when the "Patent Services" users log on to the information needs of the site, the site can provide users with an input of the user information related functions, such as the identity of the user to enter basic user usage information permissions and other personally identifiable information, as well as specific information search key identification number or character, such as the identification number "0001" and recognition of the word "patent services" through which information integration module search function 250, that person can demand the required information "patent" of related information services, and information services to support the operation and development of the SME information supply system 100 can be provided by the Patent Office and the Patent Office provided consolidated combined with each other.

In this embodiment, the user searches the database 220 relevant information, and the patent office video conferencing and network of offices above assumptions online patent application processes and other information services, followed by step S304.

In step S304, so that a billing module 270 according to the user to use this information to support the development of SMEs operating mode supply system 100, performing a service fee of statistics. It is based on the user using the information mode, calculate the required fees paid profits and the distribution of information between providers.

The front bearing, when the user 250 acquires service information to support the operation and development of the SME information supply system 100 is provided by the above process of information integration module, the billing module 270 will record the information supply Aggregated information, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will still record its information.

In this embodiment, the above-mentioned "patent application" process, for example, when users search for relevant patent office or patent offices of information from the billing module 270 begins recording the user to use the site of use, point When the selected frequency or amount of data downloaded file to record patterns of behavior and, if the user and the information provider which patent agency experience having contact with each other, the two sides as online real-time information and consulting services, the billing module 270 then record the relevant information and the user information between suppliers, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will continue to record their information. By the above information recording, the billing module 270 can connect the user based on the recorded level of the site, the connection time and / or information services and other content, calculate the corresponding service charges, which the service fees calculation basis should be developed as practicable. In addition, the billing module 270 can also provide the basis for information and managers to support the operation and development of SMEs in the information supply system 100 is provided baseline information for profit distribution, the calculated distribution of profits.

In summary, the present invention in order to support the development of the SME Business information provision method and system capable of information services through the integration of information mechanism provided by the service provider, information service integration mechanisms, billing mechanism and interface conversion mechanism , by the information supplied by a website to provide information and services provider to provide information services through the information provider sites.

Information provision method and system to support the operation and development of SMEs in the present invention can assist individuals studio, home office and SME managers and employees, in the next to take orders, to create revenue, use of external resources, conduct outsourcing services and increase business flexibility, reduce demand and office space, hiring staff, to save operating costs, reduce business barriers, such as providing help, and then to solve the unemployment problem and the purpose of the adjustment of industrial structure.

LEGAL EVENTS

Date	Code	Event	Description
Jun 30, 2004	C06	Publication	
Sep 8, 2004	C10	Request of examination as to substance	
Mar 21, 2007	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2688553 A1 2008/12/04

(21) 2 688 553

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2008/06/01
(87) Date publication PCT/PCT Publication Date: 2008/12/04
(85) Entrée phase nationale/National Entry: 2009/11/26
(86) N° demande PCT/PCT Application No.: IL 2008/000740
(87) N° publication PCT/PCT Publication No.: 2008/146296
(30) Priorité/Priority: 2007/05/30 (US60/940,882)

(51) Cl.Int./Int.Cl. *G06F 21/24* (2006.01)
(71) Demandeur/Applicant:
YOGGIE SECURITY SYSTEMS, LTD., IL

(72) Inventeur/Inventor:
TOUBOUL, SHLOMO, IL

(74) Agent: HICKS INTELLECTUAL PROPERTY LAW

(54) Titre : SYSTEME ET PROCEDE POUR FOURNIR A UN DISPOSITIF UNE PROTECTION PARE-FEU POUR RESEAU ET ORDINATEUR AVEC ISOLEMENT D'ADRESSE DYNAMIQUE

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

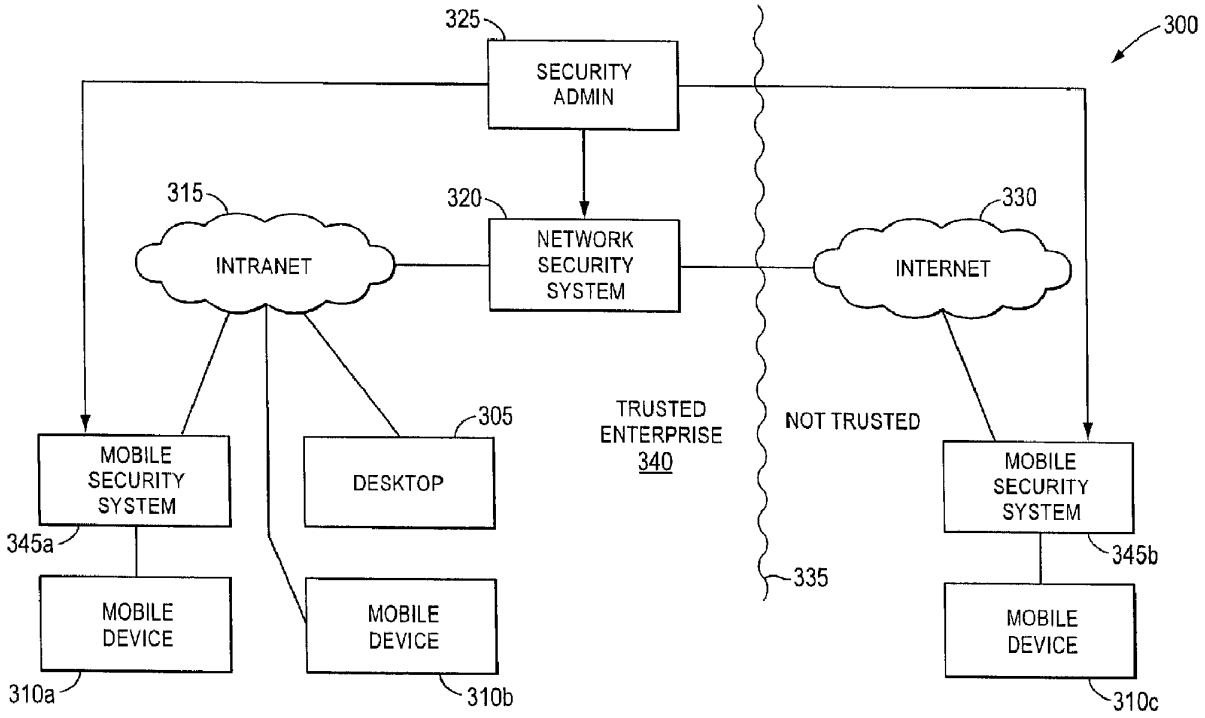


FIG. 3

(57) Abrégé/Abstract:
A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a

(21) 2 688 553

(13) A1

(57) **Abrégé(suite)/Abstract(continued)**:
network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2008 (04.12.2008)

PCT

(10) International Publication Number
WO 2008/146296 A2

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/IL2008/000740

(22) International Filing Date: 1 June 2008 (01.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/940,882 30 May 2007 (30.05.2007) US

(71) Applicant *(for all designated States except US)*: **YOGGIE SECURITY SYSTEMS, LTD.** [IL/IL]; 42870 Beit Halevy (IL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **TOUBOUL, Shlomo** [IL/IL]; 6 Main Street, 42945 Kefar Haim (IL).

(74) Agent: **SANFORD T. COLB & CO.**; P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

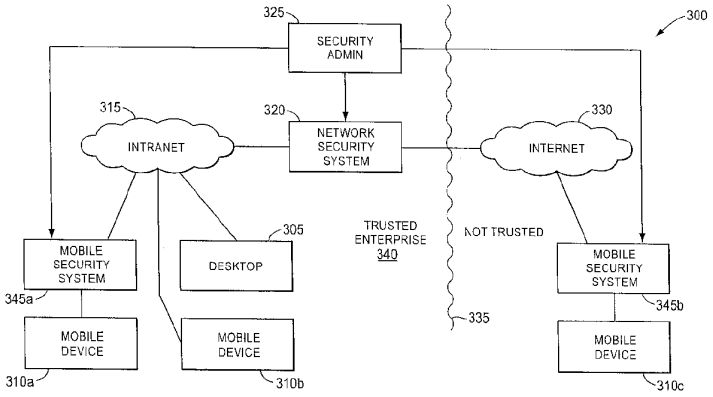


FIG. 3

(57) Abstract: A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

WO 2008/146296 A2

SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

PRIORITY CLAIM

This application claims benefit of U.S. provisional patent application serial no. 60/940,882, which is hereby incorporated by reference.

TECHNICAL FIELD

This invention relates generally to computer security, and more particularly provides a system and method for providing data and device security between external and host devices.

BACKGROUND

The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as "viruses," "spyware," "adware," "worms," "Trojan horses," and other malicious code.

To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise's network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, antivirus, antispyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses

its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM's Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

Figure 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise's intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise's gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet 130 via the network security system 120, both have two lines of defense (namely, the network security system 120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

Figure 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafé, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security

Conference in New York on December 7-8, 2005. However, no complete solutions were presented.

Similarly, when a host device is connected to an external device such as a USB flash drive, iPod, external hard drive, etc., both devices are vulnerable to receipt of malicious code or transfer of private data. Figure 11 illustrates an example prior art data exchange system 1100 that includes a host computer (host) 1105 and an external device 1110. The host 1105 includes a external device (ED) port 1115, such as a USB port, for receiving the external device 1110. The host 1105 also includes ED drivers 1120 for performing enumeration and enabling communications between the external device 1110 and the host 1105. The external device 1110 includes an ED plug, such as a USB plug, for communicating with the ED port 1115. Both of the host 1105 and external device 1110 are vulnerable to receipt of malicious code or transfer of private data.

Accordingly, there is a need for a system and method of providing security to host and external devices.

SUMMARY

In one embodiment, the present invention provides a computer comprising an application associated with an application address; a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network; a network address translation engine configured to translate between the application address and a public address; and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The network address translation engine may be part of the driver or part of a firewall. The firewall may be located on a mobile security system. The network address translation engine may be configured to use Dynamic Host Configuration Protocol. The computer may be configured to send data packets identifying the application to a firewall, and the firewall may be configured to handle both network-level security and application-level security.

In one embodiment, the present invention provides a system comprising a network interface; a firewall in communication with the network interface configured to handle both network-level security and application-level security; and a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall. Each data may be is associated with one of the one or more applications. Each data packet may comprise data identifying the application associated with the data packet. The firewall may be configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network. The network interface may be configured to receive incoming data from an external network, and to route the incoming data to the firewall. Each application may be associated with at least one address. The firewall may be configured to dynamically isolate the address from an external network. The firewall may be configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a personal computer of processing incoming data associated with a public address, the method comprising receiving the data from an external network; translating the public address into an internal address associated with an application; analyzing the data for malicious code; and routing the data to the application if the data does not comprise malicious code. The analyzing step may comprise analyzing the data for malicious code at both the network level and the application level. The translating step may use Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a computer of processing outgoing data, the method comprising receiving outgoing data from an application, the application being associated with an internal address; translating the internal address into a public address; and routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network. The translating step may use Dynamic Host Configuration Protocol. The method may further comprise configuring the outgoing data into one or more data packets; associating each of the one or more data packets with the application; and embedding application-identifying data in each of the one or more data packets. The method may further comprise creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets, wherein the routing step comprises routing the one or more data packet subsets to the external network.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art network system in a first state.

Figure 2 is a block diagram of a prior art network system in a second state.

Figure 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

Figure 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

Figure 5 is a block diagram illustrating details of the mobile security system in accordance with an embodiment of the present invention.

Figure 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Window's embodiment.

Figures 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

Figure 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

Figure 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

Figures 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

Figure 11 is a block diagram illustrating a prior art data exchange system.

Figure 12 is a block diagram illustrating a secure data exchange system, in accordance with an embodiment of the present invention.

Figure 13 is a block diagram illustrating details of a security device, in accordance with an embodiment of the present invention.

Figure 14 is a block diagram illustrating details of a security system, in accordance with an embodiment of the present invention.

Figure 15 is a block diagram illustrating a secure data exchange system, in accordance with another embodiment of the present invention.

Figure 16 is a flowchart illustrating a method of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention.

Figure 17 is a block diagram illustrating a prior art network system having a hardware-based firewall.

Figure 18 is a block diagram illustrating a prior art network system having a software-based firewall.

Figure 19 is a block diagram illustrating a network system that performs dynamic address isolation, in accordance with an embodiment of the present invention.

Figure 20 is a block diagram illustrating a prior art network system having separate network and personal firewalls.

Figure 21 is a block diagram of a network system comprising a hybrid firewall in accordance with an embodiment of the present invention.

Figure 22 is a block diagram illustrating a network system comprising a hybrid firewall and configured according to the embodiment of the present invention shown in Figure 10A.

Figure 23 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 24 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

Figure 25 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 26 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

Figure 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network 340 but in this embodiment are coupled to the intranet 315 without an intervening mobile security system 345 such as mobile security system 345b. The intranet 315 is coupled via a network security system 320 (which may be part of the enterprise's gateway) to the untrusted internet 330. Accordingly, the first mobile device 310a, the second mobile device 310b and the desktop 305 access the untrusted internet 330 via the network security system 320. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device 310c is currently outside the enterprise network 340 and is coupled via a mobile security system 345b to the untrusted internet 330. The third mobile device 310 may be in use by an employee of the trusted enterprise 340 who is currently on travel. A security administrator 325 manages the mobile security system 345a, the mobile security system 345b, and the network

security system 320 to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise 340.

Demarcation 335 divides the trusted enterprise 340 and the untrusted publicly accessible internet 330. Each of mobile device 310a, 310b and 310c may be referred to generically as mobile device 310, although they need not be identical. Each mobile security system 345a and 345b may be referred to generically as mobile security system 345, although they need not be identical.

As shown, although the mobile device 310c has traveled outside the trusted enterprise 340, the mobile device 310c connects to the untrusted internet 330 via the mobile security system 345b and thus retains two lines of defense (namely, the mobile security system 345b and the security software resident on the device itself). In this embodiment, the mobile security system 345 effectively acts as a mobile internet gateway on behalf of the mobile device 310c. In an embodiment, the mobile security system 345 may be a device dedicated to network security. In an embodiment, each mobile security system 345 may support multiple mobile devices 310, and possibly only registered mobile devices 310, e.g., those belonging to enterprise 340.

Each mobile security system 345 (e.g., 345a, 345b) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system 345 may be based on a hardened embedded Linux 2.6.

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security

systems 345 accordingly. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

The mobile security system 345 may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device. These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in Figure 8. Operating on the lower OSI layers and doing TCP/IP packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7th OSI layer (Application – HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system 345 may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system 345 may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system 345:

- Firewall and VPN – including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.
- Optional web accelerator and bandwidth/cache management based on Squid.
- IDS/IPS – Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

- Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandamay, may be offered for additional subscription fees.
- Malicious Content Detection – on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.
- URL Categorization Filtering – based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device 345 may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

FIG. 4 is a block diagram illustrating details of an example computer system 400, of which each desktop 305, mobile device 310, network security system 320, mobile security system 345, and security administrator 325 may be an instance. Computer system 400 includes a processor 405, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 410. The computer system 400 further includes an input device 415 such as a keyboard or mouse, an output device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are illustrated as different units, the data storage device 430 and memory 435 can be parts of the same unit, distributed units, virtual memory, etc.

The data storage device 430 and/or memory 435 may store an operating system 440 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs 445. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

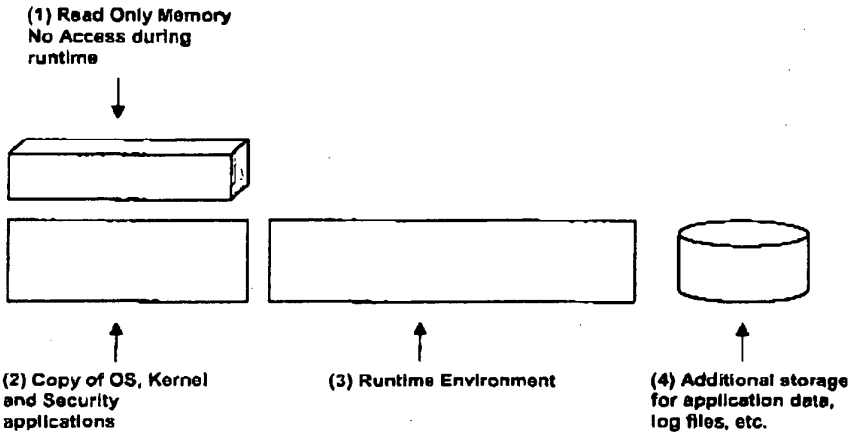
One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader 450 such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus 410 for reading a computer-readable storage medium (CRSM) 455 such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system 400 may receive programs and/or data via the CRSM reader 450. Further, it will be appreciated that the term "memory" herein is intended to cover all data storage media whether permanent or temporary.

Figure 5 is a block diagram illustrating details of the mobile security system 345 in accordance with an embodiment of the present invention. Mobile security system 345 includes adapters/ports/drivers 505, memory 510, a processor 515, a preboot flash/ROM memory module 520 storing a secure version of the mobile security system's operating system and other applications, network connection module 525, security engines 530, security policies 535, security data 540, remote management module 550, distribution module 555, and backup module 560. Although these modules are illustrated as within the mobile security system 345, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator 325 or on third-party systems in communication with the mobile security system 345. The mobile security system 345 may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system 345 may be incorporated within the mobile device 310.

The adapters/ports/drivers 505 include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection data ports on the mobile security system 345. In one embodiment, the adapters/ports/drivers 505 may be capable of connection to multiple devices 310 to provide network security to the multiple devices 310.

Memory 510 and processor 515 execute the operating system and applications on the mobile security system 345. In this example, the preboot flash 520 stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash 520 into memory 510 for execution. Since the operating system and applications are stored in the preboot flash 520, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash 520 are not corruptible. Should the copy of the operating system and applications in memory 510 be corrupted, e.g., by malicious code, the operating system and applications may be reloaded into the memory 510 from the preboot flash 520, e.g., upon restart. Although described as stored within the preboot flash 520, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

Memory (including memory 510 and preboot flash 520) on the mobile security system 345 may be divided into zones as follows:



Upon each "hard" restart, the boot loader (resident at area 1) of the mobile security system 345 copies the kernel and security applications (a fresh unchanged copy) from area 1 to 2. This causes a clean version of the OS and applications to be loaded into area 2 each time. That way, if a special mobile security system 345 attack is developed, the attack will be unable to infect the

system, since the OS and applications are precluded from accessing memory area 1 during runtime. Further, any attack that does reach memory 510 will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system 345 automatically upon infection detection.

The network connection module 525 enables network connection, e.g., to the internet 330 or the intranet 315 via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device 310 wishes to connect to the internet 330 via a WiFi connection, the adapters/ports/drivers 505 may be connected to the PCI port, USB port or PCMCIA port of the mobile device 310, and the network connection module 525 of the mobile security system 345 may include a WiFi network interface card for connecting to wireless access points. Using the network connection module 425, the mobile security system 345 may communicate with the network as a secure gateway for the mobile device 310. Other connection architectures are described in Figures 10A-10C.

The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.

To provide a higher security level provided by antivirus and antispyware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use

sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their internet experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the

source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in Figure 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally

within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540

while connecting to the security administrator 325 and via an encrypted and authenticated connection.

The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in Figure 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to Figure 7.

The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

Each mobile security system 345 may obtain its routing table with security information updates, periodically, at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

The distribution module 555 may enable rapid updates as shown in Figure 9. Currently, all commercial antivirus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in Figure 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

Figure 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345

also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the antivirus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which

relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in Figure 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

- Email Security and Anti-spam – implementation of mail relay on mobile security systems 345 (including the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.
- Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another

mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

- Information Vault – Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.)
- Safe Skype and Other IM – implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispyware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if its not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 540), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345 OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

Figures 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In Figure 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In Figure 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In Figure 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security

system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

Figure 12 is a block diagram illustrating a secure data exchange system 1200, in accordance with an embodiment of the present invention. The secure data exchange system 1200 includes a host computer (host) 1205 coupled via a security device 1210 to an external device 1110. The host 1205 may include a laptop, desktop, PDA, mobile phone, or other processor-based device. The external device 1110 may be any external device with memory such as a USB drive, external hard drive, PDA, music player, cell phone, etc. The security device 1210 is communicatively coupled to the host 1205 via an ED port 1225 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and an ED plug 1230 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The external device 1110 is communicatively coupled to the security device 1210 via an ED port 1235 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and ED plug 1120 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The connector type of the ED port 1225 and ED plug 1230 combination may be different that the connector type of the ED port 1235 and ED plug 1120 combination. In one embodiment, all ports 1225/1235 and plugs 1230/1120 are USB. Although the plugs 1120/1230 are illustrated as male and ports 1225/1235 are shown as female, one skilled in the art will recognize that the opposite is possible (plugs 1120/1230 may be female and ports 1225/1235 may be male).

The host 1205 includes ED drivers 1220 for performing enumeration and enabling communication with the security device 1210. Similarly, the security device 1210 includes ED drivers 1245 for performing enumeration and enabling communication with the external device 1110.

In one embodiment, the security device 1210 includes a programmable hardware appliance capable of enforcing security policies to protect against malicious code such as viruses,

spyware, adware, Trojan Horses, etc. and to protect against transfer of private data. In one embodiment, the security device 1210 is configured to protect both the host 1205 and the external device 1215. In one embodiment, the security device 1210 is configured to protect only one of the external device 1110 or the host 1205. Additional details of the security device 1210 are provided with reference to Figures 13 and 14.

Figure 13 is a block diagram illustrating details of the security device 1210, in accordance with an embodiment of the present invention. The security device 1210 include a processor 1305, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 1315. The security device 1210 further includes an ED plug 1230, an ED port 1235, a communications interface 1310, storage 1320 such as an EEPROM, and memory 1325 such as Random-Access Memory (RAM) or Read Only Memory (ROM), each coupled to the communications channel 1315. The communications interface 1310 may be coupled to a network such as the internet. One skilled in the art will recognize that, although the storage 1320 and memory 1325 are illustrated as different units, the data storage device 1320 and memory 1325 can be parts of the same unit, distributed units, virtual memory, etc. The term "memory" herein is intended to cover all data storage media whether permanent or temporary. One skilled in the art will recognize that the security device 1210 may include additional components, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc.

As shown, memory 1325 stores an operating system 1330 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, Unix OS, Linux OS, etc. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology. The memory 1325 also stores ED drivers 1245 and a security system 1335. The ED drivers 1245 may include standard drivers for standard external devices 1110 and proprietary drivers for proprietary external devices 1110. The ED drivers 1245 may be transferred onto the

memory 1325 via ED plug 1230. The security system 1335 includes code for enforcing security policies on data transfer actions between the host 1205 and external device 1110.

Figure 14 is a block diagram illustrating details of a security system 1335, in accordance with an embodiment of the present invention. The security system 1335 includes a security manager 1405, security engines 1410, security policies 1415, and security data 1420.

In one embodiment, the security manager 1405 includes code for performing enumeration, namely, to identify the external device 1110 or external device 1110 type and to identify the corresponding ED driver 1245 capable of establishing communication between the security device 1210 and the external device 1110. The security manager 1405 also includes code to control execution of the various security engines 1410 based on the security policies 1415 and security data 1420 to evaluate data transfer requests or other device requests. Further, the security manager 1405 includes code to communicate with the host 1205, which will be the source of the data transfer and/or other requests.

In one embodiment, the security engines 1410 includes code for securing the transfer of data between the host 1205 and the external device 1110 based on the security policies 1415 and security data 1420. The security engines 1410 may include firewalls, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. The security engines 1410 may also include data privacy modules to enforce data privacy policies 1415. Each security engine 1410 may have dedicated security policies 1415 and security data 1420 to indicate which procedures, URLs, system calls, content, ID, etc. the data requested for transfer may contain or whether the data requested for transfer is considered nontransferable (or nontransferable without additional security measure such as a password and ID).

To provide a higher security level, the security engines 1410 may implement content analysis and risk assessment algorithms. In one embodiment, a security engine 1410 assigns a weight and rank for every transfer object based on its type, complexity, richness in abilities, source, etc. The security engine 1410 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 1410 may assign weight to objects

based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 1410 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 1410 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

Thus, upon receiving a data transfer and/or other request from the host 1205, the security manager 1405 will launch the appropriate security engines 1410 based on the security policies 1415. For example, the security policies 1415 may be configured not to allow specific ActiveX controls to be loaded from the host 1205 onto the external device 1110. The security policies 1415 may be configured not to allow data transfer from private folders on the host 1205 to the external device 1110. The security manager 1405 will launch the appropriate security engines 1410 to assure that these example security policies 1415 are met. Further, the security engines 1410 may use security data 1420, which may include definition files of malicious ActiveX controls, locations of private folders, etc.

Although not shown, the security system 1335 may include additional components such as the preboot flash 520 with OS and applications, the remote management module 550, the distribution module 555, and the backup module 560 discussed above with reference to Figure 5. Other components are also possible.

Figure 15 is a block diagram illustrating a secure data exchange system 1500, in accordance with another embodiment of the present invention. The secure data exchange system 1500 includes a security device 1505 communicatively coupled to the host 1520 via an ED plug 1515 on the security device 1505 and a first ED port 1525 on the host 1520. The secure data exchange system 1500 also includes an external device 1110 communicatively coupled to the host 1520 via the ED plug 1120 on the external device 1110 and a second ED port 1535 on the host 1520.

Because the external device 1110 is not directly coupled to the security device 1505, the security device 1505 is not physically intercepting the data transfer requests between the external device 1110 and the host 1520. Accordingly, in this embodiment, the host 1520 includes a redirect driver 1530, which is configured to redirect data transfer requests between the external device 1110 and the host 1520 regardless of data transfer direction. In one embodiment, the security device 1505 may be configured to protect only one of the external device 1110 or the host 1520. Further, in one embodiment, the security device 1505 does not contain any ED drivers, e.g., ED drivers 1245.

In one embodiment, if the security device 1505 is not coupled to the host 1520, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110. In one embodiment, the host 1520 is configured not to communicate with the external device 1110 until the security device 1505 is coupled to the host 1520. In one embodiment, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110 only if additional security measures are taken, such as receipt of a password and ID, or until the security device 1505 is coupled to the host 1520.

In one embodiment, the host 1520 may conduct enumeration of the security device 1505 upon connection of the security device 1505 to the ED port 1525. Upon identifying the security device 1505 or security device 1505 type, the host 1520 may initiate the redirect driver 1530 to redirect all data transfer requests or other external device 1110 requests from all other ED ports 1535 to the security device 1505. In one embodiment, the redirect driver 1530 only accepts data transfer requests from the security device 1505, which presents the requests of the external device 1110 as a proxy. In one embodiment, the redirect driver 1530 performs data transfer requests received from the external device 1110 only after the security device 1505 has conducted its check and given its authorization. Other protocols are also possible.

Figure 16 is a flowchart illustrating a method 1600 of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention. The method 1600 begins in step 1605 with the security device 1505 being connected to the first ED

port 1525 of the host 1520. The external device 1110 in step 1610 is connected to the second ED port 1535 of the host 1520. The host 1505 in step 1615 performs enumeration techniques to identify the security device 1505 and the external device 1110 and to install the appropriate drivers 1530/1540 to enable communication with the security device 1505 and the external device 1110. The redirect driver 1530 in step 1620 receives a data transfer request from either the host 1505 to the external device 1110 or from the external device 1110 to the host 1505. The redirect driver 1530 in step 1625 redirects the data transfer request to the security device 1505, which in step 1630 enforces its security policies (antivirus, antispyware, anti-adware, data privacy, etc.) on the data transfer request. The security device 1505 in step 1635 determines whether the data transfer request passes the security policies. If so, then the security device 1505 in step 1640 authorizes the data transfer request and the host 1520 in step 1645 performs the data transfer request. If not, then the security device 1505 in step 1650 rejects the data transfer request. Method 1600 then ends.

It will be appreciated that, in one embodiment, the security device 1210/1505 may be implemented as part of the host 1205/1520, e.g., within the housing of the host 1205/1520 and/or as a security procedure executed by the host 1205/1520.

Dynamic Isolation

Figure 17 shows a prior art network system 1700 having a hardware-based firewall. The network system 1700 includes internal computers 1705a and 1705b, a first network interface card (NIC) 1710, a hardware-based firewall 1715 that performs network address translation (NAT), a second NIC 1720, an external network 1725 (such as the Internet), and external computers 1730a and 1730b.

The firewall 1715 is a hardware-based firewall, such as Check Point FW-1 or Cisco PIX. The firewall uses two different network ports (the first NIC 1720 and the second NIC 1720) to separate and isolate the internal computers 1705a and 1705b from the external network 1720. The firewall 1715 uses network address translation (NAT) to translate the Internet Protocol (IP) address of the internal computer 1705a (denoted as IP address x) and the IP address of the

internal computer 1705b (denoted as IP address y) into a public IP address z, thus hiding the IP addresses of the internal computers 1705a and 1705b. The firewall 1715 performs a similar translation on the Media Access Control (MAC) addresses of the internal computers 1705a and 1705b.

The network system 1700 provides a higher level of security than PC software-based firewalls (such as Microsoft Windows Personal Firewall and Check Point ZoneAlarm) running on the internal computers 1705a and 1705b themselves, since PC software-based firewalls do not hide the IP and MAC addresses of the internal computers.

Figure 18 shows a prior art network system 1800 having a software-based firewall. The network system 1800 includes an external network 1805 (such as the Internet), one or more NICs 1810 (denoted as 1810a, 1810b, ... 1810n), a Network Driver Interface Specification (NDIS) driver 1815 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1820 (such as MINIPort in the Microsoft Windows operating system), a software-based firewall 1825, an operating system 1830, and one or more applications 1835 (denoted as 1835a, 1835b, ... 1835m). The operating system 1830 contains a TCP/IP protocol suite 1840.

In operation, the intermediate driver 1820 directs traffic arriving from the NICs 1810 and NDIS driver 1815 to the software-based firewall 1825. The software-based firewall 1825 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to the operating system 1830.

The network system 1800 does not use a hardware-based firewall. Only one of the NICs 1810 needs to be used at any given time. However, the IP and MAC addresses of the NICs 1810 (which are visible to the external network 1805) are the same IP and MAC addresses that are viewed and used by the applications 1835 (i.e., there is no address isolation between the applications 1835 and the external network 1805).

Figure 19 shows a network system 1900 that performs dynamic address isolation, in accordance with an embodiment of the present invention. The network system 1900 includes an external network 1905 (such as the Internet), one or more NICs 1910 (denoted as 1910a, 1910b, ... 1910n), an NDIS driver 1915 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1920, a software-based or hardware-based firewall 1925, an operating system 1930, and one or more applications 1935 (denoted as 1935a, 1935b, ... 1935m). The operating system 1930 contains the TCP/IP protocol suite 1940. The intermediate driver 1920 includes a NAT engine 1945, which contains a translations table for IP and MAC addresses.

The NICs 1910, NDIS driver 1915, intermediate driver 1920, firewall 1925, operating system 1930, and applications 1935 may be installed in a mobile device 310. The firewall 1925 may be an external firewall 1925 connected to the intermediate driver 1920 by a Universal Serial Bus (USB) connection, a wireless connection, or another network wire connection. For example, the firewall 1925 may be part of the mobile security system 345.

In operation, the intermediate driver 1920 receives all data packets arriving from the NICs 1910 and NDIS driver 1915, and routes each data packet to the NAT engine 1945. The NAT engine 1945 uses Dynamic Host Configuration Protocol (DHCP) to dynamically isolate the IP addresses of the applications 1935 from the external network 1905. As shown in Figure 19, the dynamic NAT engine 1945 translates the IP address of the application 1935 (IP address x) to a different IP address (IP address z) while interfacing with the NIC, and translates the IP address z back to the IP address x when sending data to the operating system 1930. Thus, the intermediate driver 1920 provides IP address z to the external network 1905, while isolating IP address x from the external network. The NAT engine 1945 performs a similar translation on MAC addresses, if necessary. As shown, the NAT engine 1945 is part of the intermediate driver 1920. However, one skilled in the art will recognize that the NAT engine 1945 may be located elsewhere, e.g., on the mobile security system 345, part of the firewall 1925, etc.

After the NAT engine 1945 translates the IP address, the intermediate driver 1920 directs each data packet to the firewall 1925. The firewall 1925 decides what to do with each data

packet (allow, deny, or reject) and permits only the allowed data packets to proceed to the operating system 1930. The intermediate driver 1920 receives each allowed data packet back from the firewall 1925 and routes each allowed data packet to an application 1935.

For outgoing data packets, the intermediate driver 1920 receives each data packet from the application 1935 and routes each data packet to the NAT engine 1945. The NAT engine 1945 translates the IP and/or MAC address associated with the data packet as described above. The intermediate driver 1920 then receives each data packet (containing the translated IP and/or MAC address) back from the NAT engine 1945 and routes each data packet to the external network 1905.

In this way, the network system 1900 is able to isolate the IP and MAC addresses of internal computers/applications from the external network 1905, while not requiring the use of a hardware-based firewall or more than one NIC. Network isolation and separation is achieved even if the firewall lacks more than one NIC.

Thus, a connection between a mobile security system 345 and a mobile device 310 may be implemented while using the principles of NAT and DHCP, so that end-user applications running on the mobile device 310 will "see" protected virtual IP and MAC addresses, while devices connected to the external network see different physical IP and MAC addresses. The present invention provides similar protection and IP hiding that a hardware-based firewall having two network ports (internal and external) provides to a mobile device, but without the need to use a hardware-based firewall and two or more network ports.

Figure 23 is a flowchart of a method 2300 of routing a data communication from an external network (such as the external network 1905) to an application (such as application 1935), in accordance with an embodiment of the present invention. In step 2305, a NIC (such as NIC 1910) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2310, the data communication is routed to an intermediate driver (such as the intermediate driver 1920),

which in turn routes the data communication to a NAT engine (such as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses.

In step 2315, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2320, the intermediate driver routes the data communication to a firewall (such as the firewall 1925). In step 2325, the firewall analyzes the data communication for malicious code. In step 2330, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2300 proceeds to step 2335. In step 2335, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2300 then ends.

If the data communication was not found to contain malicious code, then the method 2300 proceeds to step 2340. In step 2340, the firewall allows the data communication. The intermediate driver receives the data communication back from the firewall and routes the data communication to the application. The method 2300 then ends.

Figure 24 is a flowchart of a method 2400 of routing a data communication from an application (such as application 1935) to an external network (such as the external network 1905), in accordance with an embodiment of the present invention. In step 2405, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system (such as the operating system 1930).

In step 2410, the data communication is routed to an intermediate driver (such as the intermediate driver 1920), which in turn routes the data communication to a NAT engine (such

as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses. In step 2415, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2420, the internal driver routes the data communication to the external network via a NIC (such as NIC 1910). The method 2400 then ends.

Hybrid Firewall

Figure 20 shows a prior art network system 2000 having separate network and personal firewalls. The network system 2000 includes an external network 2005 (such as the Internet), a network firewall 2010, and personal computers 2015 (denoted as 2015a, 2015b, etc.). The network firewall 2010 may reside on an external device or computer. The network firewall 2010 comprises a first NIC 2020, a NAT gateway 2025 and a second NIC 2030. Each personal computer 2015 comprises a personal firewall 2035 (denoted as 2035a, 2035b, etc.) and an application 2040 (denoted as 2040a, 2040b, etc.).

In operation, the network firewall 2010 uses the NAT gateway 2025 to translate the IP address of the personal computer 2015a (denoted as IP address x) and the IP address of the personal computer 2015b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers 2105. The network firewall 2010 performs a similar translation on the MAC addresses of the personal computers 2015. The network firewall 2010 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the network firewall 2010 is earlier in the network than the personal firewall 2035, it can stop malicious code before it enters the system 2000. However, because the network firewall 2010 is application insensitive and at a lower layer of the information stack, its processes for malicious code detection are limited.

The personal firewall 2035 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the personal firewall 2035 is application sensitive and at a higher layer of the information stack, its processes for malicious code detection can be more thorough and focused.

Figure 21 shows a network system 2100 comprising a hybrid firewall 2110 in accordance with an embodiment of the present invention. The network system 2100 includes an external network 2105 (such as the Internet), a hybrid network/personal firewall 2110, and personal computers 2115 (denoted as 2115a, 2115b, etc.).

The hybrid firewall 2110 may reside on an external device or computer. In other embodiments, the hybrid firewall 2110 may reside on the mobile security system 345, shown in Figures 10A-10C. The hybrid firewall 2110 comprises a first NIC 2120, a NAT engine 2125 and a second NIC 2130.

Each personal computer 2115 comprises an agent 2135 (denoted as 2135a, 2135b, etc.) and one or more applications 2140 (denoted as 2140a, 2140b, etc.). As shown in Figure 21, the network system 2100 comprises only two personal computers 2115, but in other embodiments the network system 2100 may comprise more than two personal computers.

In operation, the hybrid firewall 2110 uses the NAT engine 2125, which contains a translations table for IP and MAC addresses, to translate the IP address of the personal computer 2115a (denoted as IP address x) and the IP address of the personal computer 2115b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers. The network firewall 2110 performs a similar translation on the MAC addresses of the personal computers 2115.

The hybrid firewall 210 is capable of performing both the network firewall and personal firewall security measures. Because the hybrid firewall 2010 is at the same level as the traditional network firewall 2035, it can stop malicious code before it enters the system 2100.

Further, because the hybrid firewall 2110 is application sensitive, the hybrid firewall 2110 can perform the processes of the traditional personal firewall 2035.

To enable the hybrid firewall 2110 to be application sensitive, the agents 2135 send packets of data to the hybrid firewall 2110, each packet comprising data identifying the application 2140 associated with the packet. Because each packet comprises data identifying the application 2140 that is associated with the packet, the hybrid firewall 2110 can act as a personal firewall 2035 to handle application-level security. Then, the hybrid firewall 2110 can transmit a subset of the data packets, by extracting at least the application-identifying data, to the external network 2105.

Figure 22 shows a network system 2200 comprising a hybrid firewall 2210 and configured according to the embodiment of the present invention shown in Figure 10A. The network system 2200 includes an external network 2205 (such as the Internet), a hybrid network/personal firewall 2210, and a mobile device 2215.

The hybrid firewall 2210 may reside on an external device in a pocket-size, handheld-size, keychain-size, or possibly smaller housing. The hybrid firewall 2210 comprises an ED plug 2245 (such as a USB plug) for communicating with an ED port 2230 (such as a USB port) contained within the mobile device 2215. The hybrid firewall 2210 also comprises a NAT engine 2225. In other embodiments, the hybrid firewall 2210 may be installed in the mobile device 2215, or connected to the mobile device 2215 by a wireless or another network wire connection.

The mobile device 2215 comprises a NIC 220, the ED port 2230, an agent 2235, one or more applications 2240, and an intermediate driver 2250 (such as MINIPort in the Microsoft Windows operating system). As shown in Figure 22, the network system 2200 comprises only one mobile device 2215 and hybrid firewall 2210, but in other embodiments the network system 2200 may comprise more than one mobile device and hybrid firewall.

In operation, the intermediate driver 2250 directs traffic arriving from the NIC 2220 to the hybrid firewall 2210 via the ED port 2230 and ED plug 2245. The hybrid firewall 2210 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to an application 2240.

The hybrid firewall 2210 uses the NAT engine 2225, which contains a translations table for IP and MAC addresses, to translate the IP address of the mobile device 2215 into a public IP address, and thus hide the IP address of the mobile device 2215. The hybrid firewall 2210 performs a similar translation on the MAC address of the mobile device 2215.

The application 2240 can send packets of data via the ED port 2230 and ED plug 2235 to the hybrid firewall 2210 for transmission to the external network 2205. The agent 2235 associates data identifying the application 2240 with the packets of data that are sent to the hybrid firewall 2210. Each packet thus comprises data identifying the application 2240 associated with the packet. Because each packet comprises data identifying the application 2240 associated with the packet, the hybrid firewall 2210 can act as a personal firewall to handle application security.

Figure 25 is a flowchart of a method 2500 of routing a data communication from an external network (such as the external network 2105 or 2205) to an application (such as application 2140 or 2240), in accordance with an embodiment of the present invention. In step 2505, a NIC (such as NIC 2120 or 2220) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2510, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2515, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the

data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2520, the hybrid firewall associates the data communication with an application. The hybrid firewall makes this association based upon data packets previously received by the firewall that comprised application-identifying information.

In step 2525, the hybrid firewall analyzes the data communication for malicious code. Because the hybrid firewall is at the same level as a traditional network firewall, it can stop malicious code before it reaches a computer (such as computer 2115 or 2215). Further, because the hybrid firewall is application sensitive, the hybrid firewall can perform the function of a traditional personal firewall to handle application-level security.

In step 2530, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2500 proceeds to step 2535. In step 2535, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2500 then ends.

If the data communication was not found to contain malicious code, then the method 2500 proceeds to step 2540. In step 2540, the firewall allows the data communication, and the data communication is routed to the application. The method 2500 then ends.

Figure 26 is a flowchart of a method 2600 of routing a data communication from an application (such as application 2140 or 2240) to an external network (such as the external network 2105 or 2205), in accordance with an embodiment of the present invention. In step 2605, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system or by an agent (such as the agent 2135 or 2235) running on a computer.

In step 2610, data identifying the application is embedded in the data communication. This step may be performed by the application, by an operating system, or by an agent (such as the agent 2135 or 2235) running on a computer. In one embodiment, an agent running on the same computer as the application creates packets of data, each packet comprising data identifying the application associated with the packet. Because each packet comprises data identifying the application that is associated with the packet, a downstream hybrid firewall (such as the firewall 2110 or 2210) can act as a personal firewall to handle application-level security.

In step 2615, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2620, the hybrid firewall extracts and removes the application-identifying information from the data communication. In step 2625, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2630, the data communication (minus data identifying the application, internal IP address, and internal MAC address) is routed to the external network via a NIC (such as NIC 2120 or 2220). The method 2600 then ends.

The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodiments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that

matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

CLAIMS

1. A computer comprising:

an application associated with an application address;

a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network;

a network address translation engine configured to translate between the application address and a public address; and

a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address.

2. The computer of claim 1, wherein the network address translation engine is part of the driver.

3. The computer of claim 1, wherein the network address translation engine is part of a firewall.

4. The computer of claim 3, wherein the firewall is located on a mobile security system.

5. The computer of claim 1, wherein the network address translation engine is configured to use Dynamic Host Configuration Protocol.

6. The computer of claim 1, wherein the computer is configured to send data packets identifying the application to a firewall, and the firewall is configured to handle both network-level security and application-level security.

7. A system comprising:

a network interface;

a firewall in communication with the network interface configured to handle both network-level security and application-level security; and

a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall.

8. The system of claim 7, wherein:

each data packet is associated with one of the one or more applications; and

each data packet comprises data identifying the application associated with the data packet.

9. The system of claim 8, wherein the firewall is configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network.

10. The system of claim 7, wherein the network interface is configured to receive incoming data from an external network, and to route the incoming data to the firewall.

11. The system of claim 7, wherein:

each application is associated with at least one address; and

the firewall is configured to dynamically isolate the address from an external network.

12. The system of claim 11, wherein the firewall is configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

13. A method within a personal computer of processing incoming data associated with a public address, the method comprising:

receiving the data from an external network;

translating the public address into an internal address associated with an application;

analyzing the data for malicious code; and

routing the data to the application if the data does not comprise malicious code.

14. The method of claim 13, wherein the analyzing step comprises analyzing the data for malicious code at both the network level and the application level.

15. The method of claim 13, wherein the translating step uses Dynamic Host Configuration Protocol.

16. A method within a computer of processing outgoing data, the method comprising:

receiving outgoing data from an application, the application being associated with an internal address;

translating the internal address into a public address; and

routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network.

17. The method of claim 16, wherein the translating step uses Dynamic Host Configuration Protocol.

18. The method of claim 16, further comprising:

configuring the outgoing data into one or more data packets;

associating each of the one or more data packets with the application; and

embedding application-identifying data in each of the one or more data packets.

19. The method of claim 18,

further comprising creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets,

wherein the routing step comprises routing the one or more data packet subsets to the external network.

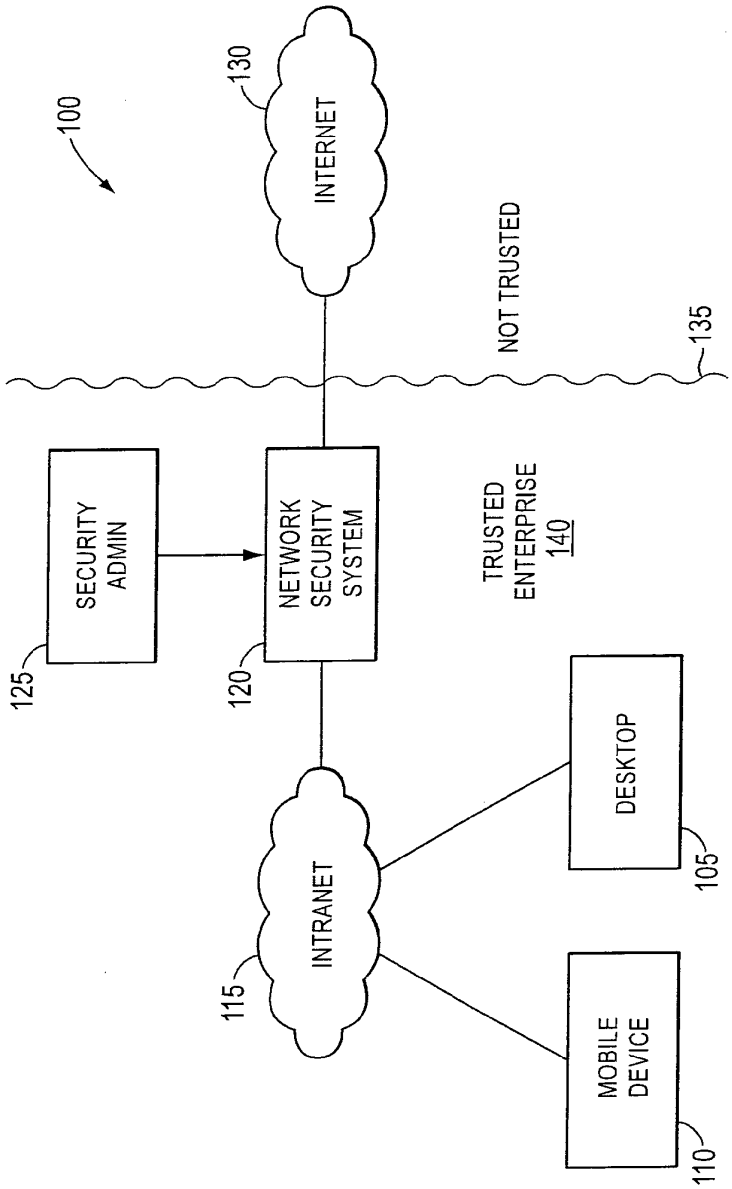


FIG. 1
(PRIOR ART)

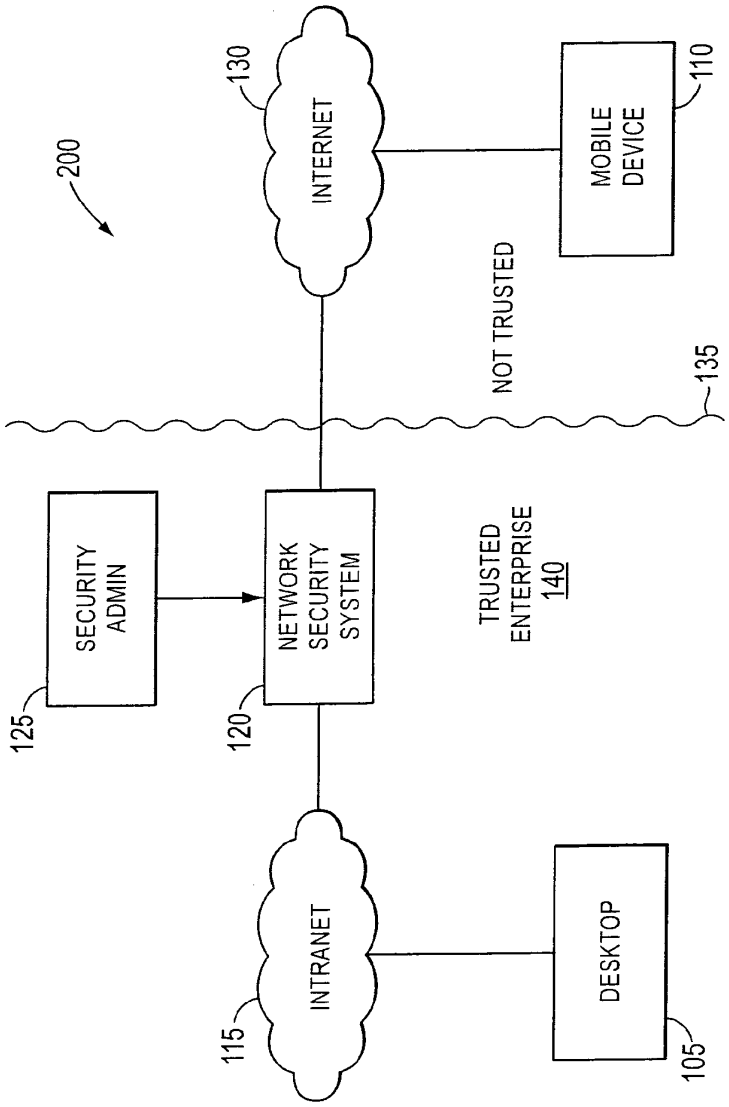


FIG. 2
(PRIOR ART)

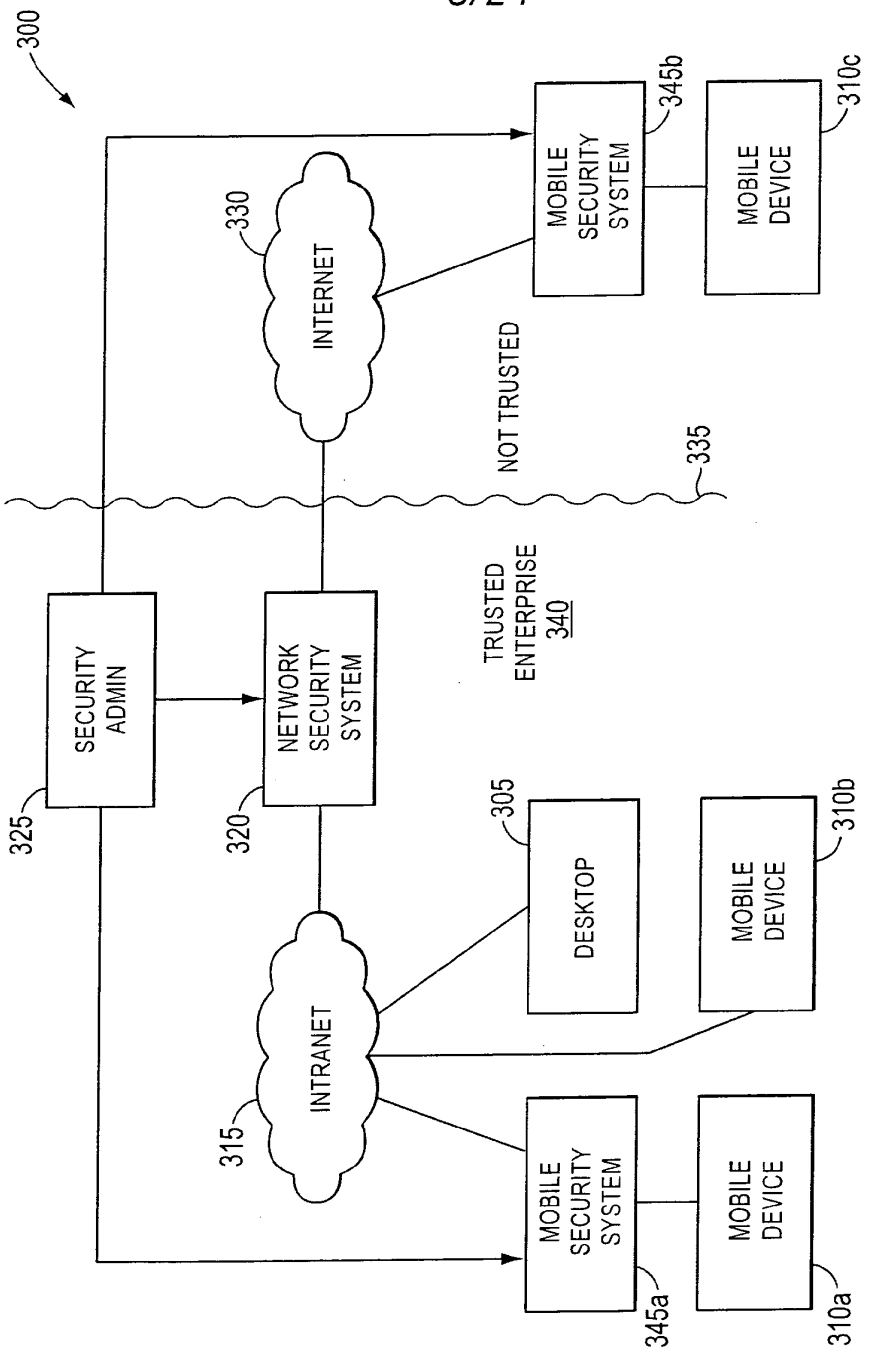

300
MOBILE SECURITY SYSTEM
345b
MOBILE DEVICE
310c
INTERNET
330
NOT TRUSTED
335
TRUSTED ENTERPRISE 340
SECURITY ADMIN
325
NETWORK SECURITY SYSTEM
320
DESKTOP
305
MOBILE DEVICE
310b
INTRANET
315
MOBILE SECURITY SYSTEM
345a
MOBILE DEVICE
310a

FIG. 3

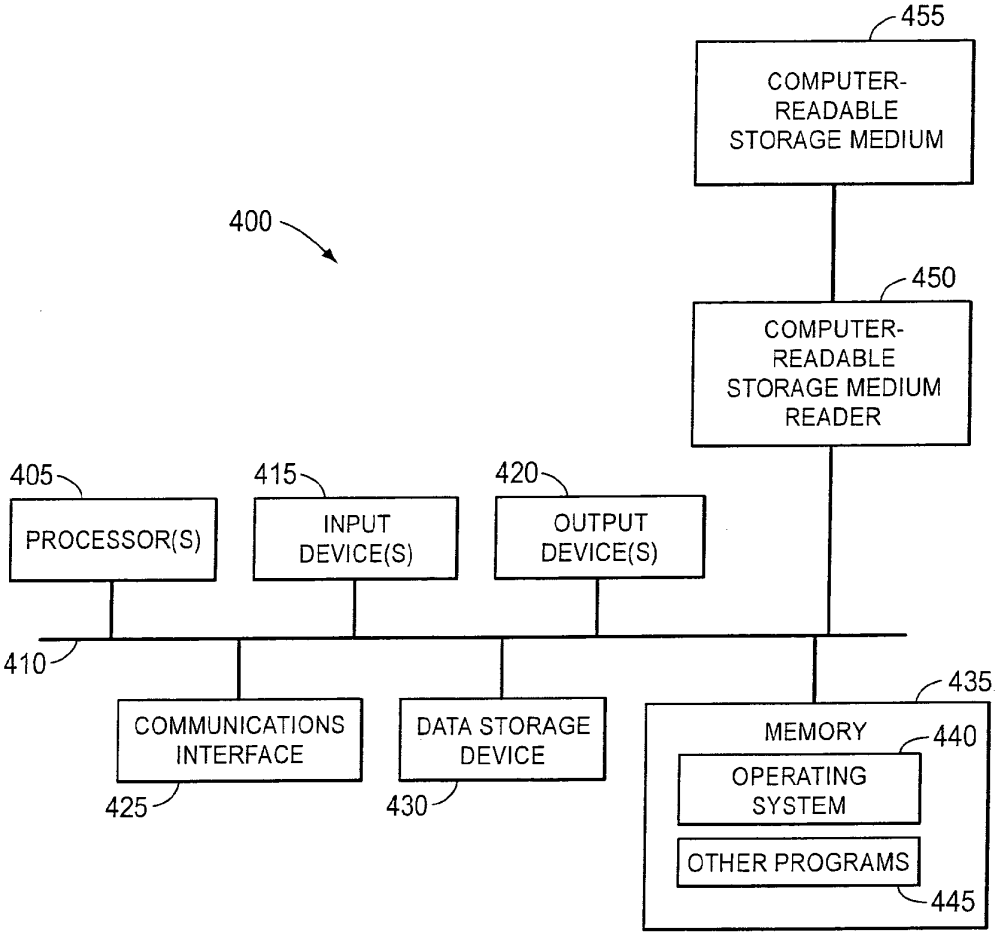

455
COMPUTER-READABLE STORAGE MEDIUM
400
450
COMPUTER-READABLE STORAGE MEDIUM READER
405
PROCESSOR(S)
415
INPUT DEVICE(S)
420
OUTPUT DEVICE(S)
410
435
COMMUNICATIONS INTERFACE
425
DATA STORAGE DEVICE
430
MEMORY
440
OPERATING SYSTEM
OTHER PROGRAMS
445

FIG. 4

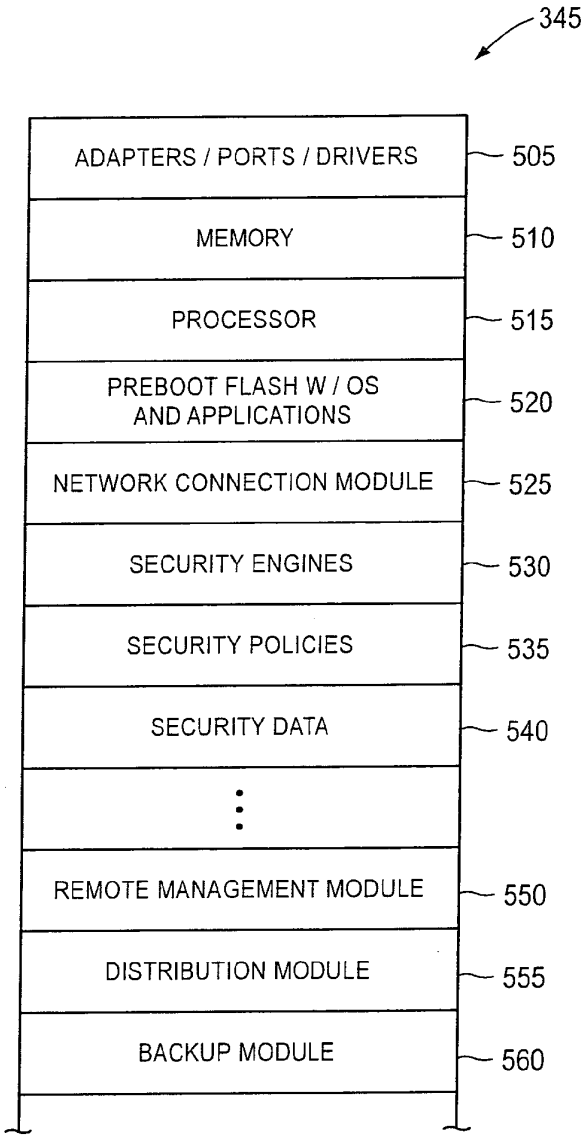

345
ADAPTERS / PORTS / DRIVERS
505
MEMORY
510
PROCESSOR
515
PREBOOT FLASH W / OS AND APPLICATIONS
520
NETWORK CONNECTION MODULE
525
SECURITY ENGINES
530
SECURITY POLICIES
535
SECURITY DATA
540
REMOTE MANAGEMENT MODULE
550
DISTRIBUTION MODULE
555
BACKUP MODULE
560

FIG. 5

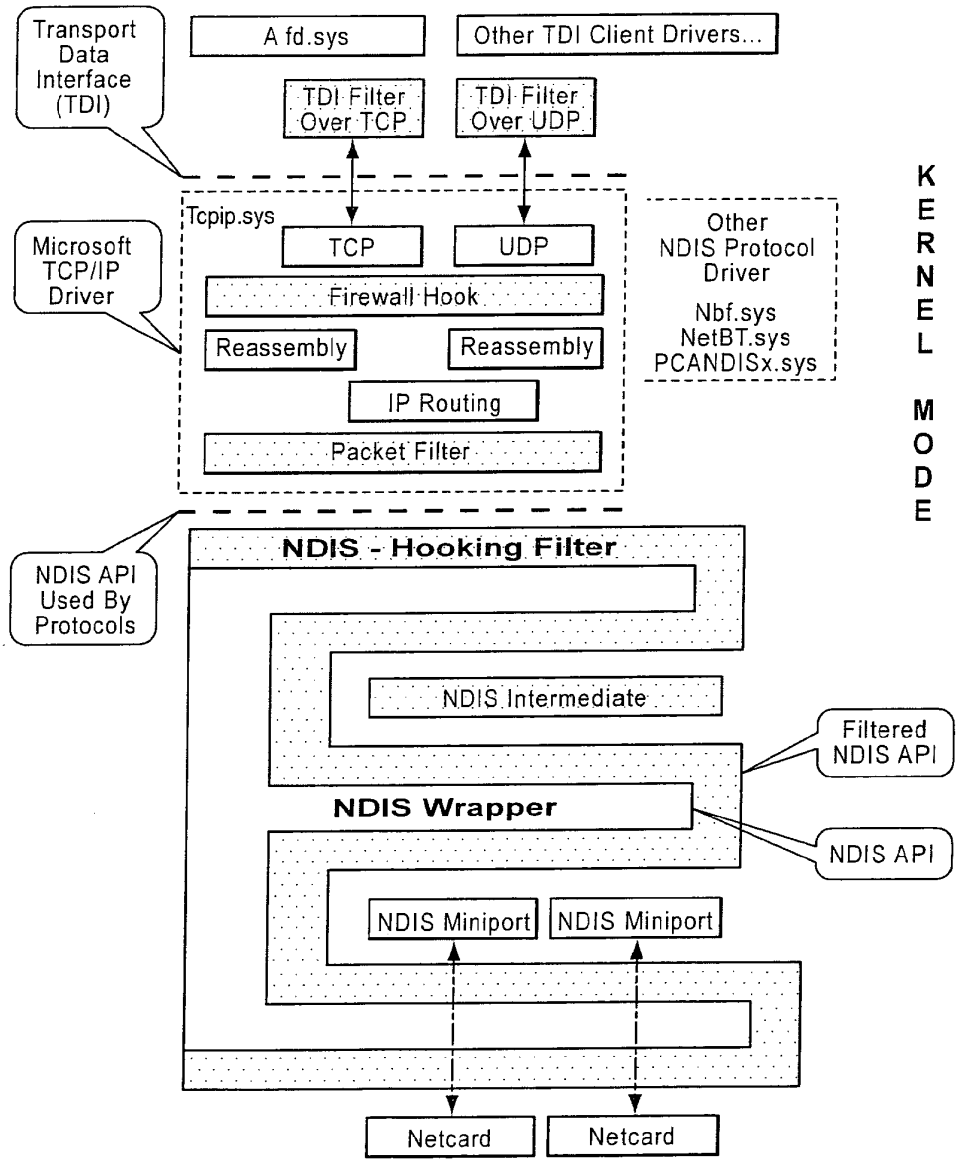

Transport Data Interface (TDI)
A fd.sys
Other TDI Client Drivers...
TDI Filter Over TCP
TDI Filter Over UDP
Tcpip.sys
TCP
UDP
Firewall Hook
Reassembly
Reassembly
IP Routing
Packet Filter
Microsoft TCP/IP Driver
Other NDIS Protocol Driver
Nbf.sys
NetBT.sys
PCANDISx.sys
KERNEL MODE
NDIS API Used By Protocols
NDIS - Hooking Filter
NDIS Intermediate
Filtered NDIS API
NDIS Wrapper
NDIS API
NDIS Miniport
NDIS Miniport
Netcard
Netcard

FIG. 6

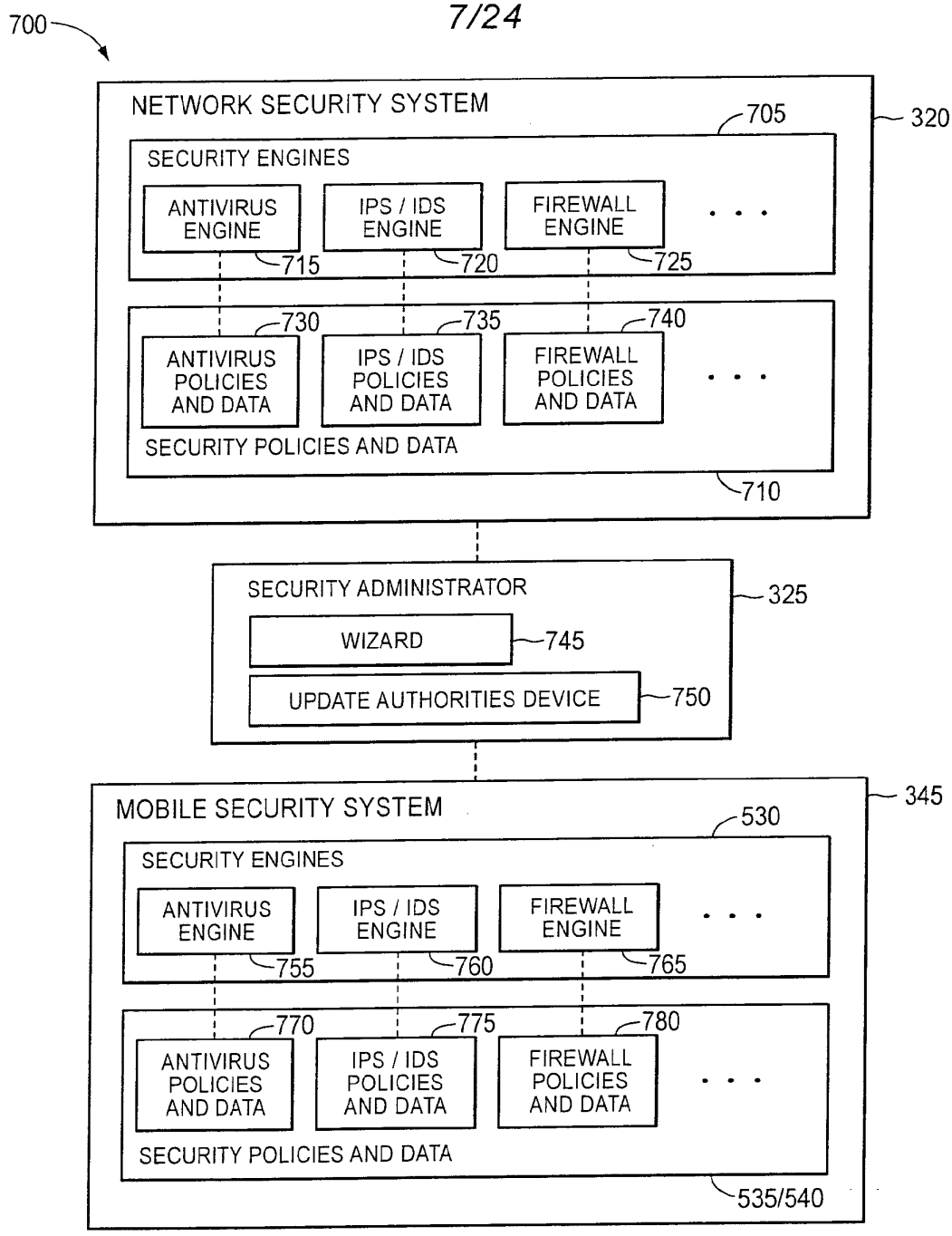

700
NETWORK SECURITY SYSTEM
705
320
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
715
720
725
730
735
740
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
710
SECURITY ADMINISTRATOR
325
WIZARD
745
UPDATE AUTHORITIES DEVICE
750
MOBILE SECURITY SYSTEM
345
530
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
755
760
765
770
775
780
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
535/540

FIG. 7

8/24

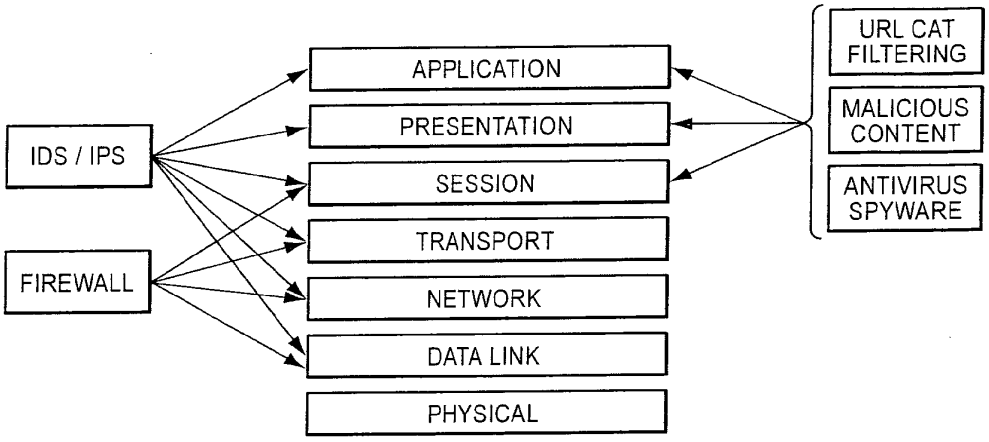


FIG. 8

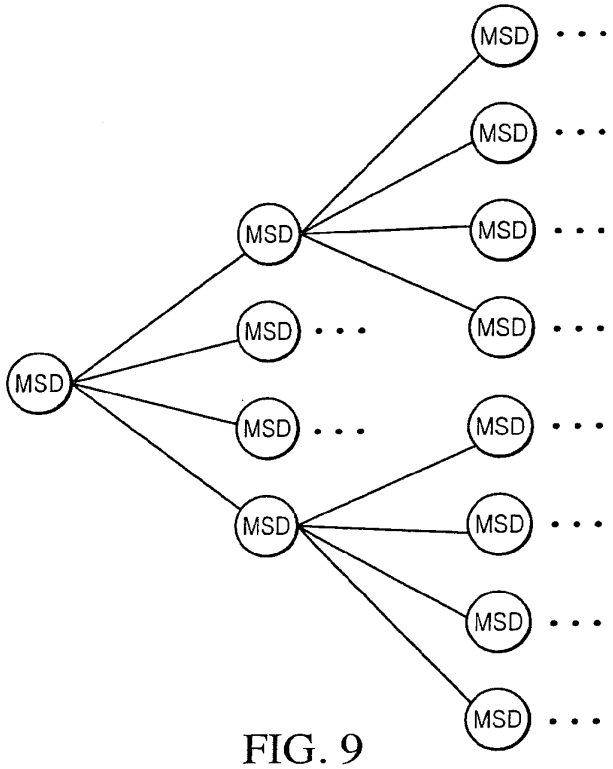


FIG. 9

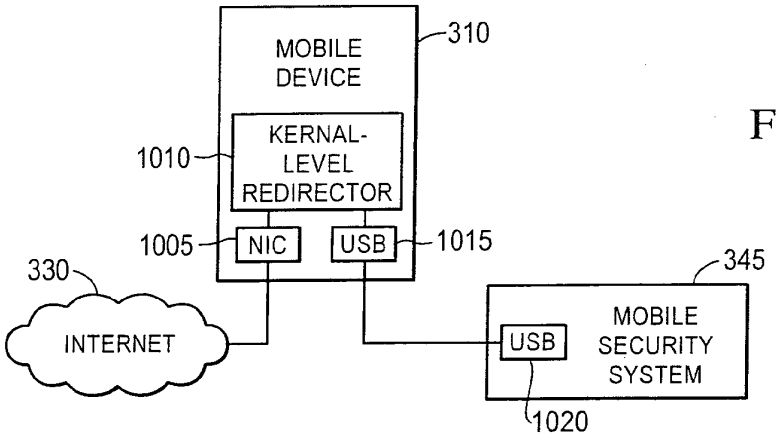


FIG. 10A

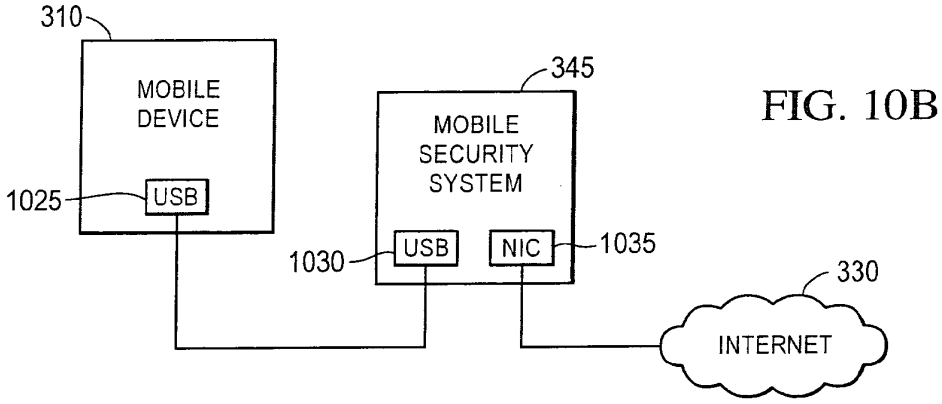


FIG. 10B

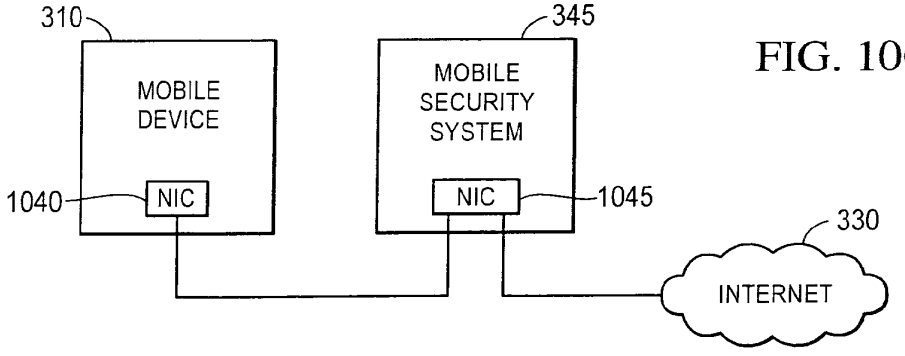


FIG. 10C

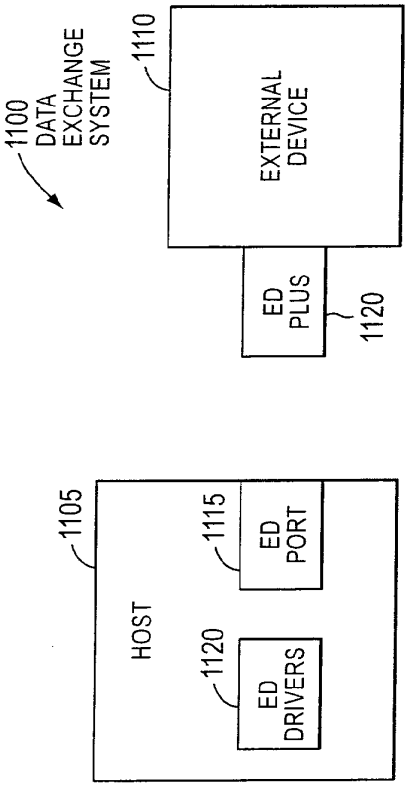


FIG. 11
(PRIOR ART)

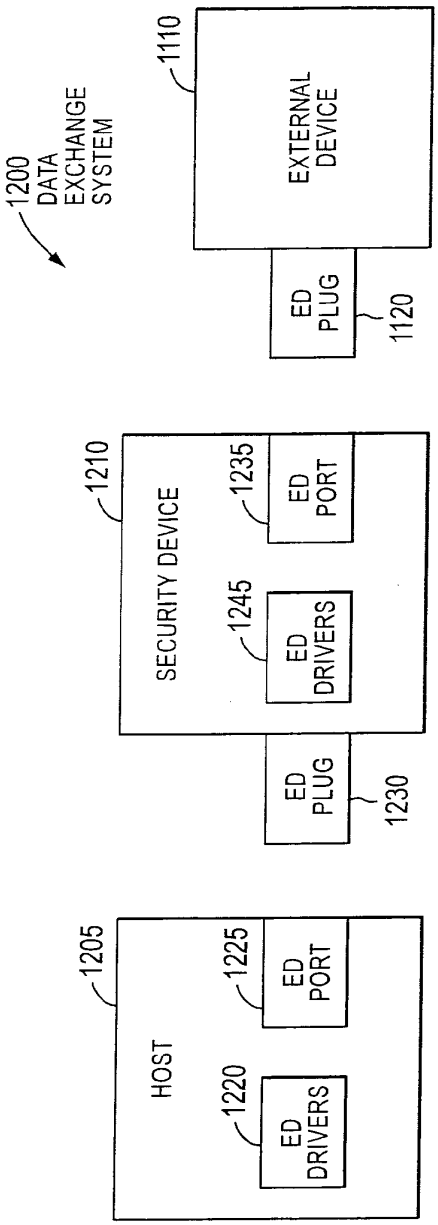


FIG. 12

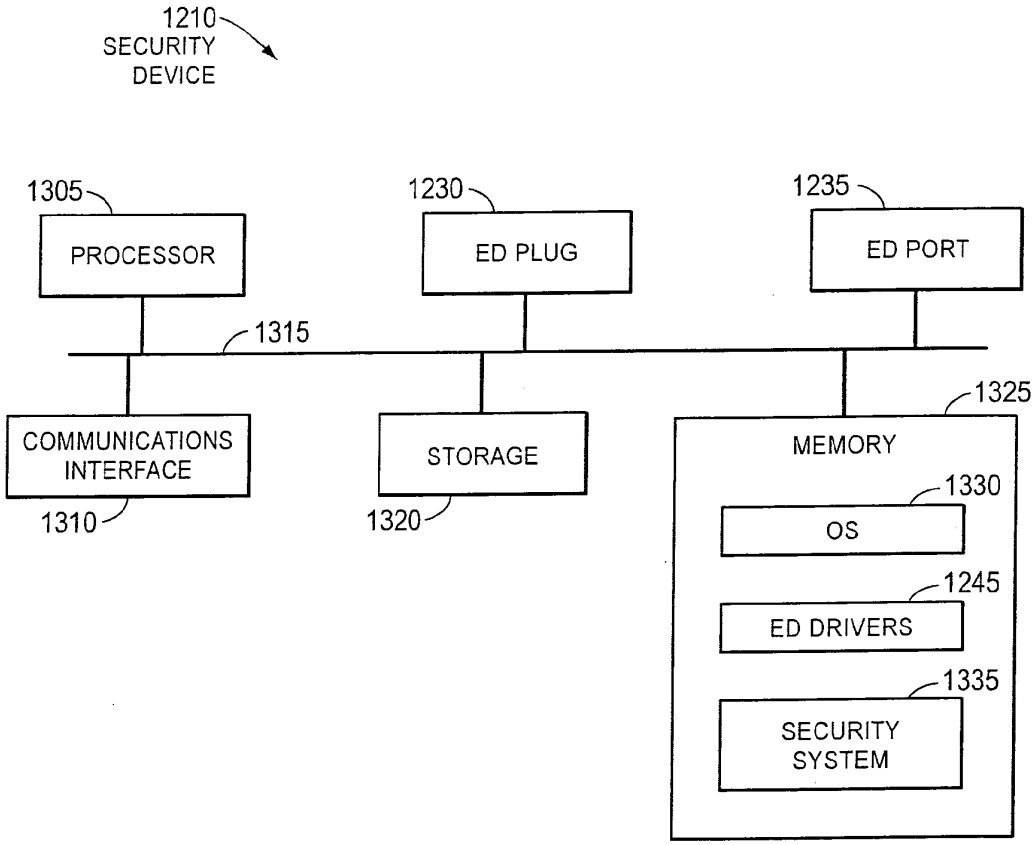

1210
SECURITY DEVICE
1305
PROCESSOR
1230
ED PLUG
1235
ED PORT
1315
COMMUNICATIONS INTERFACE
1310
STORAGE
1320
1325
MEMORY
1330
OS
1245
ED DRIVERS
1335
SECURITY SYSTEM

FIG. 13

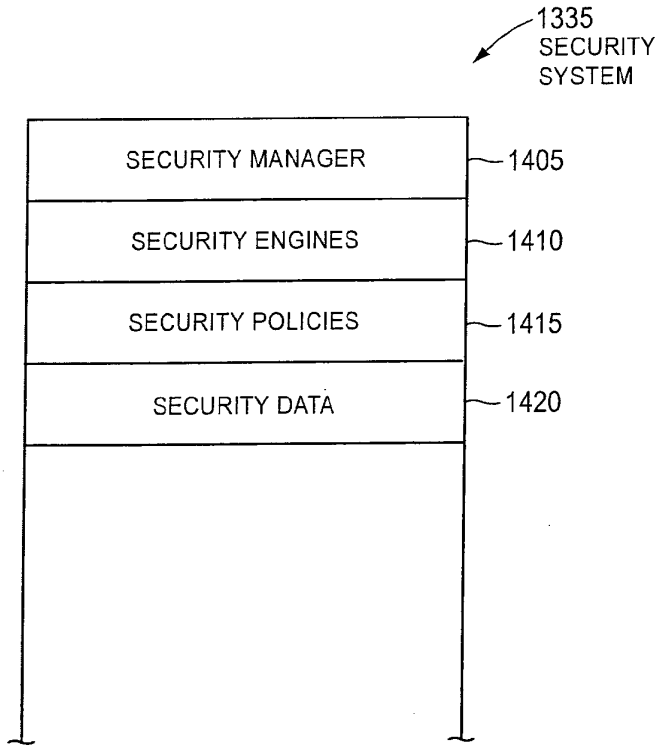

1335
SECURITY
SYSTEM
SECURITY MANAGER
1405
SECURITY ENGINES
1410
SECURITY POLICIES
1415
SECURITY DATA
1420

FIG. 14

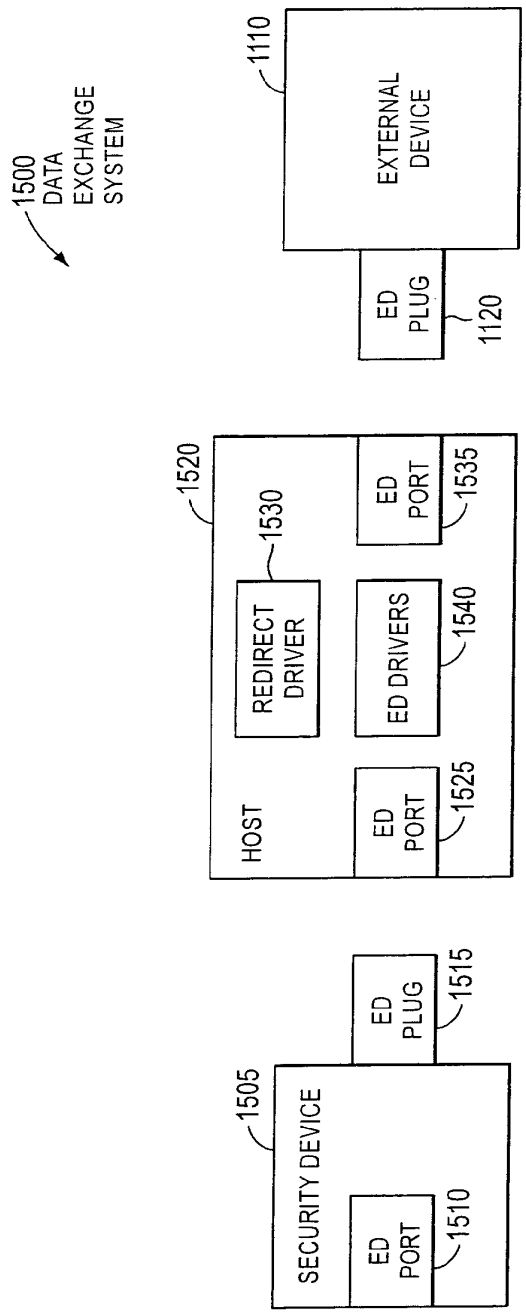

1500
DATA
EXCHANGE
SYSTEM
1110
EXTERNAL
DEVICE
ED
PLUG
1120
1520
1530
REDIRECT
DRIVER
ED
PORT
1535
ED DRIVERS
1540
HOST
ED
PORT
1525
ED
PLUG
1515
1505
SECURITY DEVICE
ED
PORT
1510

FIG. 15

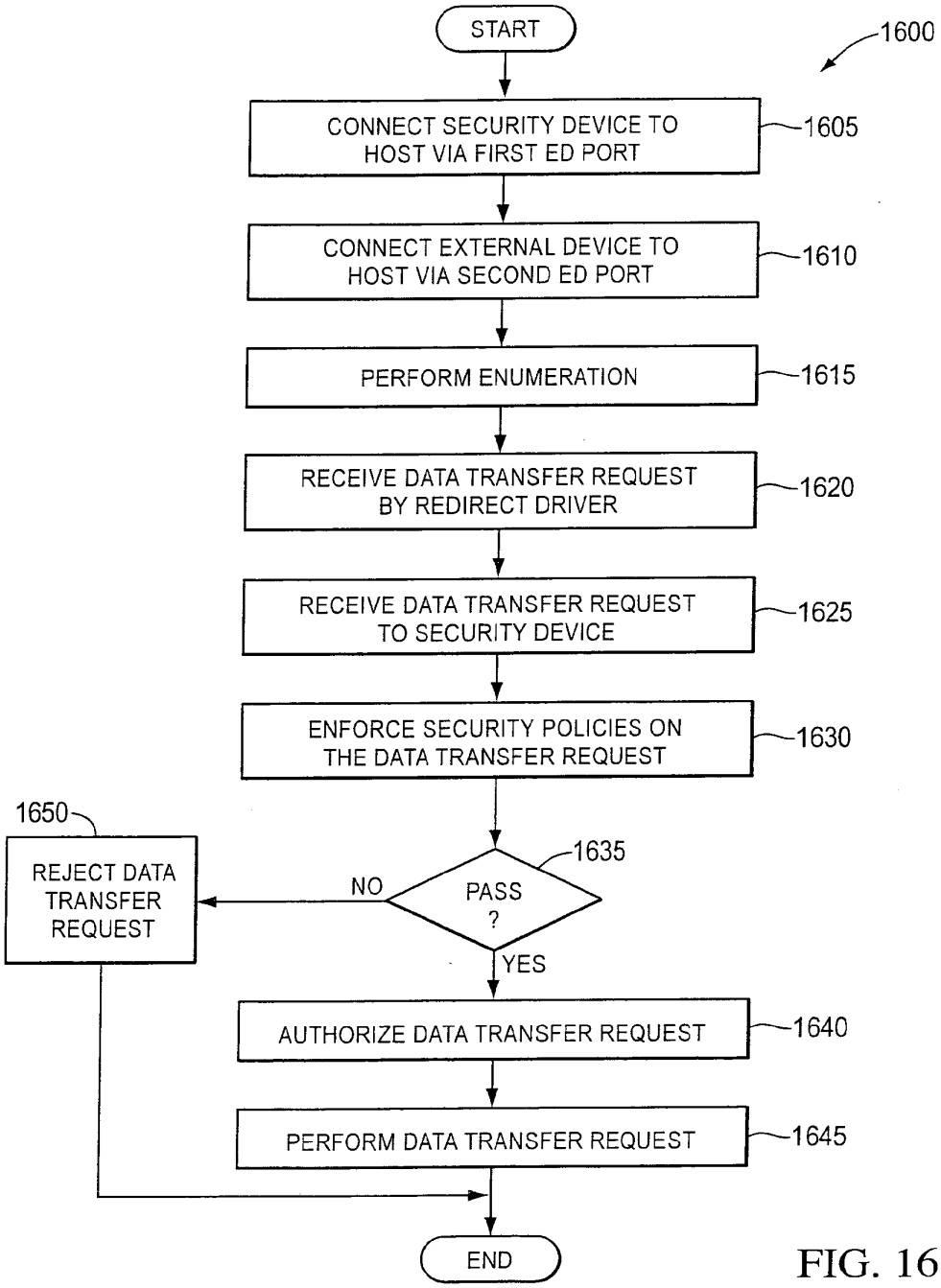

START
1600
CONNECT SECURITY DEVICE TO HOST VIA FIRST ED PORT
1605
CONNECT EXTERNAL DEVICE TO HOST VIA SECOND ED PORT
1610
PERFORM ENUMERATION
1615
RECEIVE DATA TRANSFER REQUEST BY REDIRECT DRIVER
1620
RECEIVE DATA TRANSFER REQUEST TO SECURITY DEVICE
1625
ENFORCE SECURITY POLICIES ON THE DATA TRANSFER REQUEST
1630
1650
REJECT DATA TRANSFER REQUEST
NO
PASS ?
1635
YES
AUTHORIZE DATA TRANSFER REQUEST
1640
PERFORM DATA TRANSFER REQUEST
1645
END

FIG. 16

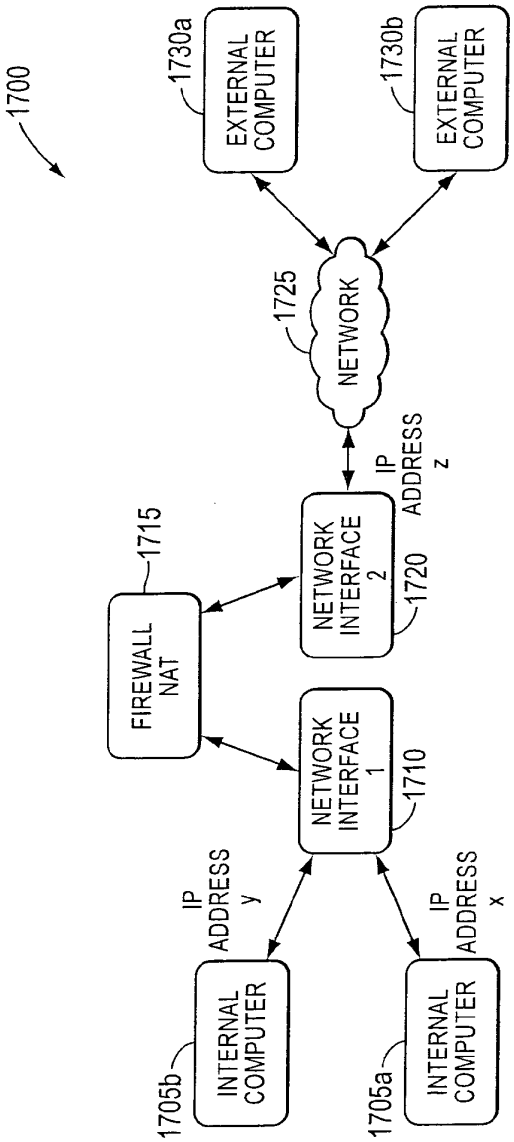


FIG. 17
(PRIOR ART)

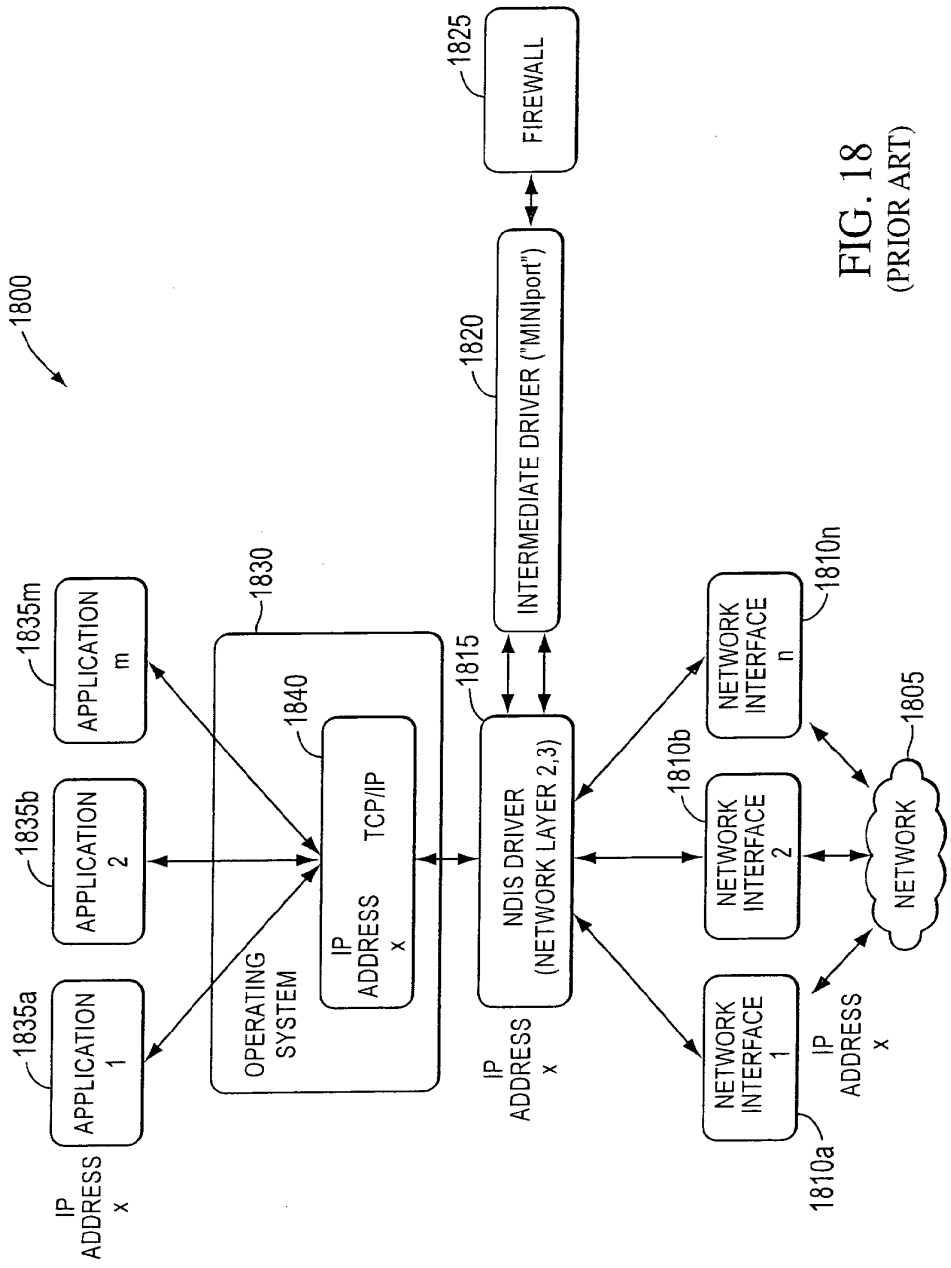


FIG. 18
(PRIOR ART)

17/24

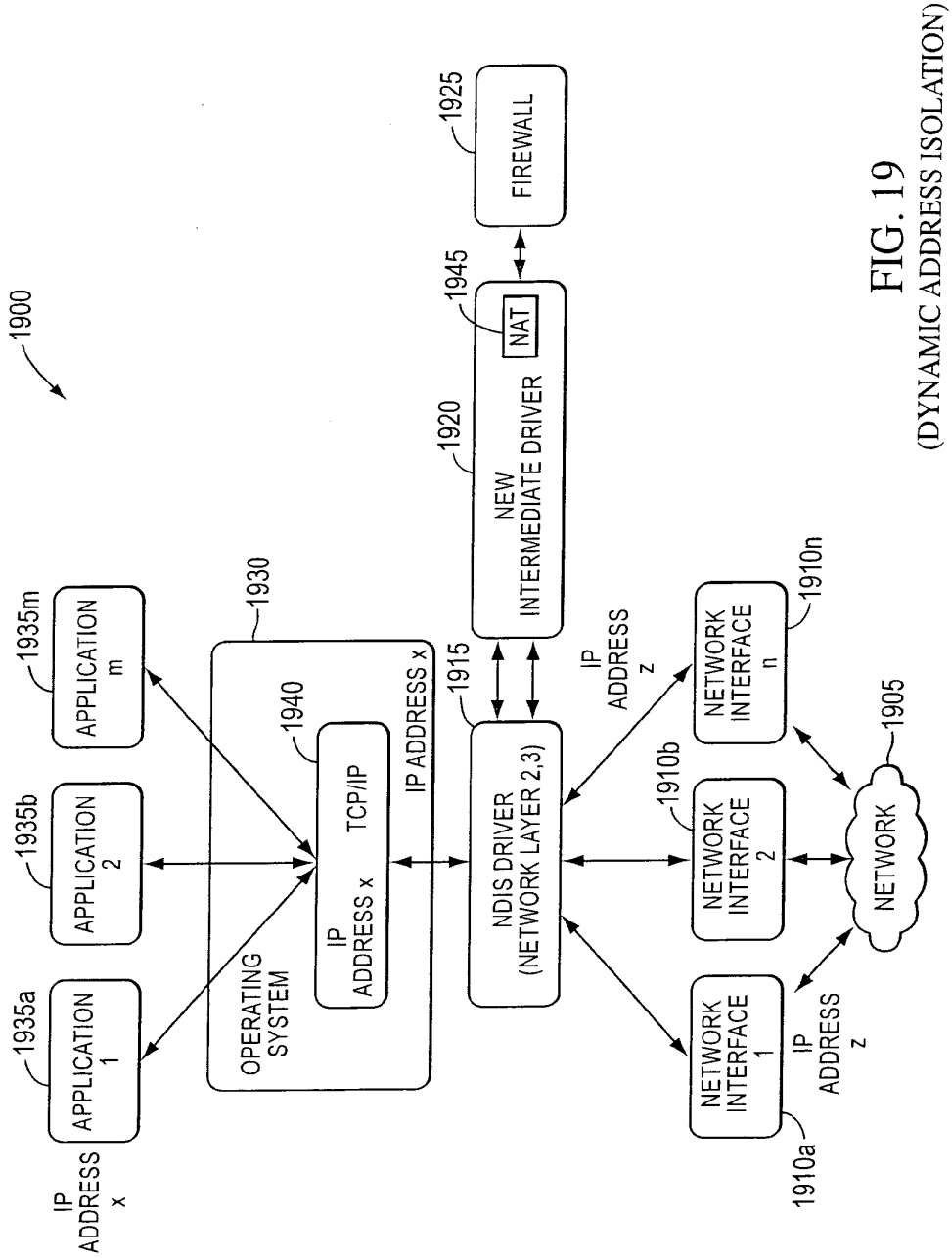


FIG. 19
(DYNAMIC ADDRESS ISOLATION)

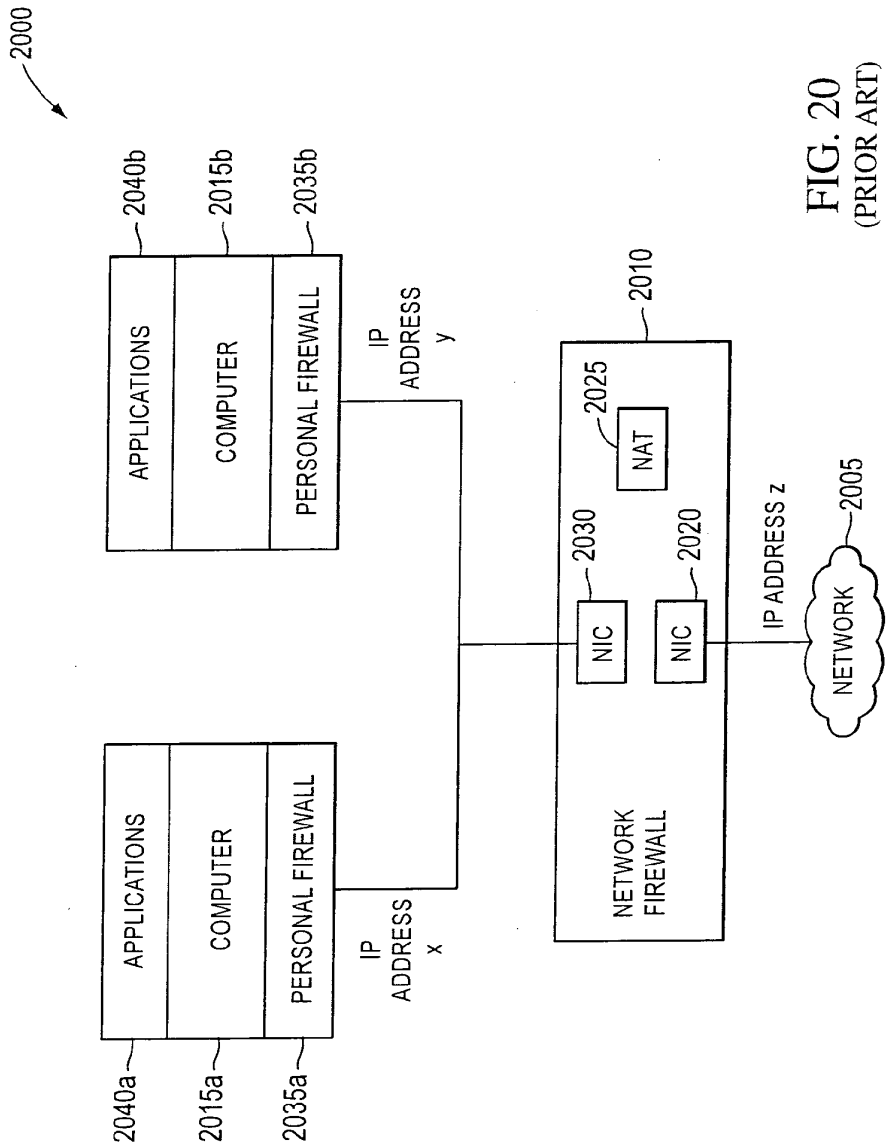


FIG. 20
(PRIOR ART)

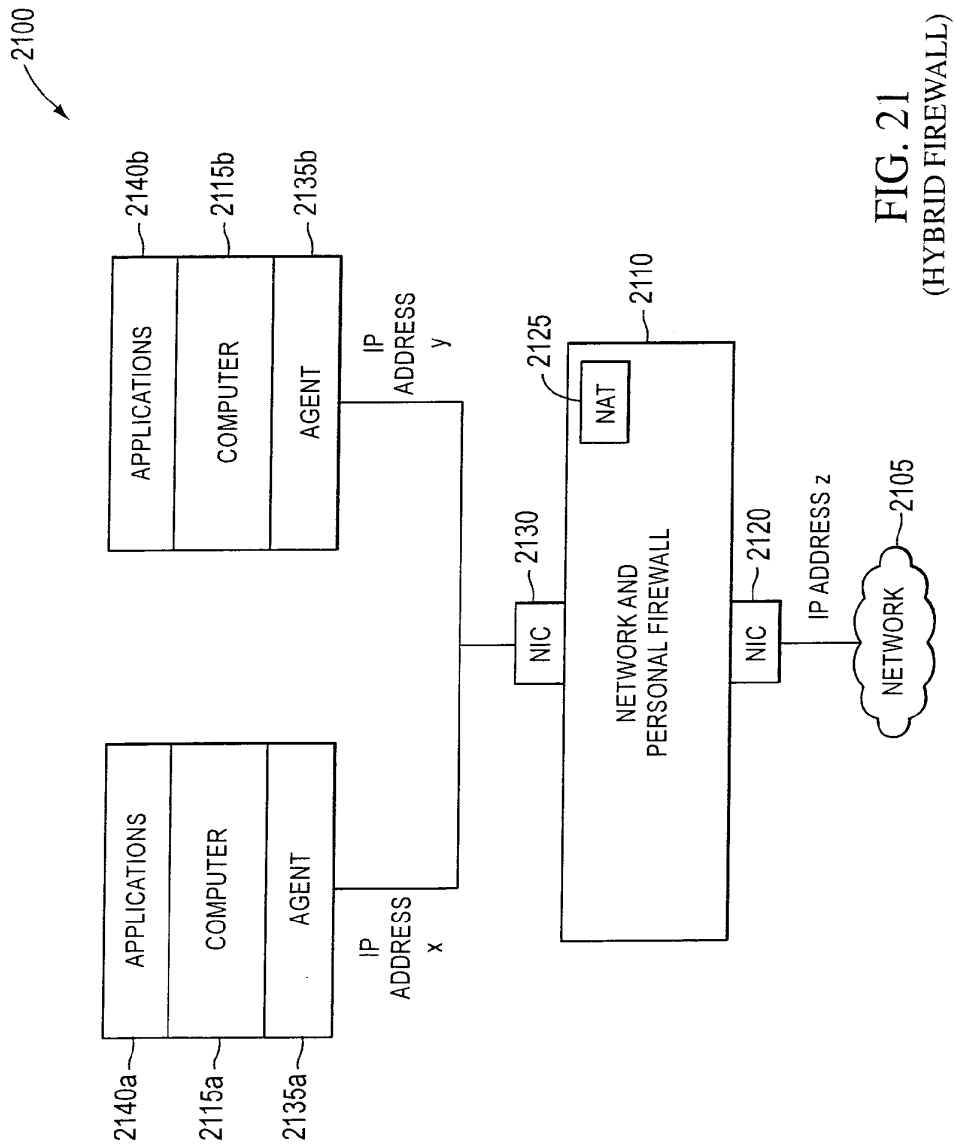


FIG. 21
(HYBRID FIREWALL)

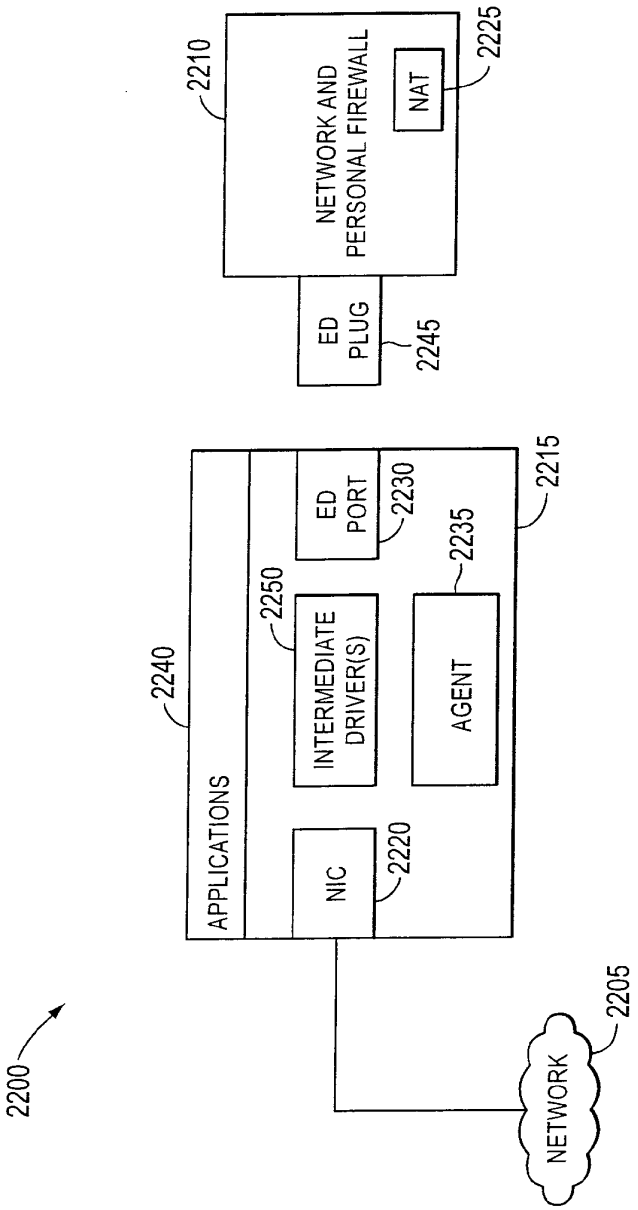


FIG. 22
(HYBRID FIREWALL EXAMPLE)

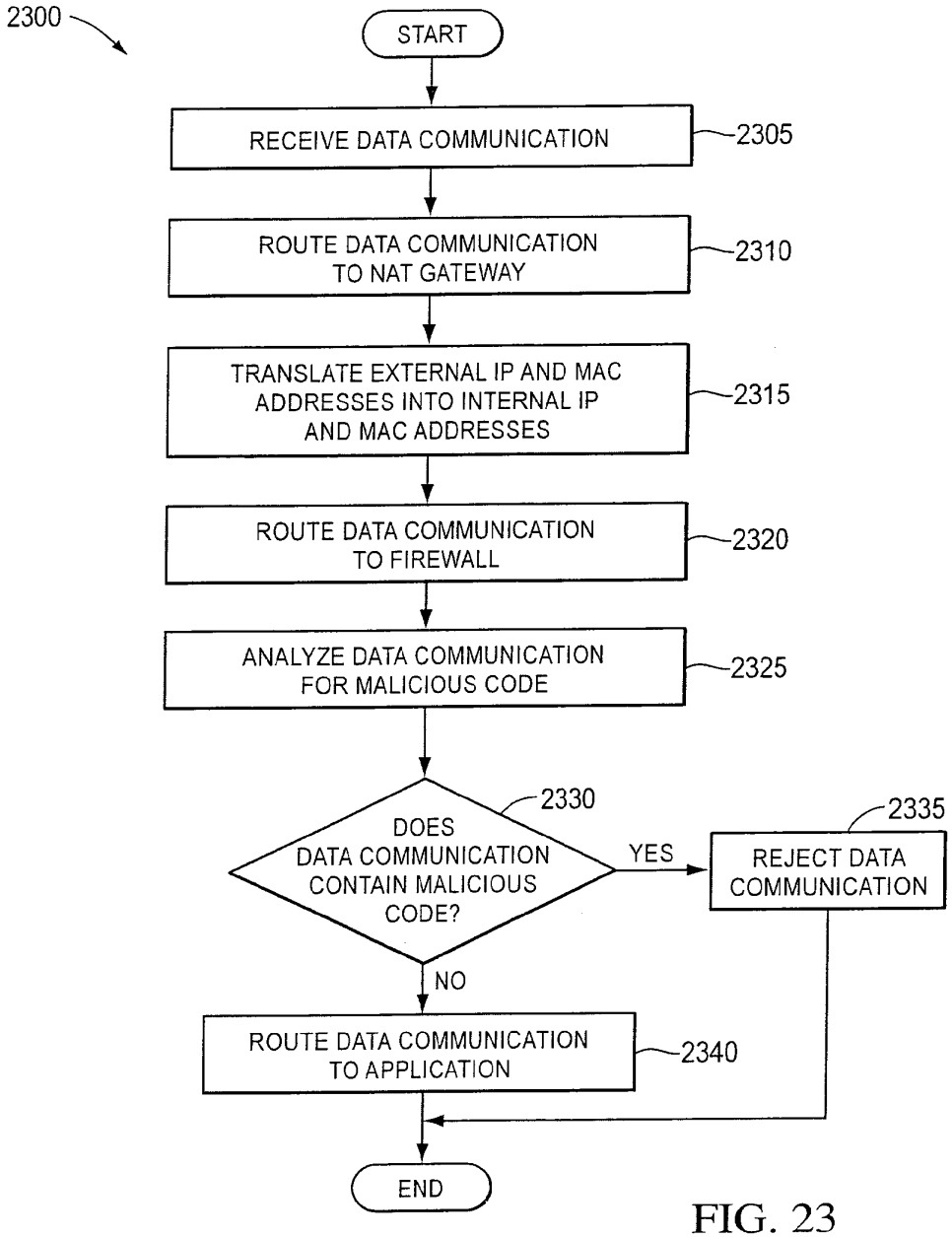

2300
START
RECEIVE DATA COMMUNICATION
2305
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2310
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2315
ROUTE DATA COMMUNICATION TO FIREWALL
2320
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2325
2330
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
YES
2335
REJECT DATA COMMUNICATION
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2340
END

FIG. 23

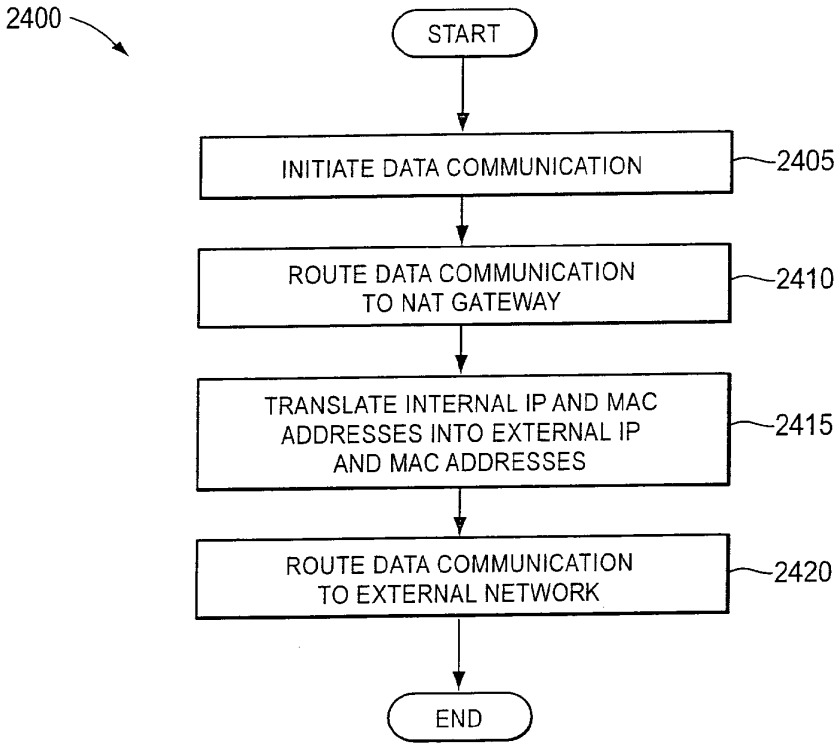

2400
START
INITIATE DATA COMMUNICATION
2405
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2410
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2415
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2420
END

FIG. 24

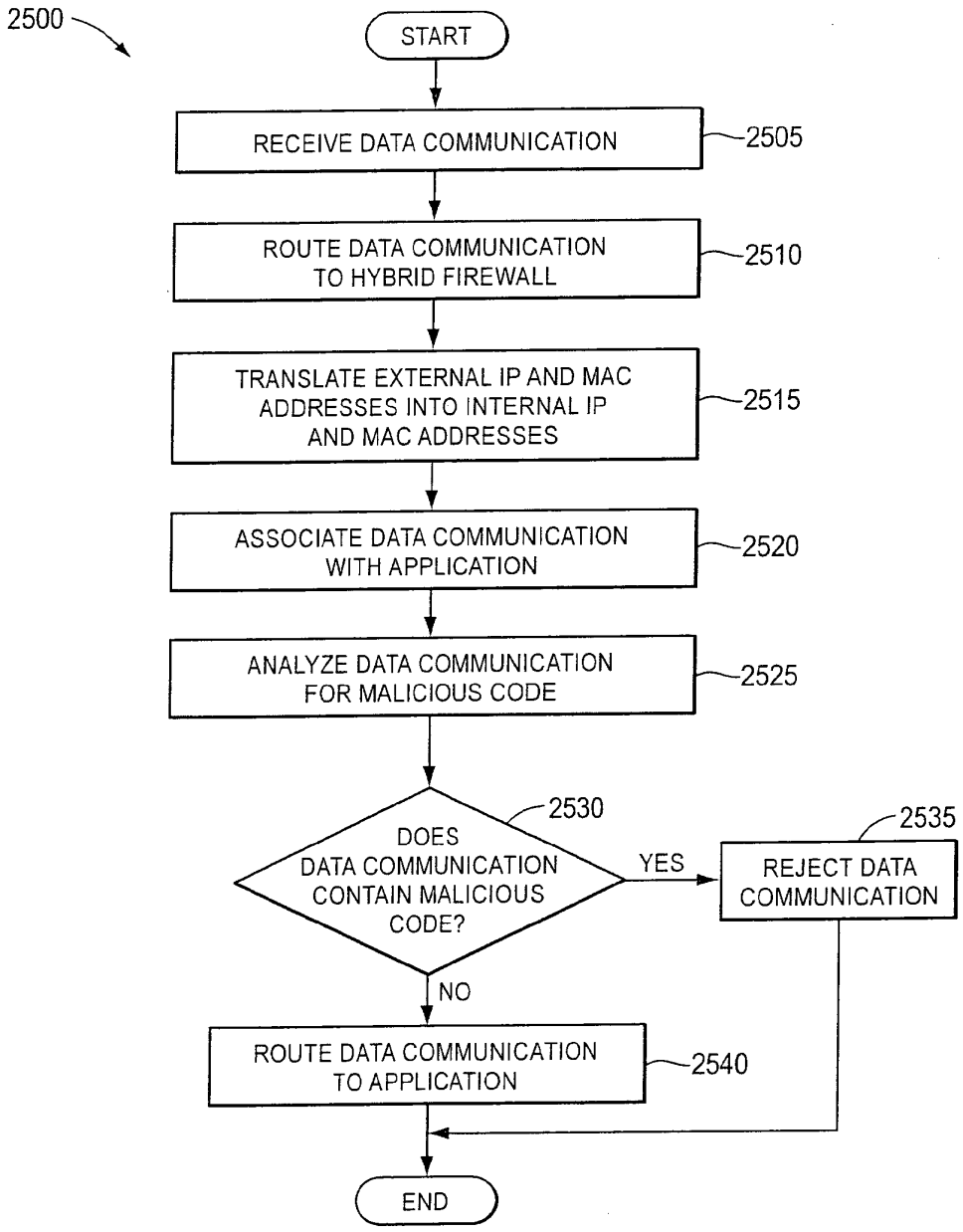

2500
START
RECEIVE DATA COMMUNICATION
2505
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2510
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2515
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2520
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2525
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
2530
YES
REJECT DATA COMMUNICATION
2535
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2540
END

FIG. 25

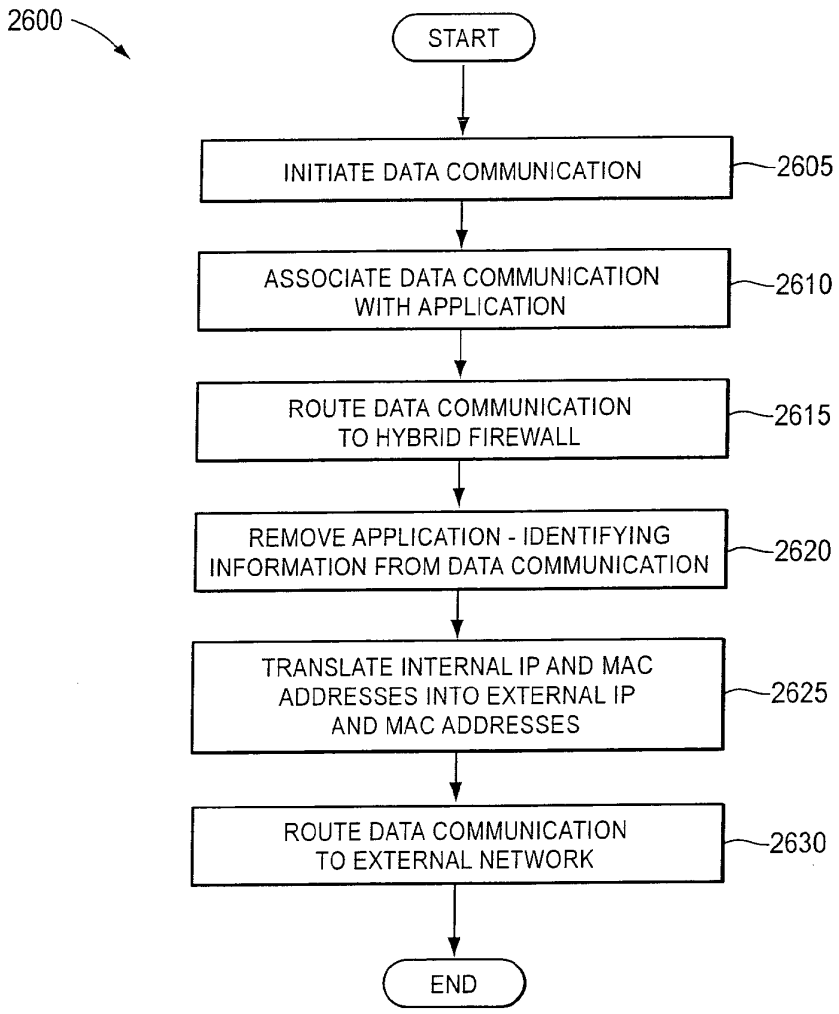

2600
START
INITIATE DATA COMMUNICATION
2605
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2610
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2615
REMOVE APPLICATION - IDENTIFYING INFORMATION FROM DATA COMMUNICATION
2620
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2625
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2630
END

FIG. 26

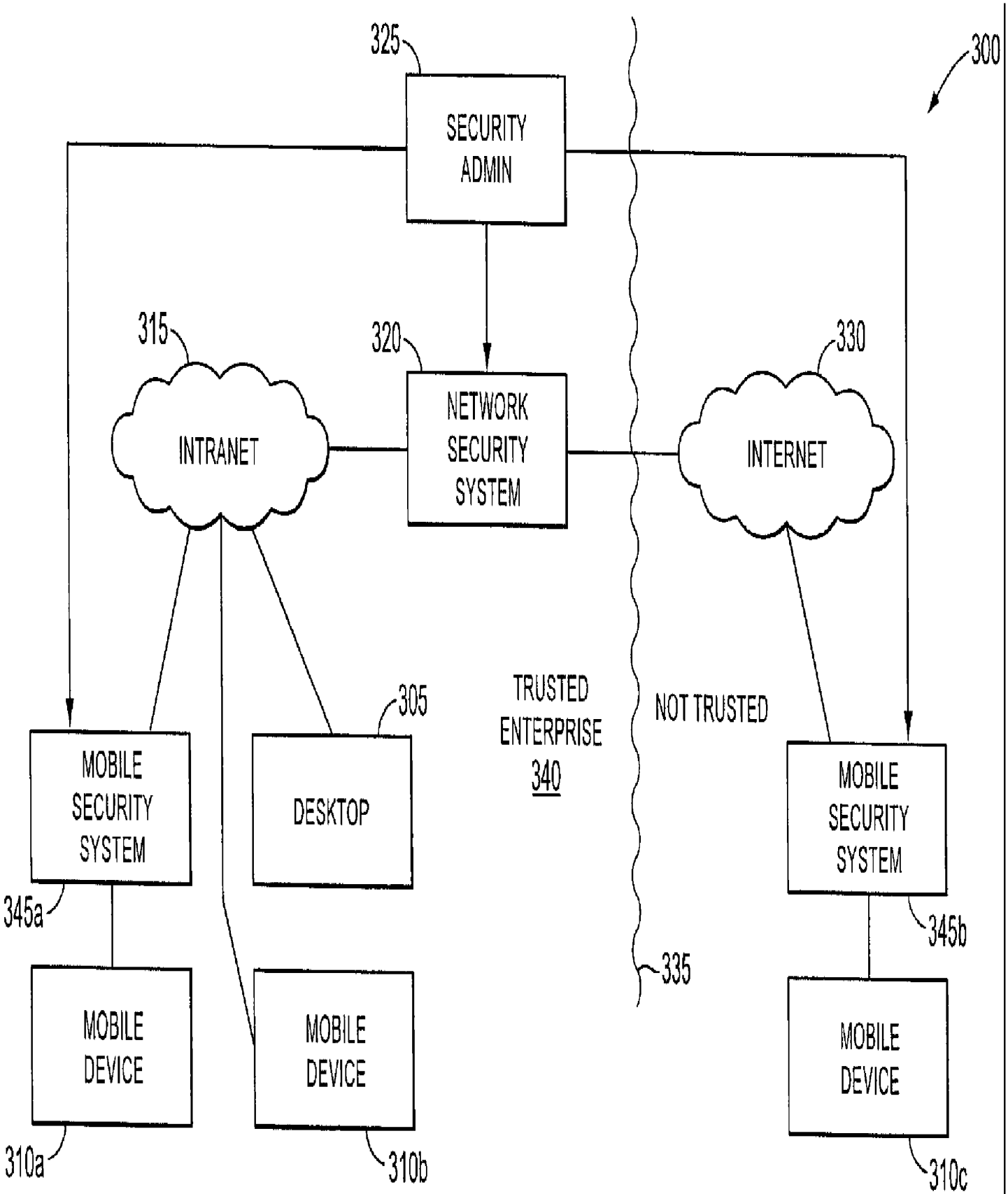

325
300
SECURITY ADMIN
315
320
330
INTRANET
NETWORK SECURITY SYSTEM
INTERNET
TRUSTED ENTERPRISE 340
NOT TRUSTED
305
MOBILE SECURITY SYSTEM
DESKTOP
MOBILE SECURITY SYSTEM
345a
345b
335
MOBILE DEVICE
MOBILE DEVICE
MOBILE DEVICE
310a
310b
310c

FIG. 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 850 575 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.10.2007 Bulletin 2007/44

(21) Application number: **06252276.8**

(22) Date of filing: **27.04.2006**

(51) Int Cl.:
H04M 15/28 *(2006.01)* ***H04M 17/00*** *(2006.01)*
H04Q 7/32 *(2006.01)* *H04Q 7/38* *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventor: **Rybak, Michal A.**
Kitchener, Ontario, N2R 1B1 (CA)

(74) Representative: **Fennell, Gareth Charles et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ (GB)

(54) Method and apparatus for monitoring and controlling wireless resource usage

(57) A mobile communications device (116) comprises a wireless resource usage module (216) operable to assist the user of the mobile communications device (116) and/or his or her employer in monitoring and/or controlling the level of resources consumed by the user in a billing period.

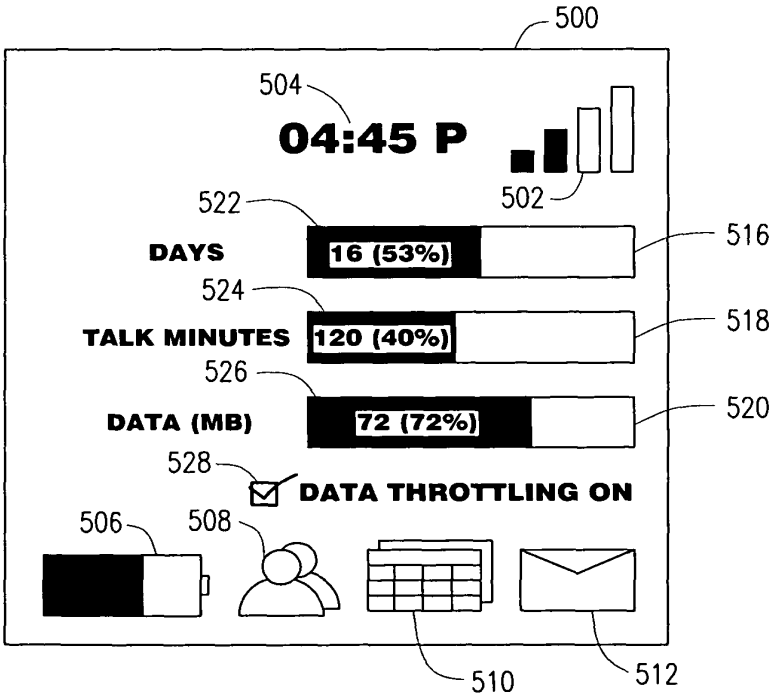


FIG. 7

EP 1 850 575 A1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD OF THE APPLICATION

[0001] The present disclosure generally relates to wireless packet data service networks. More particularly, and not by way of any limitation, the present disclosure is directed to a mobile communications device and related data service network employing features suitable for monitoring and controlling wireless service usage.

BACKGROUND

[0002] Wireless service is generally offered by wireless service providers according to certain wireless service access plans. Most wireless service access plans include limitations as to the quantity of wireless access available in a given time. For example, a first wireless service access plan may provide for a certain number of cellular telephone voice minutes per month. Certain plans provide for unlimited cellular voice minutes during off-peak periods along with a limited number of minutes available during peak periods. Wireless service access plans may also provide for specified levels of wireless data access per month. While cellular telephone minutes are generally quantified in minutes per month, wireless data access is generally quantified in some units of bandwidth per month (e.g., megabytes per month). In either event, a wireless service provider will generally continue to provide service above the specified level, but will charge an additional premium for the usage above the level specified in the wireless service access plan.

SUMMARY OF THE DISCLOSURE

[0003] In one embodiment, the present disclosure is directed to a method for monitoring resource usage of a mobile communications device comprising the steps of acquiring a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period; acquiring resource consumption data relative to the specified calendar period; calculating usage statistics based on the resource consumption data and the plan profile; and presenting the usage statistics to an entity.

[0004] In another embodiment, the present disclosure is directed to a mobile communications device comprising at least one storage area for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period; at least one storage area for containing resource consumption data relative to the specified period; and a wireless resource usage control module for calculating usage statistics based on the resource consumption data and the service plan profile.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] A more complete understanding of the embodiments of the present disclosure may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0006] Figure 1 depicts an exemplary network environment including a wireless packet data service network wherein an embodiment of the present disclosure may be practiced;

[0007] Figure 2 depicts a software architectural view of a mobile communications device operable to route incoming messages according to one embodiment;

[0008] Figure 3 depicts a block diagram of a mobile communications device operable to route incoming messages according to one embodiment;

[0009] Figure 4 depicts a flow chart for a method of monitoring and controlling wireless service access according to one embodiment; and

[0010] Figure 5 depicts a screen shot of a mobile communications device according to one embodiment;

[0011] Figure 6 depicts a screen shot of a mobile communications device according to a second embodiment;

[0012] Figure 7 depicts a screen shot of a mobile communications device having an embodiment of the usage monitoring application open;

[0013] Figure 8 depicts a screen shot of a usage monitoring application embodiment suitable for monitoring the wireless usage of a group of users; and

[0014] Figure 9 depicts a flow chart of a usage throttling method according to one embodiment.

DETAILED DESCRIPTION OF THE DRAWINGS

[0015] A system and method of the present disclosure will now be described with reference to various examples of how the embodiments can best be made and used. Like reference numerals are used throughout the description and several views of the drawings to indicate like or corresponding parts, wherein the various elements are not necessarily drawn to scale.

[0016] Referring now to the drawings, and more particularly to Figure 1, depicted therein is an exemplary network environment 100 including a wireless packet data service network 112 wherein an embodiment of the present system may be practiced. An enterprise network 102, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), wide area network (WAN) or metropolitan area network (MAN), et cetera, for serving a plurality of corporate users.

[0017] A number of application servers 104-1 through 104-N disposed as part of the enterprise network 102 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management, and the like. Accordingly, a diverse array of personal information ap-

pliances such as desktop computers, laptop computers, palmtop computers, et cetera, although not specifically shown in Figure 1, may be operably networked to one or more of the application servers 104-i, i = 1, 2,...,N, with respect to the services supported in the enterprise network 102.

[0018] Additionally, a remote services server 106 may be interfaced with the enterprise network 102 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable mobile communications device 116. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 108, as well as the wireless packet data service network 112 operable with mobile communications device 116 via suitable wireless network infrastructure that includes a base station (BS) 114 .

[0019] In one embodiment, a trusted relay network 110 may be disposed between the Internet 108 and the infrastructure of wireless packet data service network 112. By way of example, mobile communications device 116 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers, et cetera.

[0020] For purposes of the present disclosure, the wireless packet data service network 112 may be implemented in any known or heretofore unknown mobile communications technologies and network protocols. For instance, the wireless packet data service network 112 may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications (GSM)-based carrier network. In other implementations, the wireless packet data service network 112 may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple Access (CDMA) network, or any 3rd Generation (3G) network.

[0021] By way of providing an exemplary embodiment, the teachings of the present disclosure will be illustrated within the network environment 100, although those skilled in the art should readily recognize that the scope of the present disclosure is not limited thereby. Furthermore, a plan information server 109 may be coupled to any of the networks 102, 108, 110, 112 described above for purposes of the present disclosure as will be set forth below in greater detail.

[0022] Figure 2 depicts a software architectural view of a mobile communications device according to one embodiment. A multi-layer transport stack (TS) 206 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network.

[0023] As illustrated in the embodiment of Figure 2, an integration layer 204A is operable as an interface between a radio layer 202 and the transport stack 206 of mobile communications device 116. Likewise, another integration layer 204B is provided for interfacing between the transport stack 206 and a user applications layer 207 supported on the mobile communications device 116, e.g., email 208, calendar/scheduler 210, contact management 212 and browser 214. Although not specifically shown, the transport stack 206 may also be interfaced with the operating system of mobile communications device 116. In another implementation, the transport stack 206 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. As seen in Figure 2, a usage control module 216 is coupled to radio layer 202 and transport stack 206. Usage control module 216 is operable to assist the user of mobile communications device 116 in controlling his or her usage of wireless services in a manner described more fully below.

[0024] The bottom layer (Layer 1) of the transport stack 206 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 100 shown in Figure 1. For example, when a mobile communications device roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the mobile communications device. The remaining two layers of the transport stack 206, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively.

[0025] Figure 3 depicts a block diagram of a mobile communications device according to one embodiment. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of mobile communications device 116 may comprise an arrangement similar to one shown in Figure 3, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Accordingly, the arrangement of Figure 3 should be taken as illustrative rather than limiting with respect to the embodiments of the present disclosure.

[0026] A microprocessor 302 providing for the overall control of an embodiment of mobile communications device 116 is operably coupled to a communication subsystem 304 which includes a receiver 308 and transmitter 314 as well as associated components such as one or more local oscillator (LO) modules 310 and a processing module such as a digital signal processor 312. As will be apparent to those skilled in the field of communications, the particular design of the communication module 304 may be dependent upon the communications network with which the mobile communications device 116 is intended to operate.

[0027] In one embodiment, the communication module 304 is operable with both voice and data communica-

tions. Regardless of the particular design, however, signals received by antenna 306 through base station 114 are provided to receiver 308, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, analog-to-digital (A/D) conversion, and the like. Similarly, signals to be transmitted are processed, including modulation and encoding, for example, by digital signal processor 312, and provided to transmitter 314 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 316.

[0028] Microprocessor 302 also interfaces with further device subsystems such as auxiliary input/output (I/O) 318, serial port 320, display 322, keyboard 324, speaker 326, microphone 328, random access memory (RAM) 330, a short-range communications subsystem 332, and any other device subsystems generally labeled as reference numeral 333. To control access, a Subscriber Identity Module (SIM) or Removable User Identity Module (RUIM) interface 334 is also provided in communication with the microprocessor 302.

[0029] In one implementation, SIM/RUIM interface 334 is operable with a SIM/RUIM card having a number of key configurations 344 and other information 346 such as identification and subscriber-related data. Operating system software and transport stack software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 335. In one implementation, Flash memory 335 may be segregated into different areas, e.g., storage area for computer programs 336 as well as data storage regions such as device state 337, address book 339, other personal information manager (PIM) data 341, and other data storage areas generally labeled as reference numeral 343. Usage control module 216 is operably connected to flash memory 335, including transport stack 206, as shown. In one exemplary implementation, the logic associated with the usage control module 216 is operable to access one or more storage areas, e.g., non-volatile storage areas 335, that contain various values relative to monitoring resource usage (i.e., resource consumption data) as will be set forth below. Additionally, the logic associated with the usage control module 216 is operable to access the subscriber's usage plan profile (e.g., a cellular telephone voice communication service plan profile, a wireless data transmission service plan profile, etc., which may be locally stored (e.g., in non-volatile areas), or downloaded, or otherwise available to the mobile communications device) for purposes of effectuating resource usage monitoring and/or throttling.

[0030] Figure 4 depicts a flow chart detailing the operation of usage control module 216 according to one embodiment. The process begins in block 400 with acquisition of the subscriber's usage plan profile, which includes at least one resource usage limit. Such limits may include, for example, limits as to the total number of on-peak cellular voice minutes per month, limits as to the total number of megabytes of data per month and/or limits as to the number of short messaging service (SMS) messages sent per month, as examples.

[0031] After the usage plan profile is acquired in block 400, the present date and time is acquired in block 402, along with the date and time of the beginning of the current billing period in block 404. Generally, the billing period will be one month and will begin at 12:00 am on a particular day of each month, but there is nothing within the spirit and scope of the present disclosure limiting the methods herein to such an arrangement. Given the date and time for the beginning of the current period and the current date and time, the usage control module 216 can determine the elapsed time since the beginning of the current billing period, as elaborated in block 406.

[0032] The date and time for the end of the current billing period is acquired in block 408. Given the date and time of the beginning of the current billing period and the date and time of the end of the current billing period, the usage control module 216 can calculate the total time of the current billing period, as elaborated in block 410.

[0033] The usage control module 216 acquires the quantity of current period usage of at least one limited wireless resource in block 412. This resource may be on-peak cellular voice minutes, megabytes of data or quantity of SMS messages, as examples. Given the total amount of the wireless resource available in the current billing period and the total amount of usage of that wireless resource so far in the current billing period, the usage control module 216 calculates, in block 414, a usage quotient representing the proportion of the resource which has already been consumed in the current billing period. For example, if the subscriber's service plan provides for 200 on peak minutes per month and the subscriber has used 100 minutes, the usage quotient would equal 100/200, or 50%.

[0034] In a similar manner, the usage control module 216 calculates, using the quantity of time elapsed in the current billing period and the total length of the current billing period, an elapsed days quotient representing the proportion of time in the current billing period which has already elapsed. For example, if the current month has 30 days, and 9 days have elapsed, the elapsed days quotient would equal 9/30, or 30%. This step is elaborated in block 416. The usage quotient and elapsed days quotient may be displayed to the user or provided to a management entity (block 418).

[0035] Process flow subsequent to block 418 is dependent on the relative values of the calculated statistics such as the usage quotient and the elapsed days quotient. If the proportion of the resource consumed in the current billing period is at or below the proportion of time elapsed in the current billing period, then the subscriber is unlikely to exceed the limit specified in the service plan and no corrective action is necessary. If, however, the proportion of the resource consumed in the current billing period exceeds the proportion of time elapsed so far in the current billing period, then the subscriber is consum-

ing the limited resource at a rate making it likely that he or she will exceed the limit specified in the service plan, and corrective action may be necessary, as elaborated in detail below.

[0036] In decision block 420, usage control module 216 inquires as to whether the usage quotient (designated E) is greater than the elapsed days quotient (designated F). If the usage quotient is not greater than the elapsed days quotient, then there is not significant cause for alarm and process flow proceeds to decision block 422. If the usage quotient is greater than the elapsed days quotient, then there is cause for alarm and process flow proceeds to block 424.

[0037] In the event that the subscriber is on track to meet or undershoot his or her usage limit for the current billing period, and process flow has proceeded to decision block 422, the usage control module 216 determines whether the subscriber's wireless access is currently being "throttled" by the usage control module 216. In other words, usage control module 216 determines whether prior usage conditions have placed usage control module 216 in a mode in which it is restricting the subscriber's access to wireless services. Such a restriction may include, for example, a reduced data transfer rate, or some limit as to the number of cellular voice minutes or SMS messages available per day or per hour.

[0038] If the subscriber's wireless access is not being throttled by usage control module 216, then process flow proceeds to block 428, wherein the current cycle of the wireless access control process comes to an end. If the subscriber's wireless access is, however, being throttled by usage control module 216 due to a previous overrun, then process flow proceeds to block 426, wherein usage control module 216 adjusts the wireless access parameters for mobile communications device 116.

[0039] In certain embodiments, adjustment of the throttled wireless access parameters may entail removal of all throttling of wireless access once the usage quotient equals or is less than the elapsed days quotient. In other embodiments, adjustment of the wireless access parameters may entail a reduction in the degree of throttling proportional to the difference between the usage quotient and the elapsed days quotient. In such an embodiment, so long as the usage quotient is only slightly lower than the elapsed days quotient, a certain level of throttling may continue to be imposed, with the goal of generating a "buffer" of wireless resources. In any event, after adjustment of the wireless access parameters, process flow proceeds to block 428, where the current cycle of the wireless access control process ends.

[0040] Returning to block 420, when the usage quotient exceeds the elapsed days quotient, reflecting the fact that the subscriber is consuming wireless resources at a rate expected to result in a budget overrun, process flow will proceed from block 420 to block 424. In block 424, usage control module 216 will determine whether the subscriber or some other party has activated an alarm function. The usage control module may have the capability to provide wireless usage overrun alarms to the subscriber and/or to other individuals or components in a network. If the alarm function is activated, process flow proceeds to block 430, wherein at least one alarm is generated to at least one individual or network component, and then to block 432. This alarm may be of any a number of types, including audio, video and tactile alarms. If the alarm function is deactivated, process flow proceeds directly to block 432.

[0041] In block 432, usage control module 216 determines whether the wireless resource throttling function has been activated, either by the subscriber or by some other individual or component. If the wireless resource throttling function has not been activated, process flow proceeds directly to block 428, where the current cycle of the wireless access control process ends. If the wireless resource throttling function has been activated, process flow proceeds to block 434.

[0042] In block 434, usage control module 216 adjusts wireless access parameters in order to control consumption of one or more wireless resources by the subscriber. As described above, in certain embodiments, the throttling may take the form of a pre-set usage limit imposed whenever throttling is deemed necessary. In other embodiments, the usage limit may vary within a range. The usage limit may vary, for example, according to the difference between the usage quotient and the elapsed days quotient. In such an arrangement, where the usage quotient of a wireless resource exceeds the elapsed days by 10%, the usage control module may reduce the maximum rate of consumption of the wireless resource by a proportional percentage, which could be 10%, 20% or 5%, as examples. In certain embodiments, the degree of throttling may be linearly proportional to the degree of projected overrun, while in others the degree of throttling may be geometrically proportional, so that minor overruns would have negligible effects on bandwidth, which would become increasingly dramatic as usage overruns increased. Any and all of the above are within the spirit and scope of the present disclosure. After the parameters are adjusted by the specific algorithm employed, process flow then proceeds from block 434 to block 428, where the current cycle ends.

[0043] Figure 5 depicts one embodiment of a user interface screen 500 for a mobile communications device. For example, screen 500 displays information to the user of mobile communications device 116. Certain information, such as time readout 504, will generally be presented on screen 500 in textual format. In order to maximize special efficiency, however, other information is presented on screen 500 in a graphical format including a set of descriptive icons. Representative icons shown on screen 500 include a wireless signal strength icon 502, a battery strength icon 506, contacts icon 508, calendar icon 510, message icon 512 and wireless resource usage icon 514.

[0044] Each of icons 502, 506, 508, 510, 512, 514 has a specific function within mobile communications device 116, and each may generally be associated with a spe-

cific software application. Contacts icon 508, for example, may generally be associated with a software application such as contact management application 212 (shown in Figure 2), while calendar icon 510 and message icon 512 may be associated with calendar/scheduler application 210 and email application 208, respectively.

[0045] Wireless resource usage icon 514 is exemplified with three separate horizontal bars that may represent different parameters depending on the application. In one embodiment, one bar may represent the passage of time over the billing period, a second bar may represent peak cellular voice minutes used in the current billing period and a third bar may represent data bandwidth used in the current billing period. By comparing the size of bars representing wireless resource usage to the size of bars representing the passage of time, a subscriber can monitor his or her rate of usage. In alternate embodiments, the bars may represent other parameters, which may include the number of off-peak cellular telephone voice minutes used and/or the number of SMS messages sent/received in the current billing period, as examples.

[0046] An alternative embodiment of a display screen is shown in Figure 6 and designated 600. Display screen 600 is similar to screen 500, having a signal strength meter icon 602, a current time display 604, a battery strength meter icon 606, a contacts icon 608, a calendar icon 610 and a message icon 612, each of which corresponds to a similar icon depicted in Figure 5. In contrast to display screen 500, display screen 600 has a rotary wireless resource usage icon 614 in place of the horizontal bar wireless resource usage icon 514 shown in Figure 5. In place of linear bars, wireless resource usage icon 614 employs rotary elements, including a needle pivoting about the center of the icon and a sector and marker disposed at the circumference thereof. Any of the elements may represent any of the parameters heretofore described.

[0047] Figure 7 depicts display screen 500 at a separate point in time at which an embodiment of the user interface application for usage control module 216 is open. An elapsed days graphical indicator 516 reflects the proportion of the current billing period elapsed as compared to the total span of the current billing period. Similarly, voice minutes graphical indicator 518 and data resources graphical indicator 520 reflect the proportion of each resource consumed as compared to the total amount of each resource available in the current billing period. Textual indicators 522, 524, 526 provide the same information as graphical resource indicators 516, 518, 520, but in alphanumeric rather than graphical format.

[0048] By comparing the state of resource indicators 518, 520, 524, 526 to elapsed days indicators 516, 522, a subscriber can quickly determine whether his or her rate of usage is likely to exceed the allotted resources for the current billing period. In order to assist the subscriber in controlling resource usage, a throttling indicator 528 reflects whether or not wireless bandwidth throttling is currently activated. In certain embodiments, throttling may be controlled by the subscriber, while in other embodiments throttling may be controlled partly or completely by a process external to mobile communications device 116 or by another individual.

[0049] Display screen 500 as shown in Figure 7 is only representative of one embodiment of the present disclosure. Alternative embodiments may incorporate additional information or less information. In certain embodiments, for example, the throttling indicator 528 may reflect a variable quantity representing the degree of throttling being imposed on wireless communications rather than functioning as a simple on/off indicator as shown in Figure 7. In certain other embodiments, an alarm control indicator may be included as part of the display. These and other variations are within the spirit and scope of the present disclosure.

[0050] Figure 8 depicts a display screen 850 designed to assist enterprise managers in controlling wireless resource usage at the department level. A set of employees having mobile communications devices are displayed in tabular format. For a first employee, Alex Jones, a set of resource bars 852, 854, 856 are shown reflecting the level of Alex Jones' usage of certain wireless resources in the current billing period. The information for an employee also includes his or her name 858, employee number 860 and telephone number 862. The information also includes a throttling control indicator 864. In certain embodiments, throttling control indicator 864 may only reflect whether throttling is activated on the employee's mobile communications device, while in other embodiments it may control whether throttling is activated. While not specifically described for each person shown, the same information is presented for each of the seven individuals, as seen in Figure 8.

[0051] A department summary is included in the lower-right corner of Figure 8, which reflects the total resource usage for the department. This information is provided via graphical resource usage indicators 880, 882, 884 along with textual resource usage indicators 886, 888 and an estimated budget overrun amount 890. Given this information, a manager can budget, and in certain cases control, wireless resource usage within his or her department.

[0052] Corporate control of resource usage can be employed in a number of ways. In certain embodiments, a manager may be given the power to disallow resource usage above a certain limit, which may be expressed in minutes, megabytes or dollars, as examples. A manager may also be tasked with the option to allow unlimited usage through the admin tool. In certain embodiments, the management console may show data for one or more users spanning multiple billing periods. Assuming a user is consistently over or under one or more of his or her allocated resource limits, the management console may highlight the user to the manager for possible plan alteration.

[0053] In embodiments employing some form of usage

throttling mechanism, the manner of usage throttling can vary depending on the application. One method of throttling is depicted in Figure 9. According to the embodiment of Figure 9, throttling is imposed when data usage is higher than expected, while a data boost may be provided when data usage is lower than expected.

[0054] Process flow begins in block 902 and proceeds from there to decision block 904. In decision block 904, a data usage control module, which may include logic or software instructions, determines whether data usage has been greater than expected. If usage is greater than expected, process flow is directed to block 906, where the data usage control module slows down the data transfer rate. If usage is not greater than expected, process flow is directed to decision block 908.

[0055] In decision block 908, data usage control module determines whether usage is less than expected. If data usage is less than expected, process flow is directed to block 910, where the data usage control module speeds up the data transfer rate. If data usage is not less than expected, no throttling mechanism is imposed process flow is directed to block 912, where the process ends.

[0056] As those of skill in the art will appreciate, the present disclosure encompasses a wide variety of individual embodiments and applications within its broader teachings. For example, in certain embodiments, a mobile communications device may be operable to query for a period beginning and period end (or beginning and duration) and from this information measure the elapsed time by comparing the difference from the beginning to the current time on the device against the duration. Also, the device may be operable to measure consumption since the beginning of the billing period.

[0057] In an alternate embodiment, a server may supply the proportion between the resources used and resources available as well as between the time elapsed and time available directly to the device, such that little or no computation is required on the device itself. In certain embodiments, a system may be operable to work with non-periodic "pay as you go" plans. Such a system may, for example, display a portion of used vs. total available resources since the last resource purchase, where the used indicator resets to 0 at the time of purchase. Alternatively, the system may display the remaining resources as a bulk quantity. The current available resources may be acquired from a server, or the system can maintain its own running total by adding up all the purchases and subtracting out the measured usage. In addition, such a "pay as you go" system may display the remaining number of days, projected based on the current consumption rate.

[0058] In certain applications, a combination of the above may be employed. Where, for example, a customer has purchased a monthly plan which provides for a certain level of resources while allowing for the pre-purchase of additional resources during the billing period, the elapsed time vs. time period display would remain, though the resource usage bars could actually go "backward" to reflect the additional resource capacity available after additional resources are purchased.

[0059] In certain embodiments, the resource usage bars may change in appearance if maximum resource usage is exceeded. According to one embodiment, the bar length is proportional to the usage percentage up until 100% of resource usage is reached. After 100% of available resource usage is exceeded, the bar length may then be proportional to the fraction of the planned 100% vs. the running total usage. In certain embodiments, the color or other appearance characteristic of the bars may change at this transition. Further, the device may be operable to display the current price or expense per unit time being incurred by usage of the resource.

[0060] The device may be operable to take into account any periods during which additional resource usage does not incur additional cost under the current billing plan. These may include, for example, nights and weekends. When the device is operating within an unlimited usage period, the usage indicator may be hidden or grayed out.

[0061] Billing plan details stored within the device or elsewhere may contain information about any number of overlapping conditional periods. The server may simply provide the current utilization ratios directly. Alternately, the server may provide static information about the plan, such as the starting and ending conditions for a given period, which may include the time of day or day of the week. From this information, the device could then determine the period within which it is operating and the quantity of resources consumed. Alternately, the device may calculate the ratios from durations and current consumption and elapsed time values provided by the server.

[0062] In certain embodiments, the device may be operable to display the level of resource utilization incurred within a number of different periods without respect to the period within which the device is currently operating.

[0063] In certain embodiments, the device may roam to a network on which it does not have pre-allocated resources. In this situation, the device is in a similar situation to that in which all pre-paid resources have been consumed. In this situation, the device may be operable to begin displaying the immediate rate of resource usage in either resource terms or monetary terms.

[0064] It is believed that the operation and construction of the embodiments of the present disclosure will be apparent from the Detailed Description set forth above. While the exemplary embodiments shown and described may have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present disclosure as set forth in the following claims.

Claims

1. A method for monitoring resource usage of a mobile communications device (116) comprising the steps of:

   acquiring (400) a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period;
   acquiring (402, 404, 408, 412) resource consumption data relative to the specified calendar period;
   calculating (414, 416) usage statistics based on the resource consumption data and the plan profile; and
   presenting (418) the usage statistics to an entity.

2. The method of claim 1 wherein the specified calendar period is a month.

3. The method of claim 1 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

4. The method of claim 1 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

5. The method of claim 1 wherein the usage statistics are displayed to a user of the mobile communications device.

6. The method of claim 1 wherein an alert is generated depending on the usage statistics.

7. A mobile communications device (116) comprising:

   at least one storage area (335) for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period;
   at least one storage area (335) for containing resource consumption data relative to the specified period; and
   a wireless resource usage control module (216) for calculating usage statistics based on the resource consumption data and the service plan profile.

8. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

9. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

10. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to throttle the amount of bandwidth provided depending on the usage statistics.

11. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to generate an alert depending on the usage statistics.

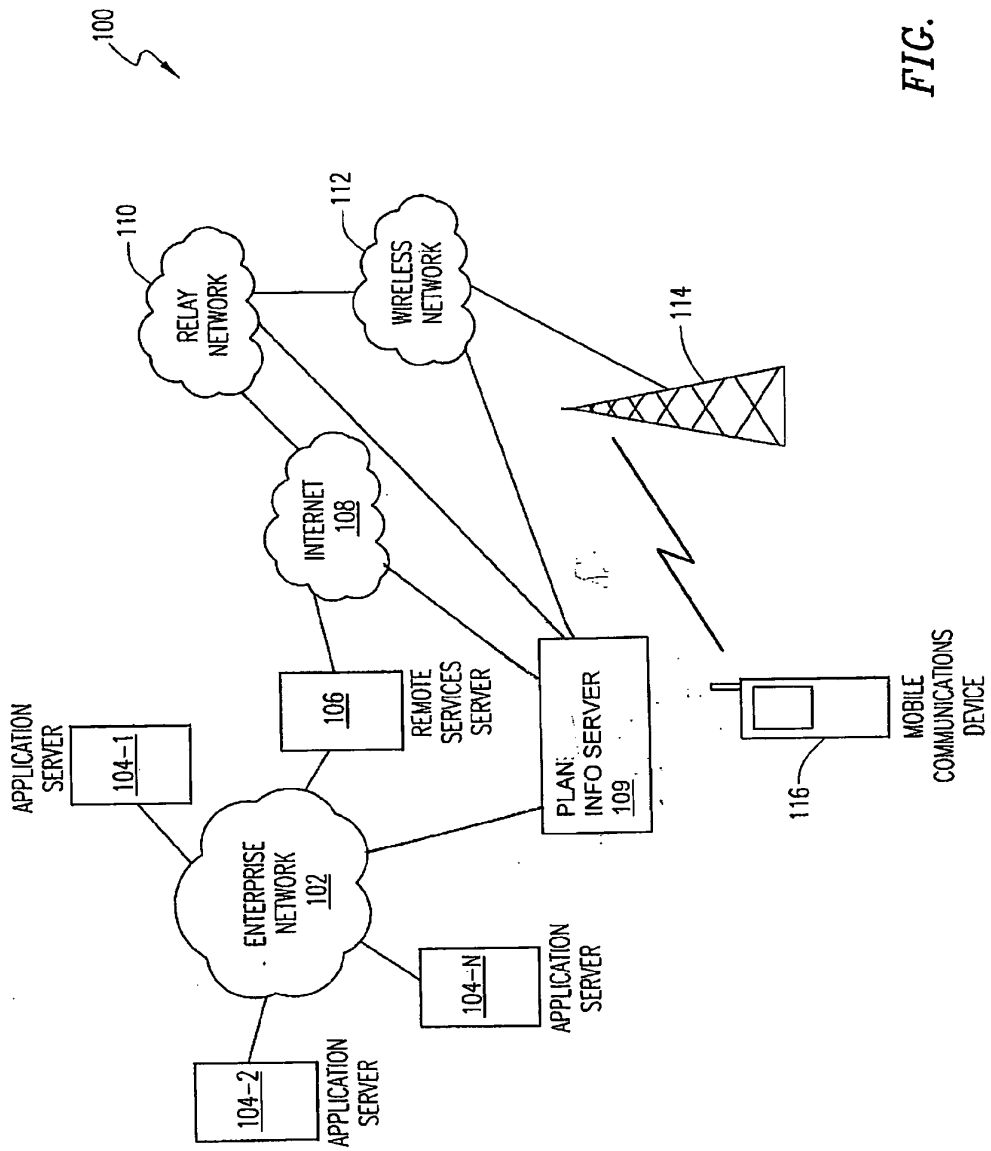

100
110
RELAY NETWORK
112
WIRELESS NETWORK
114
INTERNET 108
106
REMOTE SERVICES SERVER
PLAN INFO SERVER 109
APPLICATION SERVER
104-1
ENTERPRISE NETWORK 102
104-N
APPLICATION SERVER
104-2
APPLICATION SERVER
116
MOBILE COMMUNICATIONS DEVICE

FIG. 1

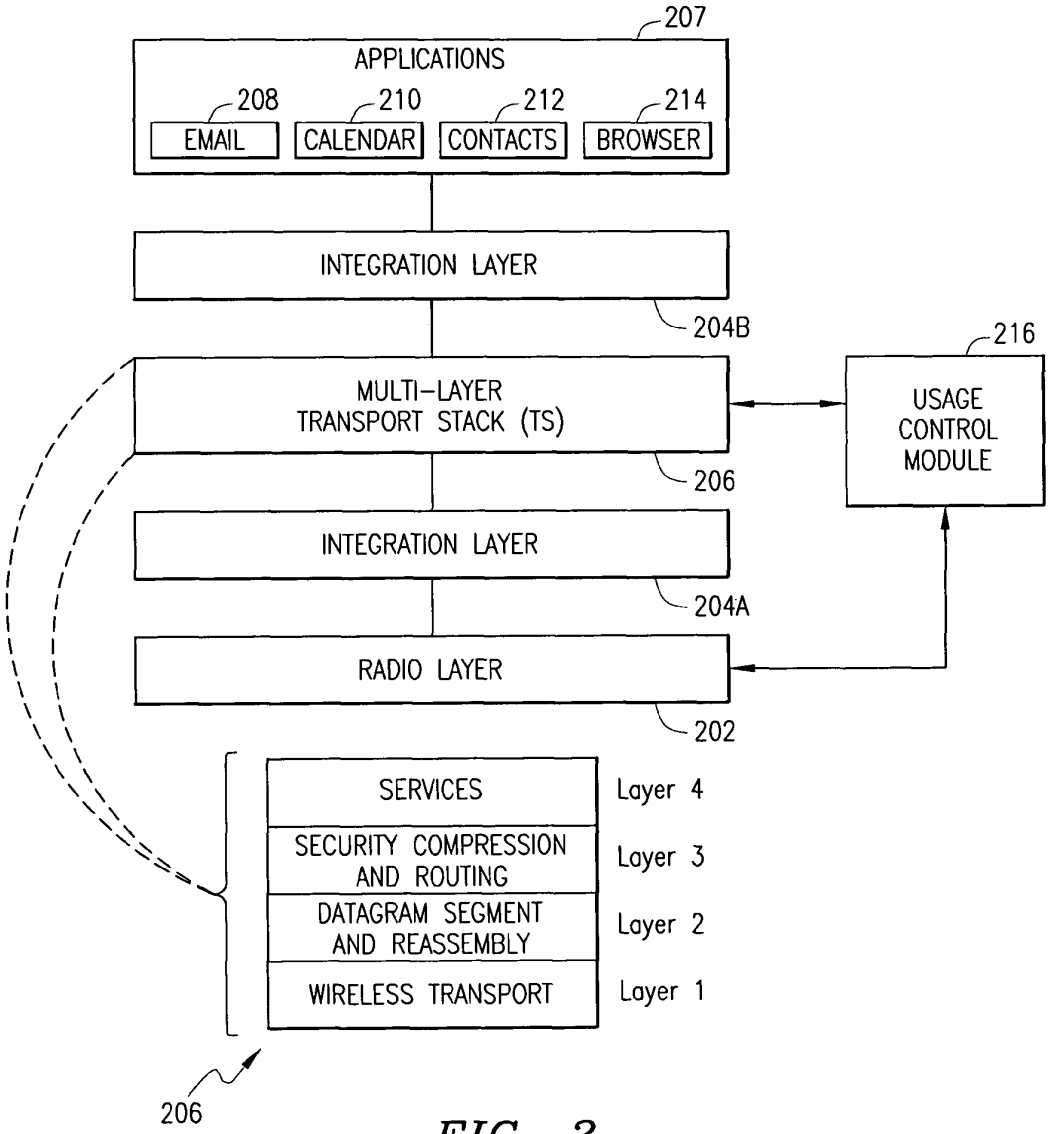

207
APPLICATIONS
208
EMAIL
210
CALENDAR
212
CONTACTS
214
BROWSER
INTEGRATION LAYER
204B
216
MULTI-LAYER
TRANSPORT STACK (TS)
USAGE
CONTROL
MODULE
206
INTEGRATION LAYER
204A
RADIO LAYER
202
SERVICES
Layer 4
SECURITY COMPRESSION
AND ROUTING
Layer 3
DATAGRAM SEGMENT
AND REASSEMBLY
Layer 2
WIRELESS TRANSPORT
Layer 1
206

FIG. 2

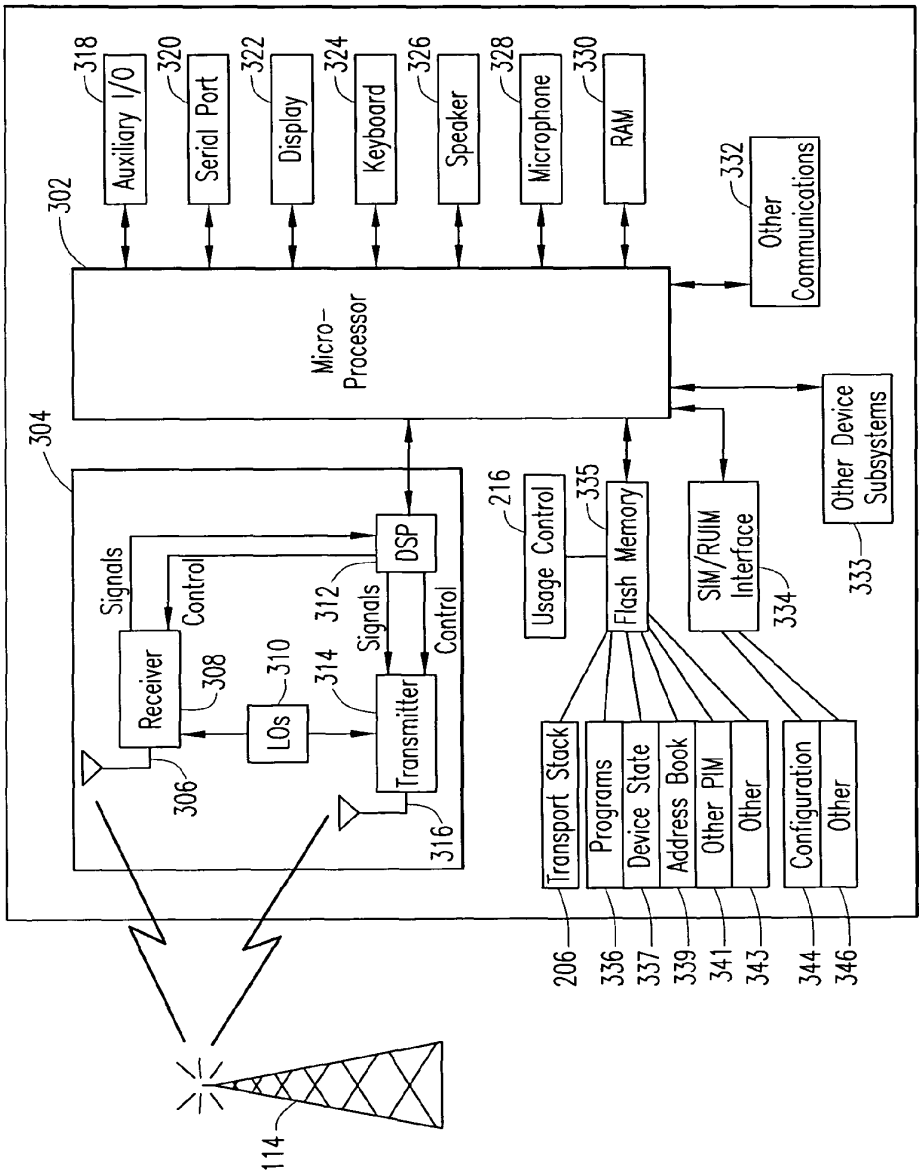

318
Auxiliary I/O
320
Serial Port
322
Display
324
Keyboard
326
Speaker
328
Microphone
330
RAM
332
Other Communications
302
Micro-Processor
304
Signals
Control
Receiver
308
306
LOs
310
314
312
Signals
Control
DSP
Transmitter
316
216
Usage Control
335
Flash Memory
SIM/RUIM Interface
334
333
Other Device Subsystems
Transport Stack
Programs
Device State
Address Book
Other PIM
Other
Configuration
Other
206
336
337
339
341
343
344
346
114

FIG. 3

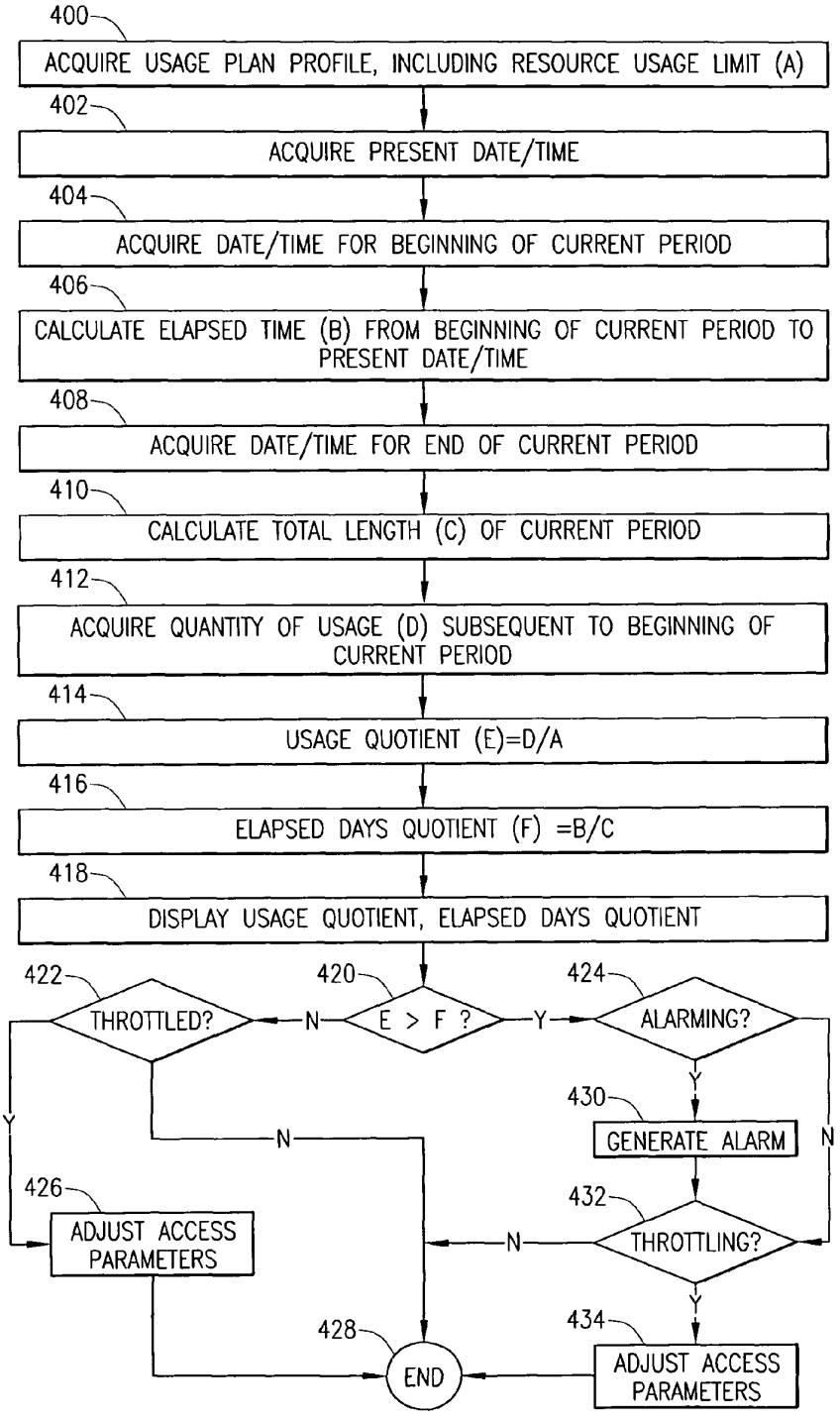

400
ACQUIRE USAGE PLAN PROFILE, INCLUDING RESOURCE USAGE LIMIT (A)
402
ACQUIRE PRESENT DATE/TIME
404
ACQUIRE DATE/TIME FOR BEGINNING OF CURRENT PERIOD
406
CALCULATE ELAPSED TIME (B) FROM BEGINNING OF CURRENT PERIOD TO PRESENT DATE/TIME
408
ACQUIRE DATE/TIME FOR END OF CURRENT PERIOD
410
CALCULATE TOTAL LENGTH (C) OF CURRENT PERIOD
412
ACQUIRE QUANTITY OF USAGE (D) SUBSEQUENT TO BEGINNING OF CURRENT PERIOD
414
USAGE QUOTIENT (E)=D/A
416
ELAPSED DAYS QUOTIENT (F) =B/C
418
DISPLAY USAGE QUOTIENT, ELAPSED DAYS QUOTIENT
420
E > F ?
N
Y
422
THROTTLED?
424
ALARMING?
Y
N
430
GENERATE ALARM
Y
N
426
ADJUST ACCESS PARAMETERS
432
THROTTLING?
N
Y
428
END
434
ADJUST ACCESS PARAMETERS

FIG. 4

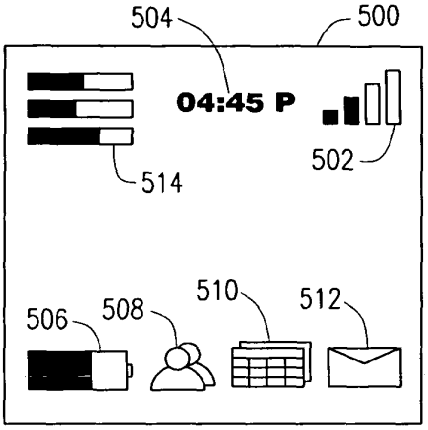


FIG. 5

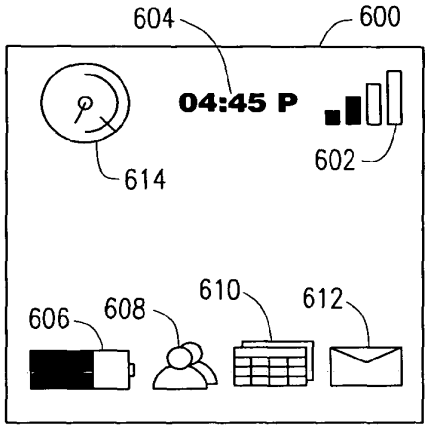


FIG. 6

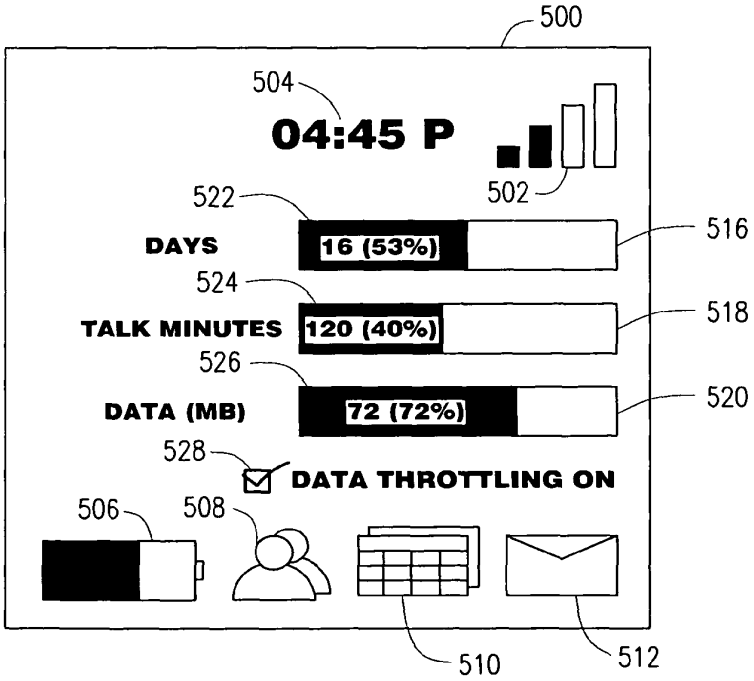


FIG. 7

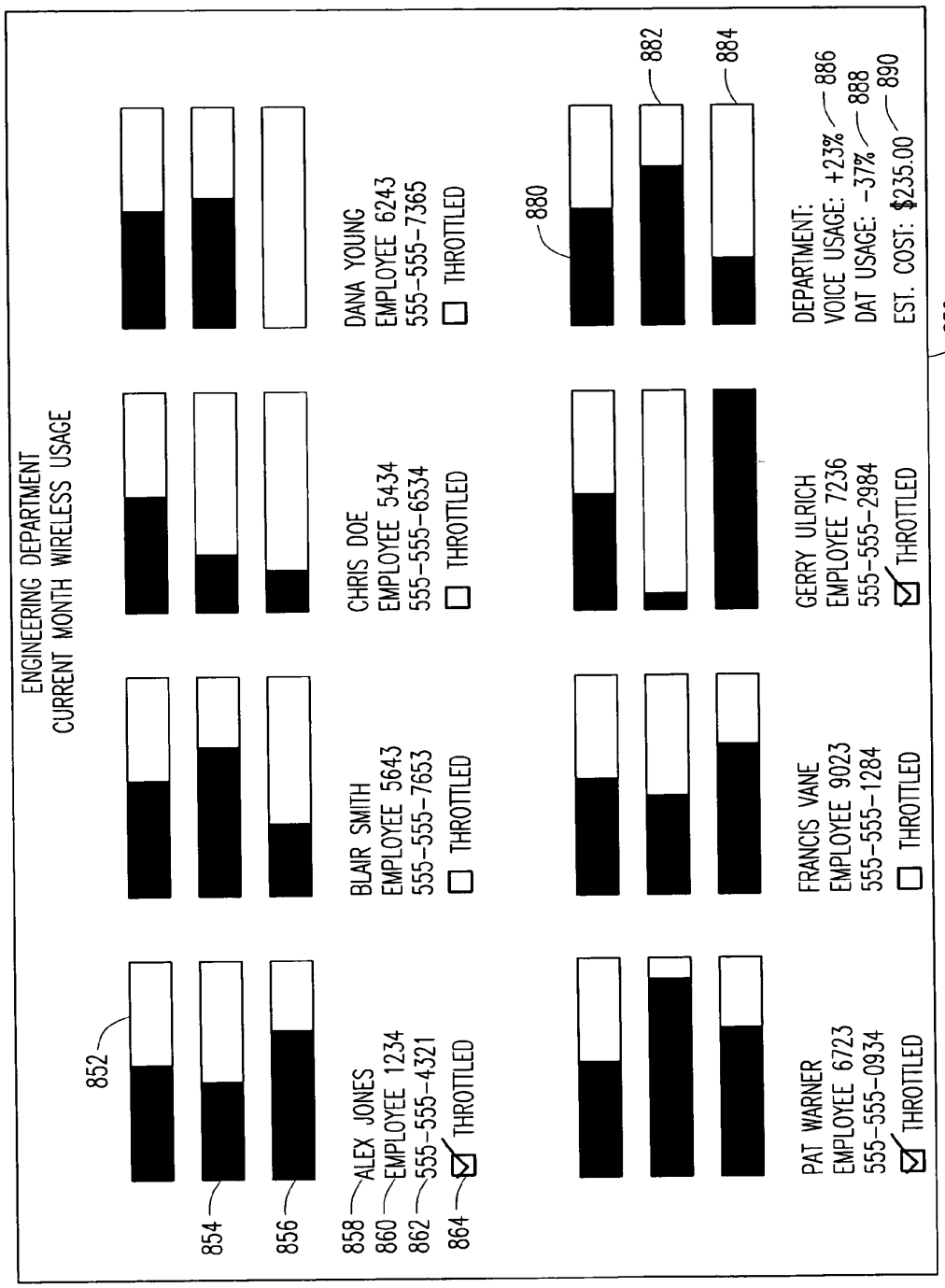

ENGINEERING DEPARTMENT
CURRENT MONTH WIRELESS USAGE
852
854
856
858 ALEX JONES
860 EMPLOYEE 1234
862 555-555-4321
864 THROTTLED
BLAIR SMITH
EMPLOYEE 5643
555-555-7653
THROTTLED
CHRIS DOE
EMPLOYEE 5434
555-555-6534
THROTTLED
DANA YOUNG
EMPLOYEE 6243
555-555-7365
THROTTLED
880
882
884
PAT WARNER
EMPLOYEE 6723
555-555-0934
THROTTLED
FRANCIS VANE
EMPLOYEE 9023
555-555-1284
THROTTLED
GERRY ULRICH
EMPLOYEE 7236
555-555-2984
THROTTLED
DEPARTMENT:
VOICE USAGE: +23% 886
DAT USAGE: -37% 888
EST. COST: $235.00 890
850

FIG. 8

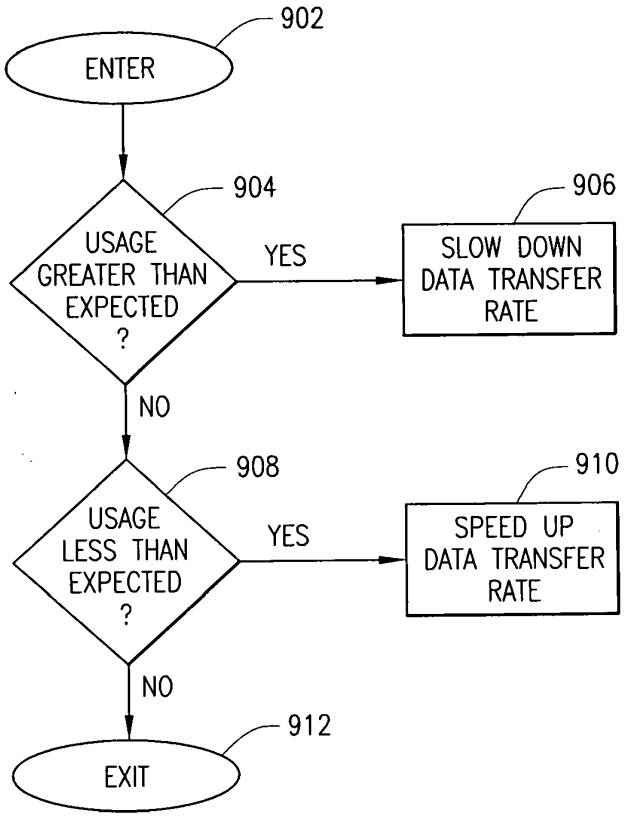

902
ENTER
904
USAGE GREATER THAN EXPECTED ?
YES
906
SLOW DOWN DATA TRANSFER RATE
NO
908
USAGE LESS THAN EXPECTED ?
YES
910
SPEED UP DATA TRANSFER RATE
NO
912
EXIT

FIG. 9

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2001/055961 A1 (NAKAJIMA TAKETOSI) 27 December 2001 (2001-12-27) * paragraphs [0023] - [0046] * * figures 1,2 *	1,2,4-7, 9-11	INV. H04M15/28 H04M17/00 ADD. H04Q7/32 H04Q7/38
X	WO 00/70860 A (ERICSSON, INC) 23 November 2000 (2000-11-23) * page 8, line 6 - page 9, line 16 * * page 12, line 13 - page 17, line 17 * * figures 3,4,9,10,11A,11B *	1-9,11	
X	EP 1 528 781 A (BOUYGUES TELECOM) 4 May 2005 (2005-05-04) * paragraphs [0002], [0003], [0019] - [0032], [0034], [0040], [0045] * * figures 1-6 *	1-5,7-9	
X	WO 02/058326 A (TELEFONAKTIEBOLAGET L M ERICSSON ; ERICSSON, ANDREAS) 25 July 2002 (2002-07-25) * page 3, line 13 - page 6, line 15 * * page 8, lines 9-25 * * figures 1-3 *	1,2,4-7, 9,11	TECHNICAL FIELDS SEARCHED (IPC) H04M H04Q
X	WO 2004/030390 A (BRIGHT STAR TECHNOLOGIES, INC; BEKANICH, JOSEPH) 8 April 2004 (2004-04-08) * page 15, line 22 - page 21, line 21 * * page 26, line 14 - page 27, line 20 * * figures 8-13 *	1-9,11	
X	US 2002/151293 A1 (TYSOR ARTHUR JAMES) 17 October 2002 (2002-10-17) * paragraphs [0022] - [0048] * * figures 3,5A,5B,6 *	1-3,5-8, 11	

-/--

1 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2006/000994 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; MOTTE, STEFAAN; MASSCHELEIN, MARC) 5 January 2006 (2006-01-05) * page 3, line 31 - page 6, line 18 * -----	7,9,10	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 25 2276

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-06-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001055961 A1	27-12-2001	CN 1305268 A	25-07-2001
		GB 2364213 A	16-01-2002
		HK 1036703 A1	30-06-2005
		JP 3509670 B2	22-03-2004
		JP 2001168916 A	22-06-2001
WO 0070860 A	23-11-2000	AT 303038 T	15-09-2005
		AU 4465100 A	05-12-2000
		CN 1361974 A	31-07-2002
		DE 60022181 D1	29-09-2005
		DE 60022181 T2	01-06-2006
		EP 1179262 A1	13-02-2002
		JP 2003500904 T	07-01-2003
		US 6493547 B1	10-12-2002
EP 1528781 A	04-05-2005	FR 2861942 A1	06-05-2005
WO 02058326 A	25-07-2002	JP 2004517586 T	10-06-2004
WO 2004030390 A	08-04-2004	NONE	
US 2002151293 A1	17-10-2002	NONE	
WO 2006000994 A	05-01-2006	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Electronic Patent Application Fee Transmittal

Application Number:	14667353
Filing Date:	24-Mar-2015
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	23748543
Application Number:	14667353
International Application Number:	
Confirmation Number:	8845
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3
Receipt Date:	09-OCT-2015
Filing Date:	24-MAR-2015
Time Stamp:	19:17:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	4741
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P007C11C3_OAR.pdf	130636 8076de5792ad42a5099654145dfebacda73639e8	yes	14
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	14	
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3_IDS.pdf	615907 d0994dbe2c9bc9187ed43bd194e19bd5fe10b625	no	15
Warnings:					
Information:					
3	Foreign Reference	2066_Fujitsu.pdf	856885 72e75495c5d83e30e4fbefee0e38a1bb25a5405f	no	22
Warnings:					
Information:					
4	Foreign Reference	2067_Kyocera.pdf	641903 024bbc366c4ffca0d6206fd9400790e51cab71c3	no	27
Warnings:					
Information:					
5	Foreign Reference	2068_Citrix.pdf	14110049 6b5308424d6052f222f99c6297e0f2cd005b02d2	no	118
Warnings:					
Information:					
6	Foreign Reference	2069_CN1508734A.pdf	3021193 c8818fe2ac00cd927bb1eb76517cffb16566e7c4	no	24

Warnings:					
Information:					
7	Foreign Reference	2070_CA2688553.pdf	2542550 eaac858569669488781074475 9dc83d1126bb215	no	72
Warnings:					
Information:					
8	Foreign Reference	2071_EP1850575A1.pdf	306349 f0b875706a2088fd443e7a61ffec5c6632823551	no	18
Warnings:					
Information:					
9	Non Patent Literature	3044_Jing.pdf	233308 23bf275a591ba14bba9ea0e8edf96ff232de6df3	no	41
Warnings:					
Information:					
10	Non Patent Literature	3045_Rivadeneyra.pdf	140975 e344ac7c8eee7e286c50068b497b45c8a4dbefbe	no	11
Warnings:					
Information:					
11	Non Patent Literature	3046_loopt.pdf	380265 711a9ba25d7f71b9274655d90ad2022e3b79c85c	no	17
Warnings:					
Information:					
12	Non Patent Literature	3047_MobilInternet.pdf	168840 0ed6b390575399526 5d6ebaf790a5696b8b5efb3	no	3
Warnings:					
Information:					
13	Non Patent Literature	3048_GoldCoast.pdf	164580 e7407b7a4570d9ebfc790e44249d0cdb07f36182	no	2
Warnings:					
Information:					
14	Non Patent Literature	3049_Richtel.pdf	92162 6eecd8013a6328084fb9f16f25afc3b9619c9dee	no	3
Warnings:					
Information:					
15	Non Patent Literature	3050_Kim.pdf	94063 d57c26581b209a675dcd915b2be9c9e56a005a1f	no	4

Warnings:					
Information:					
16	Non Patent Literature	3051_Koutsopoulou.pdf	113527 7992fa4c1d1306edb1de247f743fd1ce8b1f3e7d	no	9
Warnings:					
Information:					
17	Non Patent Literature	3052_Sun.pdf	102743 66e9aab3798130ba2a58b46d24cec206617531de	no	8
Warnings:					
Information:					
18	Non Patent Literature	3053_Sabat.pdf	389581 c6862777fa3e8b3a13a7509f02610e154cf4299d	no	31
Warnings:					
Information:					
19	Non Patent Literature	3054_Nuzman.pdf	580822 f0c09248f7c9794a5ea827b4d574c49719823113	no	19
Warnings:					
Information:					
20	Fee Worksheet (SB06)	fee-info.pdf	30614 b54bbe28546deb7e00e66eff5fab5cd5aa1b448e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	24716952	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/667,353	Filing Date 03/24/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	10/09/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/KAREN VESTAL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 11/04/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 11/04/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

TITLE OF INVENTION: Mobile device with common secure wireless message service serving multiple applications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/04/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 11/04/2015
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

TITLE OF INVENTION: Mobile device with common secure wireless message service serving multiple applications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/04/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	726-003000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

106963 7590 11/04/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 11/04/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/667,353	Applicant(s) RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *09 October 2015 Amendment*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *2-22*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant's additional Information Disclosure Statement (IDS) submitted October 9, 2015 has been reviewed. Note the attached IDS.

3. Applicant cancelled claim 1.

Allowable Subject Matter

4. Claims 2-22 are allowed.

5. The following is an examiner's statement of reasons for allowance: Claims 2-22 are allowed as the prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Further, claims 2-22 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014).

Claims 2-22 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the

following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/667,353	RALEIGH, GREGORY G.	
	Examiner	Art Unit	
	ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
370	252,351	10/28/2015	AJR
380	44,27	10/28/2015	AJR
705	28,30	10/28/2015	AJR
709	229,238	10/28/2015	AJR
713	150	10/28/2015	AJR
726	2-7	10/28/2015	AJR
455	405,406	10/28/2015	AJR
455	414.1	10/28/2015	AJR
455	432.2	10/28/2015	AJR
H04L	63/08	10/28/2015	AJR
H04L	63/10	10/28/2015	AJR
H04L	63/20	10/28/2015	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
726	**2-7**	**10/28/2015**	**AJR**
455	432.2	10/28/2015	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	10/28/2015	AJR

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	5974439	A	1999-10-26	Bollella, Gregory	
	4	6393014	B1	2002-05-21	Daly et al.	
	5	6397259	B1	2002-05-28	Lincke et al.	
	6	6445777	B1	2002-09-03	Clark, Curtis	
	7	6628934	A	2003-09-30	Rosenberg et al.	
	8	6662014	B1	2003-12-09	Walsh, Patrick Jay	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	6901440	B1	2005-05-31	Bimm et al.	
	11	6970692	B2	2005-11-29	Tysor, Arthur James	
	12	7007295	B1	2006-02-28	Rose et al.	
	13	7017189	B1	2006-03-21	DeMello et al.	
	14	7039027	B2	2006-05-02	Bridgelall, Raj	
	15	7047276	B2	2006-05-16	Liu et al.	
	16	7058022	B1	2006-06-06	Carolan et al.	
	17	7149521	B2	2006-12-12	Sundar et al.	
	18	7162237	B1	2007-01-09	Silver et al.	
	19	7200112	B2	2007-04-03	Sundar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	20	7203752	B2	2007-04-10	Rice et al.	
	21	7222190	B2	2007-05-22	Klinker et al.	
	22	7224968	B2	2007-05-29	Dobson et al.	
	23	7266371	B1	2007-09-04	Amin et al.	
	24	7366654	B2	2008-04-29	Moore, Robert C.	
	25	7379731	B2	2008-05-27	Natsuno et al.	
	26	7391724	B2	2008-06-24	Alakoski et al.	
	27	7395244	B1	2008-07-01	Kingsford, Bryan	
	28	7411930	B2	2008-08-12	Montojo et al.	
	29	7454191	B2	2008-11-18	Dawson et al.	
	30	7457870	B1	2008-11-25	Lownsbrough et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	31	7508799	B2	2009-03-24	Sumner et al.	
	32	7515926	B2	2009-04-07	Bu et al.	
	33	7536695	B2	2009-05-19	Alam et al.	
	34	7554983	B1	2009-06-30	Muppala, Suresh	
	35	7564799	B2	2009-07-21	Holland et al.	
	36	7586871	B2	2009-09-08	Hamilton et al.	
	37	7627767	B2	2009-12-01	Sherman et al.	
	38	7752330	B2	2010-07-06	Olsen et al.	
	39	7792257	B1	2010-09-07	Vanier et al.	
	40	7801783	B2	2010-09-21	Kende et al.	
	41	7817615	B1	2010-10-19	Breau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	42	7844034	B1	2010-11-30	Oh et al.	
	43	7849161	B2	2010-12-07	Koch et al.	
	44	7849477	B2	2010-12-07	Cristofalo et al.	
	45	7860088	B2	2010-12-28	Lioy, Marcello	
	46	7865187	B2	2011-01-04	Ramer et al.	
	47	7894431	B2	2011-02-22	Goring et al.	
	48	7899039	B2	2011-03-01	Andreasen et al.	
	49	7933274	B2	2011-04-26	Verma et al.	
	50	7978686	B2	2011-07-12	Goyal et al.	
	51	7987496	B2	2011-07-26	Bryce et al.	
	52	7990049	B2	2011-08-02	Shioya, Shunsuke	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	53	8005726	B1	2011-08-23	Bao, Yulin	
	54	8050690	B2	2011-11-01	Neeraj, Chawla	
	55	8073427	B2	2011-12-06	Koch et al.	
	56	8086398	B2	2011-12-27	Sanchez et al.	
	57	8104080	B2	2012-01-24	Burns et al.	
	58	8107953	B2	2012-01-31	Zimmerman et al.	
	59	8112435	B2	2012-02-07	Epstein et al.	
	60	8150394	B2	2012-04-03	Bianconi et al.	
	61	8180886	B2	2012-05-15	Overcash et al.	
	62	8190122	B1	2012-05-29	Alexander et al.	
	63	8195661	B2	2012-06-05	Kalavade, Asawaree	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	64	8200163	B2	2012-06-12	Hoffman, George E.	
	65	8200818	B2	2012-06-12	Freund et al.	
	66	8208788	B2	2012-06-26	Ando et al.	
	67	8254880	B2	2012-08-28	Aaltonen et al.	
	68	8270955	B2	2012-09-18	Ramer et al.	
	69	8326828	B2	2012-12-04	Zhou et al.	
	70	8331223	B2	2012-12-11	Hill et al.	
	71	8339991	B2	2012-12-25	Biswas et al.	
	72	8358975	B2	2013-01-22	Bahl et al.	
	73	8385964	B2	2013-02-26	Haney, Richard D.	
	74	8503455	B2	2013-08-06	Heikens, Heico	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	75	8504032	B2	2013-08-06	Lott et al.	
	76	8522337	B2	2013-08-27	Adusumilli et al.	
	77	8527662	B2	2013-09-03	Biswas et al.	
	78	8533775	B2	2013-09-10	Alcorn et al.	
	79	8538394	B2	2013-09-17	Zimmerman et al.	
	80	8538458	B2	2013-09-17	Haney, Richard D.	
	81	8565746	B2	2013-10-22	Hoffman, George E.	
	82	8571501	B2	2013-10-29	Miller et al.	
	83	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	84	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	85	8644813	B1	2014-02-04	Gailloux et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	86	8667542	B1	2014-03-04	Bertz et al.	
	87	8713535	B2	2014-04-29	Malhotra et al.	
	88	8713641	B1	2014-04-29	Pagan et al.	
	89	8730842	B2	2014-05-20	Collins et al.	
	90	8732808	B2	2014-05-20	Sewall et al.	
	91	8761711	B2	2014-06-24	Grignani et al.	
	92	8793304	B2	2014-07-29	Lu et al.	
	93	8948726	B2	2015-02-03	Smith et al.	
	94	8966018	B2	2015-02-24	Bugwadia et al.	
	95	9002342	B2	2015-04-07	Tenhunen et al.	
	96	RE44412		2013-08-06	Naqvi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020154751	A1	2002-10-24	Thompson et al.	
	2	20020191573	A1	2002-12-19	Whitehill et al.	
	3	20030084321	A1	2003-05-01	Tarquini et al.	
	4	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	5	20040260766	A1	2004-12-23	Barros et al.	
	6	20050041617	A1	2005-02-24	Huotari et al.	
	7	20060095517	A1	2006-05-04	O'Connor et al.	
	8	20060098627	A1	2006-05-11	Karaoguz et al.	
	9	20060136882	A1	2006-06-22	Noonan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	10	20060143066	A1	2006-06-29	Calabria	
	11	20070073899	A1	2007-03-29	Judge et al.	
	12	20070174490	A1	2007-07-26	Choi et al.	
	13	20070234402	A1	2007-10-04	Khosravi et al.	
	14	20080018494	A1	2008-01-24	Waite et al.	
	15	20080034063	A1	2008-02-07	Yee, Robert	
	16	20090048913	A1	2009-02-19	Shenfield et al.	
	17	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
	18	20090181662	A1	2009-07-16	Fleischman et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	10/28/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667353	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC							
Symbol						**Type**	**Version**
H04W		12	/	08		F	2013-01-01
G06Q		10	/	06375		I	2013-01-01
G06Q		20	/	102		I	2013-01-01
G06Q		20	/	20		I	2013-01-01
G06Q		20	/	40		I	2013-01-01
G06Q		30	/	0207		I	2013-01-01
G06Q		30	/	0283		I	2013-01-01
G06Q		30	/	0284		I	2013-01-01
G06Q		30	/	04		I	2013-01-01
G06Q		30	/	0601		I	2013-01-01
G06Q		40	/	00		I	2013-01-01
H04L		12	/	14		I	2013-01-01
H04L		41	/	0893		A	2013-01-01
H04L		41	/	5003		I	2013-01-01
H04L		41	/	5025		A	2013-01-01
H04M		15	/	00		I	2013-01-01
H04M		15	/	58		I	2013-01-01
H04M		2215	/	0188		A	2013-01-01
H04W		4	/	24		I	2013-01-01
H04W		4	/	26		I	2013-01-01
G06F		15	/	177		I	2013-01-01
G06Q		30	/	0241		I	2013-01-01
H04L		9	/	32		I	2013-01-01
H04L		63	/	10		I	2013-01-01
H04W		28	/	02		I	2013-01-01
H04W		4	/	001		I	2013-01-01
H04W		8	/	02		A	2013-01-01
H04L		47	/	2408		I	2013-01-01
H04L		63	/	08		I	2013-01-01
H04L		67	/	306		I	2013-01-01
G06Q		40	/	12		I	2013-12-03

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 21	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	10/25/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 8

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667353	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

H04W	8	/	20	I	2013-01-01
H04W	28	/	12	I	2013-01-01
H04W	48	/	14	I	2013-01-01
H04W	88	/	08	I	2013-01-01
H04W	4	/	20	I	2013-01-01
H04W	12	/	00	I	2013-01-01
H04M	15	/	88	I	2013-01-01
H04W	28	/	0268	I	2013-01-01
H04M	15	/	61	I	2013-01-01
H04W	24	/	08	I	2013-01-01
H04W	84	/	04	A	2013-01-01
H04W	84	/	12	A	2013-01-01
H04W	12	/	02	I	2013-01-01
H04L	51	/	046	I	2013-01-01
H04L	63	/	0428	I	2013-01-01
H04W	4	/	12	I	2013-01-01
H04W	4	/	18	I	2013-01-01
H04W	8	/	18	I	2013-01-01
H04W	72	/	0453	I	2013-01-01

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**
/				
/				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 21	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	10/25/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 8

U.S. Patent and Trademark Office

Part of Paper No. 20151028

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667353	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	3	H	0	4	L	63 / 08						
CROSS REFERENCE(S)		H	0	4	L	63 / 10						
		H	0	4	L	63 / 20						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)	H	0	4	W	92 / 02 (2009.01.01)						
455	432.2											

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	10/25/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	8

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667353	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1	17	17												
1	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	2	22												
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	10/25/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	8

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6038540	A	2000-03-14	Krist et al.	
	2	6058434	A	2000-05-02	Wilt et al.	
	3	6125391	A	2000-09-26	Meltzer et al.	
	4	6735206	B1	2004-05-11	Oki et al.	
	5	6748437	B1	2004-06-08	Mankude et al.	
	6	7024460	B2	2006-04-04	Koopmas et al.	
	7	7248570	B2	2007-07-24	Bahl et al.	
	8	7512128	B2	2009-03-31	DiMambro et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	7676673	B2	2010-03-09	Weller et al.	
	10	7889384	B2	2011-02-15	Armentrout et al.	
	11	7966405	B2	2011-06-21	Sundaresan et al.	
	12	8032168	B2	2011-10-04	Ikaheimo, Jorma	
	13	8131840	B1	2012-03-06	Denker, Richard E.	
	14	8407763	B2	2013-03-26	Weller et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060075506	A1	2006-04-06	Sanda et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-11-06
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14667353
Filing Date:	24-Mar-2015
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	24009398
Application Number:	14667353
International Application Number:	
Confirmation Number:	8845
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3
Receipt Date:	06-NOV-2015
Filing Date:	24-MAR-2015
Time Stamp:	13:20:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	9758
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3_IDS.pdf	612250 e02a8c43844dfe6729118bbf8ab92ff0dd52c10c	no	5
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30614 f5df44f318129c359e2fe835bfc8a8eb312c8cb0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	642864		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 11/04/2015
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Ann Taylor	(Depositor's name)
	(Signature)
November 9, 2015	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

TITLE OF INVENTION: Mobile device with common secure wireless message service serving multiple applications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/04/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	726-003000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 James E. Harris
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Headwater Partners I LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Redwood City, CA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date November 9, 2015
Typed or printed name James E. Harris Registration No. 40013

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	14667353
Filing Date:	24-Mar-2015
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt	
EFS ID:	24024317
Application Number:	14667353
International Application Number:	
Confirmation Number:	8845
Title of Invention:	Mobile device with common secure wireless message service serving multiple applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3
Receipt Date:	09-NOV-2015
Filing Date:	24-MAR-2015
Time Stamp:	14:34:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	861
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P007C11C3_IssueFee.pdf	397727 a60aec85de6fdca926c314eda1290de66be88ebb	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30480 ca7ea24a70c6f1ccb4c2b91d0f2a67a2ccabee64	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	428207		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	03/24/2015	Gregory G. Raleigh	RALEP007C11C3	8845

106963 7590 12/03/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
12/03/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/667,353	24 March, 2015	RALEIGH, GREGORY G.	RALEP007C11C3

		EXAMINER	
Headwater Partners I LLC 555 Twin Dolphin Drive, Suite 310 Redwood Shores, CA 94065		ANDREW JOSEPH RUDY	
		ART UNIT	PAPER
		3687	20151129

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Applicant's Information Disclosure Statement (IDS) submitted November 6, 2015 has been reviewed. Note the attached IDS.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

PTO-90C (Rev.04-03)

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14667353
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6038540	A	2000-03-14	Krist et al.	
	2	6058434	A	2000-05-02	Wilt et al.	
	3	6125391	A	2000-09-26	Meltzer et al.	
	4	6735206	B1	2004-05-11	Oki et al.	
	5	6748437	B1	2004-06-08	Mankude et al.	
	6	7024460	B2	2006-04-04	Koopmas et al.	
	7	7248570	B2	2007-07-24	Bahl et al.	
	8	7512128	B2	2009-03-31	DiMambro et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	9	7676673	B2	2010-03-09	Weller et al.	
	10	7889384	B2	2011-02-15	Armentrout et al.	
	11	7966405	B2	2011-06-21	Sundaresan et al.	
	12	8032168	B2	2011-10-04	Ikaheimo, Jorma	
	13	8131840	B1	2012-03-06	Denker, Richard E.	
	14	8407763	B2	2013-03-26	Weller et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060075506	A1	2006-04-06	Sanda et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667353
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	11/25/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,353	01/05/2016	9232403	RALEP007C11C3	8845

106963 7590 12/16/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Gregory G. Raleigh, Woodside, CA;
Headwater Partners I LLC, Redwood City, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.