(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 545 114 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.06.2005 Bulletin 2005/25

(51) Int Cl.[7]: **H04M 15/00**, H04Q 3/00

(21) Application number: **04027514.1**

(22) Date of filing: **19.11.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK YU

(30) Priority: **19.12.2003 CN 200310122726**

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventors:
- **ShuGuang, Jin,**
CTO, Alcatel Shanghai Bell Co. Ltd.
201206 Shanghai (CN)
- **Yan, Chen, CTO, Alcatel Shanghai Bell Co. Ltd.**
201206 Shanghai (CN)
- **Peiliang, Xu, CTO, Alcatel Shanghai Bell Co. Ltd.**
201206 Shanghai (CN)

(74) Representative:
Dreiss, Fuhlendorf, Steimle & Becker
Patentanwälte
Postfach 10 37 62
70032 Stuttgart (DE)

(54) A method and apparatus for division of revenue of communication among different proprietors

(57) A method and apparatus for division of revenue of communication among different proprietors is provided in this invention, where the division of revenue among the different proprietors is performed by a gateway office, wherein the gateway office will set a source parameter and a destination parameter respectively from the source and the destination when a call goes through the gateway office; Judge the two parameters to get a revenue zone index; Judge the value of the revenue zone index, and modulate the revenue zone index to get a revenue class index; The gateway office generates contents related to the revenue class index; A central memory receives all these contents, adds an increment of each counter of the revenue class memory related to the revenue class index to a corresponding counter and carries out multiple safety mechanisms; Output the information in the revenue class memory to a storage medium for storing, then output it to a billing center for revenue sorting. The billing mode present in this invention is based on group pairs, so it is more adaptive for the gateway office to divide revenue.

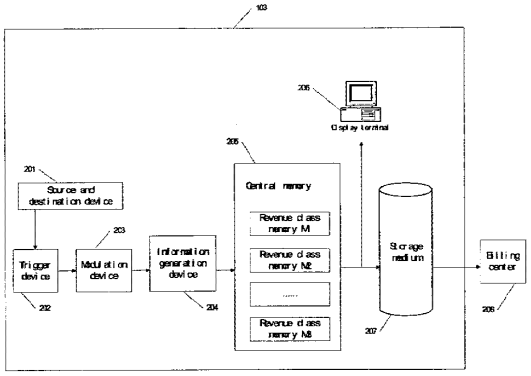


Fig. 2

Printed by Jouve, 75001 PARIS (FR)

EP 1 545 114 A1

GOOGLE EXHIBIT 1002

Description

TECHNICAL FIELD

[0001] The present invention relates to a method and apparatus for division of revenue of telecommunication among different proprietors.

RELATED ART

[0002] As to the relay jumping table billing, in the SPC exchange, it takes relay groups (income and outgoing) as revenue billing units, and accumulates all metering impulses of the relay group as the billing content. Although this technology is simple, it is not able to provide enough flexibility in resource sorting and billing content selecting.

[0003] As to the detail billing, in the SPC exchange, it generates a detail record for each call. All these records (telephone billing list) will be sent out from the SPC exchange after a specific period. A specific sorting department sorts all received telephone billing list, which will be treated as the billing content after sorting and summation. It can satisfy all kinds of user's customized demands, but there is a large number of temporary data transferring between the SPC exchange and the sorting department, and the investments on the equipments will be expanded greatly in order to satisfy demands.

SUMMARY OF THE INVENTION

[0004] In order to solve said problems of existing technology, this invention provides all kinds of methods for the division of revenue at the SPC exchange level of the gateway office, to satisfy various potential billing demands among the proprietors. Moreover, it is needless for proprietors to add investments immediately to meet with the additional demands for detail billing because of this demand.

[0005] The present invention provides a method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2... n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

[0006] In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0007] In said step f), the central memory sends the information in the revenue class memory M_j as said in step e) to a display terminal.

wherein in said step e), the multiple safety mechanisms include:

[0008] The central memory introducing a windowing mechanism during a receiving procedure;

[0009] The accumulation of each counter having a hot backup;

[0010] Each counter backups its information to a pair of hard disks with specific intervals.

wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

[0011] The present invention provides an apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device□a central memory and a storage medium which are all located in the gateway office, wherein:

[0012] When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;

[0013] The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue , the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, t the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;

[0014] The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;

[0015] The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;

[0016] The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;

[0017] The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

[0018] Wherein said contents related to the revenue class index R_j include static and dynamic information on the said call;

[0019] Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0020] Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

wherein said multiple safety mechanisms include:

[0021] The central memory introducing a windowing mechanism during a receiving procedure;

[0022] The accumulation of each counter having a hot backup;

[0023] Each counter backups its information to a pair of hard disks with specific intervals.

wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

[0024] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the present technology whose billing unit is simply based on relays. The revenue class in this invention is abstract, and can be a mixture of several different entity types. Besides, the present invention also adopts a new normalized input and output format for the division of revenue.

DESCRIPTION OF THE DRAWINGS

[0025]

Fig .1 is a flowchart illustrating different proprietors realizing division of revenue by the gateway office in accordance with a preferred embodiment of the invention;

Fig .2 is a map of the gateway office realizing division of revenue in accordance with a preferred embodiment of the invention;

Fig .3 is a flowchart illustrating the safety mechanisms of the central memory in accordance with a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0026] This invention will be further explained with reference to the drawings and an embodiment.

[0027] This invention provides a method and a apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office.

[0028] Here, the gateway office is an interface exchanging office carrying out transmission of telephone services among different proprietors. For instance, a user of the Shanghai Mobile makes a call to another fixed phone user of the Shanghai Telecom, which will reach the fixed phone user via a gateway office between the two companies. Since the Shanghai Telecom proprietor has supplied its resource, it will count this kind of resource at the gateway office, and then come to a settlement with the Shanghai Mobile for the revenue. Therefore, the main function of the gateway office is to separately count resources occupied and divide revenue among different proprietors. At the same time, it also provides other gateway services such as the call identification authority and black/white list. The Division of Revenue (DOR) is used to count communication resource among different proprietors.

[0029] As shown in Fig.1, the user 101 is a user of the proprietor A 102 and the user 105 is a user of the proprietor B 104. When a call from the calling user 101 to the called user 104 go in and out from the gateway office 103, the gateway office 103 will get a source from the proprietor A, such as Beijing, and get a destination from the proprietor B, such as Shanghai.

[0030] Fig.2 is a map of the gateway office implementing division of revenue in accordance with an embodiment of the invention, including a source and destination device 201, a billing center 208, which are existing technology, and a trigger device 202, a modulation device 203, an information generation device 204, a central memory 205, a display terminal 206 and a storage medium 207, which are added in this invention. As shown in Fig.2, the source and destination device 201 of the gateway office 103 gets a source parameter and a destination parameter respectively from the source and the destination, which is a numeric value (0-255). For example, if the source is Beijing, the value of the source parameter is "1", and if the destination is Shanghai, the value of the destination parameter is "2".

[0031] At this time the route is already elected to pass, namely when the called user starts ringing, the trigger device 202 of the gateway office 103 judges the value of source and destination parameters. If there is a parameter's value corresponding to the value for stopping the division of revenue function, for example, in this embodiment, if there is a parameter whose value is 0, the division of revenue function is stopped. Those users who do not need this function shield it to consume the least resources. Otherwise, the trigger device 202 obtains a revenue zone parameter according to the source parameter and the destination parameter, as show in table 1.

Destination / Source	Beijing	Shanghai	...	...
Beijing	X1 (north china revenue zone index(1))	X2 (north china-east china revenue zone index (2))	...	...
Shanghai	X3 (east china - north china revenue index (3))	X4 (east - china revenue zone index (4))	...	...
...	...	...	...	...
...	...	...	...	Xn

Table.1

[0032] x_1, x_2, x_3, x_4 ... x_n in the table 1 are revenue zone indices. In this embodiment, the source is Beijing (1) and the destination is Shanghai (2). The trigger device 202 judges the source parameter value and the destination parameter value, if neither of them is zero, the corresponding revenue zone index x_2 is obtained, namely North China - East China revenue zone index, whose revenue zone index value is "2". As shown in table 1, in this invention, the revenue zone indices with different values can simply correspond to the different revenue class indices, which means obtaining many different revenue class indices. In existing technology, if the source and the destination are respectively output relay group and input relay group, it realizes the relay jump table function, and the largest number of the relay group soft table is 10 or 14. In this invention, we can dynamically assign many revenue class indices to one input relay group + several destinations, or to one output relay group + several sources, which actually means a relay group can have the nearly infinite number of the soft tables. This already breaks through the number limitation of the relay group soft table,

which is 10 or 14 in the existing technology, therefore, this invention actually functions better than the current relay jump table technology.

[0033] The trigger device 202 judges the revenue zone index value, if the value is 0, the function of division of revenue is stopped. This is helpful to users' flexible choice, and save system resource to the greatest extent. Otherwise, the modulation device 203 will modulate the revenue zone index. For instance, in this embodiment, the value of the revenue zone index x_2 is "2", not "0", so x_2 is modulated. Refer to table 2 for detailed modulation process.

[0034] As shown in table 2, for instance, proprietors are interested in the voice service of this call, namely require to count and charge the voice service, then said revenue zone index is modulated with one of the modulation parameters and the corresponding revenue class index R_j, j=1, 2...n is obtained. In this embodiment, the revenue zone index x_2 is modulated with the type of call (voice) modulation parameter and the corresponding revenue class index R1 is obtained, which corresponds to the voice service of the DDD call, namely the DDD call list. Furthermore, if there are other calls corresponding to the ISDN call, the revenue zone index x_2 will be modulated with the type of call (voice) modulation parameter, and the corresponding revenue class index R2 will be obtained, which means R2 corresponds to the voice service of the ISDN, namely the ISDN call list.

Revenue zone index	Type of call	Revenue class index	Billing list
X2 (north china- east china revenue zone index(2))	Type of call (voice)	R1 (east china - north china revenue class index (1)) (DDD call)	DDD billing list
		R2 (east china - north china revenue class index (2)) (ISDN call)	ISDN billing list
		R3 (east china - north china revenue class index (3)) (IN call)	IN billing list
		...	...

		R4 (east china - north china revenue class index (n)) (other types of call)	Other types of billing lists

Table.2

[0035] This invention provides an extremely flexible modulation method, wherein said modulating characteristics in this invention means modulating said revenue zone index using one or several modulation parameters, and the different corresponding revenue class indices by different combinations of these modulation parameters are obtained. The purpose of the modulation is to further conclude and arrange all revenue by different modulation parameters, and make revenue sortable according to the proprietor's demand, namely to perform revenue class indexing. At the end, various billing data will be obtained through different revenue class indices. The modulation parameters can be type of call (voice), bear capacity, high level carrying(HLC), analog or ISDN user and so on.

[0036] Said modulation in this invention is carried out during the calling process. In the existing technology, the relationship between each revenue zone index and revenue class index is usually one-to-one correspondence, which could satisfy the demand of most users. In this case, the modulation step can be ignored.

[0037] After the called user 105 gives reply, and before the call is released, the information generation device 204 of the gateway office 103 generates contents related to said revenue class index, such as R1, which include static and dynamic information on the call. The static information contains the modulating characteristics as shown in table 2, the calling number, the called number, the route and so on, the dynamic information contains the call holding time, the answering time and so on. These static information and dynamic information related to the call will be sent to the central memory 205 of the gateway office 103 after the call is finished.

[0038] After the call is released, namely the call is finished, the central memory 205 of the gateway office 103 receives these contents related to said revenue class index R_j, and based on these contents, adds the increment values of every counter of the revenue class memory M_j (j=1, 2...n), which is related to said revenue class index R_j, to the corresponding counter. For example, in this call there are several counters in the revenue class memory M1 corresponding to the revenue class index R1 of the central memory 205, such as a total-number-of-calls counter□total-length-of-calls counter, etc, which respectively accumulate the total number of calls and the total length of calls, based on this call. This revenue class memory M_j (j=1, 2...n) is set according to users' needs during the gateway office initializing procedure.

[0039] Because of the importance of the resource, multiple safety mechanisms are performed in the present invention, which including: The central memory 205 introduces a windowing mechanism during the receiving procedure. The accumulation of each counter has a hot backup, as shown in Fig.3, the central memory 205 is comprised of primary central storage region 301, hot backup central storage region 302, primary hard disk 305 and standby hard disk 307, the primary central storage region 301 and the hot backup central storage region 302 stores at the same time, as arrow 303 shows, one-region working task can be performed under certain circumstances. However, synchronous working starts as soon as the two-region working task takes over.Each counter backups its information to a pair of hard disks with specific intervals, namely to the primary hard disk 305 and the standby hard disk 306, the backuping task is executed by the primary central storage region 301, as arrow 304 shows. Since these safety mechanisms are existing technology, just a simply introduction is provided.

[0040] The central memory 205 sends the information of said revenue class memory M_j to the storage medium 207, which stores the information with reference to a predefined formatted scheme and sends the information to the billing center 208 for revenue sorting the same way as other bill documents. The central memory 205 also can send the information of said revenue class memory M_j to the display terminal 206. For example, display contents of each counter of the revenue class memory M_j through display terminal 206, then the network resource occupation situation of each

proprietor can be observed directly and instantly, which realizes flexible online operation. The revenue sorting here means arranging the billing data (such as the detailed billing phone list, the double counting jump table file, all said revenue class indices) generated in the gateway office in a document, sending the entire document to the billing center 208, where the document will be operated according to the predefined procedure and reorganized into a list of each revenue class and the corresponding total number of calls, total length of calls.

[0041] The predefined format can be a general style, as shown in table 3, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc. The following is a revenue class index sequence, the last part is a file trailer, such as an end-of-file indicator; The format can also be a customized style according to the user's need, as shown in table 4, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc, the following is a each revenue class index arranged in an order of the relay group and the bear type, the last part is a file trailer, such as an end-of-file indicator.

Table.3

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in order</td><td>Revenue class index sequence number 1</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

Table.4

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in an order of the relay group and the bear type</td><td>Revenue class index sequence number (1, 2, 3)</td></tr>
<tr><td>Corresponding relay group name</td></tr>
<tr><td>Corresponding bear type</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td rowspan="2"></td><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

[0042] Therefore, the output format adopted in this invention greatly meets the users' demand, and makes it very convenient for the users to introduce this new function. Moreover, the output format can be customized to meet the needs of various high-end users. The output format provides more options, such as bureau name, file generation time, relay group name and other specific information, making it more supportive to on-line transmission.

[0043] More detailed steps corresponding to the embodiment of this invention are as follows:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue

area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2... n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

[0044] As to a medium-sized gateway office (10 hours when busy, 100CAPS bill list), the data volume ratio of detail billing in existing technology to the division of revenue in the present invention is over 100:1.

[0045] The present invention also greatly reduces the massive dump of the exchanger, the mass data processing of the sorting center and the mass data storage and transmission, saving various resources.

[0046] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide telecommunication revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the exiting technology whose billing unit is simply based on relays.

[0047] It should be understood that the said embodiment has been presented by way of example only, and not limitation. Thus, all modifications that fall within the scope of this invention are intended to be included therein.

Claims

1. A method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

   a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

   b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

   c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

   d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

   e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

   f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

2. The method according to claim 1, wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

3. The method according to claim 1, wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

   In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

   In said step f), the central memory sends the information in the revenue class memory M_j as said in step e)

to a display terminal.

4. The method according to claim 1, wherein in said step e) the multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

5. The method according to claim 1, wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

6. An apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device, a central memory and a storage medium which are all located in the gateway office, wherein:

When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;
The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue ,the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;
The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;
The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;
The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;
The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

7. The apparatus according to claim 6, wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

8. The apparatus according to claim 6, wherein:

Said contents related to the revenue class index R_j include static and dynamic information on the said call;
Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;
Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

9. The apparatus according to claim 6, wherein said multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

10. The apparatus according to claim 6, wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

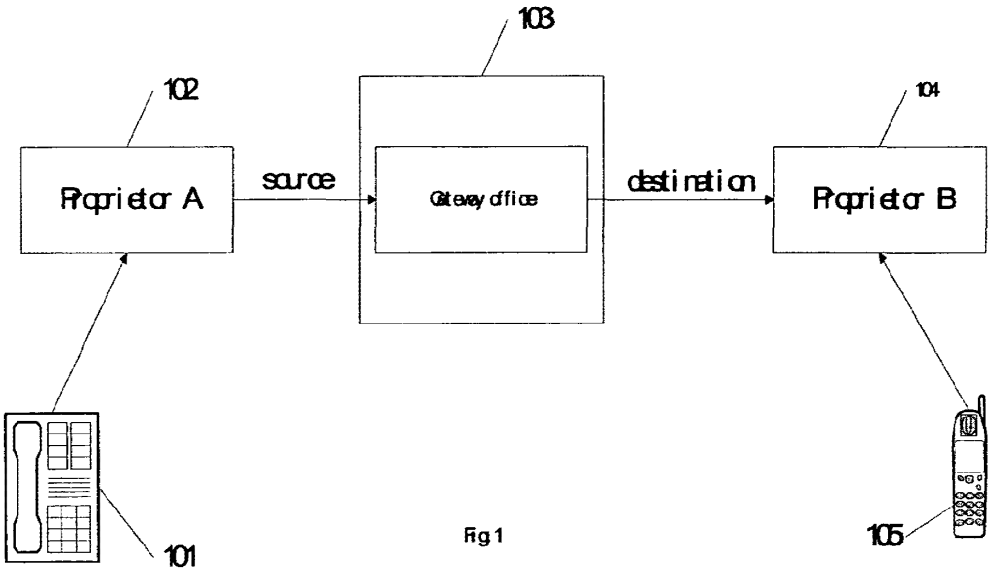

103
102
104
Proprietor A
source
Gateway office
destination
Proprietor B
101
105

Fig 1

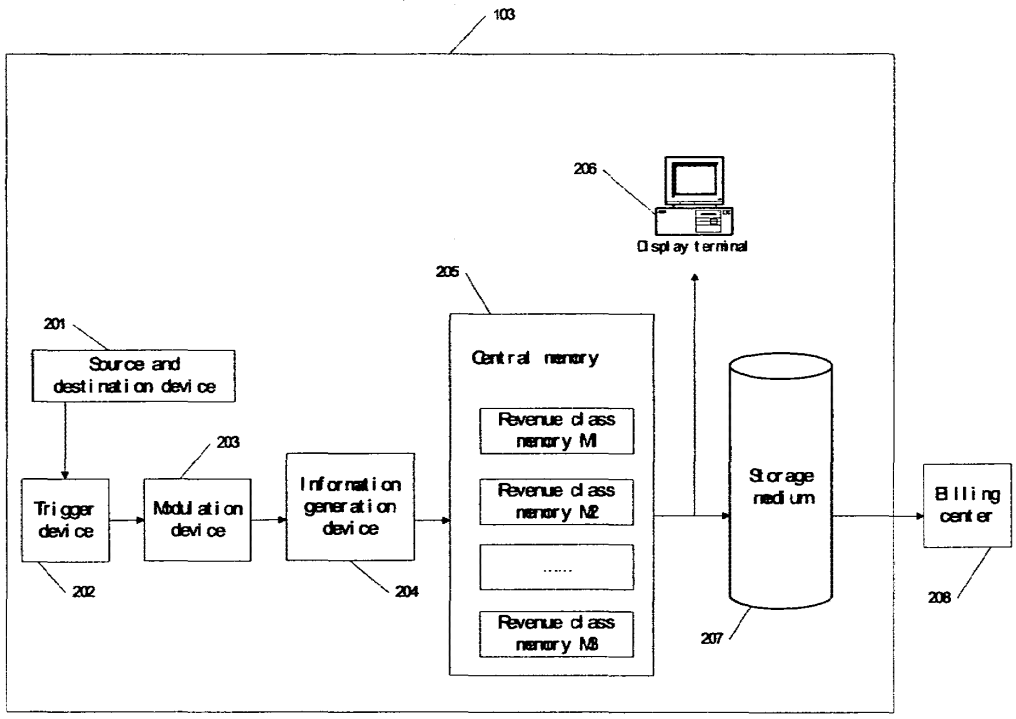

103
206
Display terminal
205
201
Source and destination device
Central memory
Revenue class memory M1
203
Trigger device
Modulation device
Information generation device
Revenue class memory M2
.....
Revenue class memory M8
Storage medium
Billing center
202
204
207
208

Fig. 2

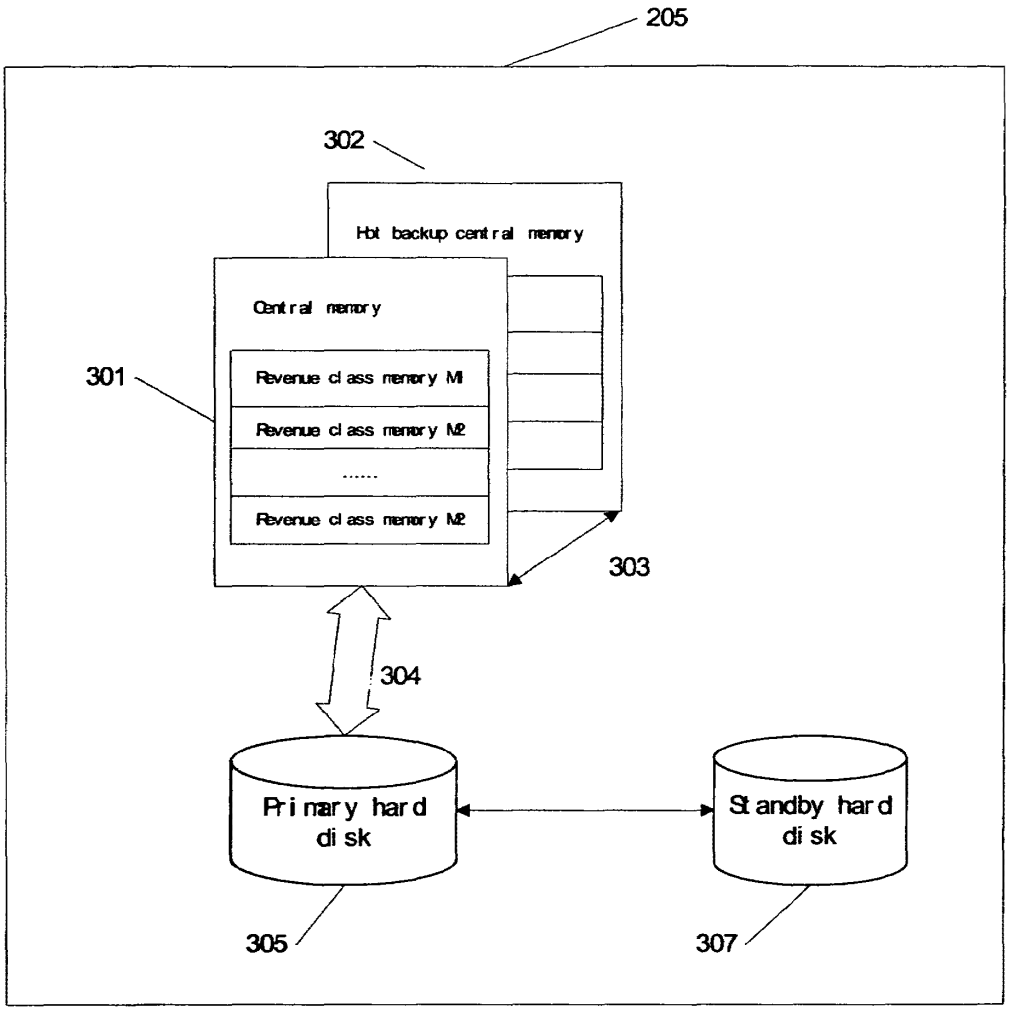

205
302
Hot backup central memory
Central memory
301
Revenue class memory M1
Revenue class memory M2
.....
Revenue class memory M2
303
304
Primary hard disk
Standby hard disk
305
307

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 02 7514

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 768 353 A (BROWNE ET AL) 16 June 1998 (1998-06-16) * column 1, line 33 - column 3, line 26 * * column 5, line 25 - column 7, line 39 * * column 10, line 22 - column 15, line 58 * * claims 1-17 *	1-10	H04M15/00 H04Q3/00
P,A	US 2004/033797 A1 (RAIVISTO TOMMI ET AL) 19 February 2004 (2004-02-19) * claims 1-20 * * figures 1,2 *	1-10	
A	EP 0 483 091 A (ERICSSON - GE MOBILE COMMUNICATIONS HOLDING INC; ERICSSON INC) 29 April 1992 (1992-04-29) * column 2, line 30 - line 47 * * claims 1-3 *	1-10	
A	WO 03/049351 A (CIBERNET, INC) 12 June 2003 (2003-06-12) * page 10, line 3 - page 11, line 29 * * page 12, line 21 - page 13, line 13 * * page 14, line 29 - page 16, line 28 * * page 18, line 1 - page 23, line 16 * * page 41, line 15 - page 44, line 7 * * figures 1-4,9 *	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04M H04Q
P,A	US 2004/210522 A1 (BISSANTZ ANNETTE S ET AL) 21 October 2004 (2004-10-21) * paragraph [0027] - paragraph [0029] *	1-10	
A	US 6 134 307 A (BROUCKMAN ET AL) 17 October 2000 (2000-10-17) * column 4, line 13 - column 5, line 17 *	1-10	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

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 04 02 7514

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 569 175 A (AMERICAN TELEPHONE AND TELEGRAPH COMPANY; AT&T CORP) 10 November 1993 (1993-11-10) * column 6, line 24 - column 7, line 19 * * figure 5 * * claims 1-3 *	1-10	
A	US 5 910 979 A (GOEL ET AL) 8 June 1999 (1999-06-08) * claims 1-3 *	1-10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

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 04 02 7514

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.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768353 A	16-06-1998	AU 697367 B2	01-10-1998
		AU 6383094 A	24-10-1994
		AU 697499 B2	08-10-1998
		AU 6383194 A	24-10-1994
		CA 2159000 A1	13-10-1994
		CA 2159002 A1	13-10-1994
		CN 1122639 A ,C	15-05-1996
		CN 1122640 A ,C	15-05-1996
		DE 69404452 D1	28-08-1997
		DE 69404452 T2	15-01-1998
		DE 69433814 D1	01-07-2004
		DK 692172 T3	02-03-1998
		EP 0692172 A1	17-01-1996
		EP 0692173 A1	17-01-1996
		ES 2107200 T3	16-11-1997
		FI 954627 A	09-11-1995
		FI 954628 A	10-11-1995
		WO 9423529 A1	13-10-1994
		WO 9423530 A1	13-10-1994
		HK 1001747 A1	03-07-1998
		HK 1014410 A1	11-03-2005
		JP 8508619 T	10-09-1996
		JP 8508620 T	10-09-1996
		JP 2002199130 A	12-07-2002
		NO 953898 A	29-11-1995
		NO 953899 A	29-11-1995
		NZ 263224 A	26-07-1996
		NZ 263225 A	26-01-1998
		SG 48839 A1	18-05-1998
		SG 50490 A1	20-07-1998
		US 5802142 A	01-09-1998
		US RE37856 E1	24-09-2002
		US RE37857 E1	24-09-2002
US 2004033797 A1	19-02-2004	AU 2003255864 A1	25-02-2004
		WO 2004015971 A1	19-02-2004
EP 0483091 A	29-04-1992	CA 2098191 A1	02-05-1993
		US 5063591 A	05-11-1991
		CN 1061692 A ,C	03-06-1992
		CN 1108851 A ,C	20-09-1995
		EP 0483091 A2	29-04-1992
		NZ 240072 A	25-02-1994
		WO 9309639 A1	13-05-1993
		DE 69127161 D1	11-09-1997
		DE 69127161 T2	18-12-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 02 7514

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.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0483091 A		ES 2107448 T3	01-12-1997
		HK 1001948 A1	17-07-1998
WO 03049351 A	12-06-2003	US 2003120594 A1	26-06-2003
		AU 2002365834 A1	17-06-2003
		WO 03049351 A2	12-06-2003
US 2004210522 A1	21-10-2004	NONE	
US 6134307 A	17-10-2000	NONE	
EP 0569175 A	10-11-1993	US 5333184 A	26-07-1994
		CA 2092590 A1	07-11-1993
		DE 69332461 D1	12-12-2002
		DE 69332461 T2	28-08-2003
		EP 0569175 A2	10-11-1993
		ES 2184736 T3	16-04-2003
		JP 2795596 B2	10-09-1998
		JP 6037936 A	10-02-1994
US 5910979 A	08-06-1999	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 887 732 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
13.02.2008 Bulletin 2008/07

(21) Application number: **06742044.8**

(22) Date of filing: **30.05.2006**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2006/001156

(87) International publication number:
WO 2006/128371 (07.12.2006 Gazette 2006/49)

(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

(30) Priority: **30.05.2005 CN 200510073415**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen
Guangdong 518129 (CN)

(72) Inventor: **ZHAO, Hang,**
Huawei Administration Building
Shenzhen Guangdong 518129 (CN)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Patent- und Rechtsanwälte
Theresienhöhe 13
80339 München (DE)

(54) **A METHOD AND SYSTEM FOR CONTENT CHARGING**

(57) A method for content charging includes: the portal server transmits the service activation request to the policy server based on the request for user using the service; the policy server determines the service policy corresponding to the service request after responding to the service activation request and distributes the service policy activation message to the content control gateway; the content control gateway performs the service policy and reports the user service usage message to the policy server; the policy server performs the charging according to the user service usage message. The solution provided by the present invention can realize the exact and low-cost charging for the content service and meet the requirement of QoS dynamic adjustment of the content service.

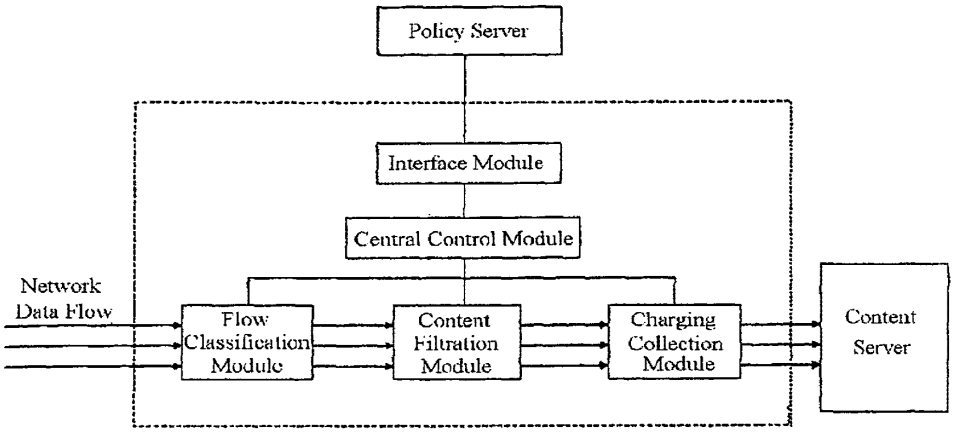


Fig.3

EP 1 887 732 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to the technical field of network communications, in particular, to a method and a system for content charging.

Background of the Invention

[0002] With the rapid development of the Internet, content services become more and more abundant. Correspondingly, Internet Content Providers (ICPs) for getting profit by providing contents come on the scene. By cooperating with the ICP, service providers may increase the income of the access service by expanding the scale of network userson one hand, and earn the profit sharing of content income of the ICP on the other hand. At the same time, the ICP may obtain a low-cost channel for selling its content service rapidly.

[0003] The content platform of the service provider is developed on such background. The general mode of the content platform is as follows: The service provider provides a technical platform, and the ICP issues its content service via this platform. The service provider performs advertising, authentication, charging for the use of the content service via the platform. The user uses the content service provided by each ICP via the platform. The content platform records various fees caused by the user, and all of the fees will be recorded on a content account provided to the user by the service provider. With this content platform, the user does not need to settle accounts with each ICP; instead, the user only needs to settle accounts with the service provider.

[0004] The existing content charging solution for this content platform is usually implemented as follows:

[0005] A user connects to the network, logs in a portal website Portal Server, and connects to a Content Server of an ICP via a content channel. If the user is interested in a content provided by the ICP, then he/she clicks the button "OK", and the ICP Content Server will send an authentication request to the content platform of the service provider. If the authentication is passed, the right to use the content is assigned to the user and a charging start message is sent to the content platform.

[0006] To ensure the accuracy of the charging, the Content Server of the ICP sends an intermediate charging message to the content platform at a certain time interval during the usage of the content. When the user logs out the Content Server, the Content Server of the ICP sends a charging completion message to the content platform.

[0007] The content platform processes the charging message in real time, and performs rating and accounting on the content consumption of the user according to the information in the charging message such as service number, time length traffic flow, etc., together with the charging policy of the service.

[0008] In the prior art, strict requirements are laid on the interconnection technology between the content platform and the ICP. The ICP has to carry out customized development according to the content platform authentication and charging interface provided by the service provider, and joint debugging and testing should be performed after the development. Services may only be formally issued after the testing is passed. Thus, the cost is very high.

[0009] Some small-scale ICPs are weak in technical strength and they are not able to carry out customized development according to the charging interface. Some other ICPs purchase their service contents, such as multiplayer-fighting games, from other software company, so they have no source code for interface development, and are not able to implement content charging for such services.

[0010] Quality of Service (QoS) is required for some content services. For example, Video On Demand (VOD) service requires a broad bandwidth. However, in the mode aforementioned, the bandwidth may not be dynamically adjusted according to the service, and it is disadvantageous for operation and management.

[0011] In the actual operation of the ICP, it is difficult for the service provider to control the correctness of the service number, traffic flow and time length in the charging message, thus accurate charging may not be performed.

Summary of the Invention

[0012] The present invention provides a method and a system for implementing content charging at low cost, so that the service charging may be more accurate and reasonable, and the bandwidth may be adjusted dynamically according to the service.

[0013] The present invention provides a method for content charging, including:

[0014] sending, by a Portal Server, a service activation request to a Policy Server, based on a service request from a user;

[0015] responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;

[0016] executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

[0017] The method further includes:

[0018] sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and

[0019] responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consump-

tion information, by the Policy Server.

[0020] The content control gateway reports the user service consumption information to the Policy Server periodically during the service;

[0021] The Policy Server performs rating according to the user service consumption information, and settles accounts on the service consumption of the user according to each rating information after the user stops using the service.

[0022] After responding to the service activation request, the Policy Server queries a preset correlation table between the service and the service policy according to the service activation request, determines the service policy corresponding to the service, and extracts the parameters needed for executing the service policy, then fills the parameters in the service policy activation message and delivers the service policy activation message to the content control gateway.

[0023] Wherein, the service policy message includes the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

[0024] The content control gateway grants the right to the source IP address of the user network packet to access the destination IP address, destination port and destination service resource, and controls the network flow according to the traffic flow information in the policy message.

[0025] The content control gateway distinguishes between the content data flows according to the Content Server or the service port of the content, controls the content data flow and collects the consumption information.

[0026] In another aspect of the invention, there is provided a system for content charging, which includes a Portal Server and a Content Server, wherein

[0027] the system further includes a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;

[0028] the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

[0029] The Policy Server includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0030] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0031] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0032] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0033] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0034] The content control gateway includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0035] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0036] The flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass.

[0037] The content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass.

[0038] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0039] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0040] In still another aspect of the invention, there is provided a Policy Server for implementing content charging, which includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0041] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0042] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0043] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0044] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0045] The server further includes a database interface and a memory database, Through the database interface, an external database and the memory database may be accessed. The memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

[0046] The invention further provides a content control gateway for implementing the charging method according to claim 1, which includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0047] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0048] The flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass.

[0049] The content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass.

[0050] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0051] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0052] In summary, in the method and system for content charging according to the embodiments of the invention, by determining the service policy corresponding to the service information and executing the service policy, the user is controlled to use the service, the content data flows are distinguished according to the Content Server or the service port of the content, and the content data flow is controlled and the consumption information is collected. So that charging may be performed according to the user service consumption information reported. As a result, the interconnection difficulty and interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and a non-coding interconnection operation solution may be provided. Thus, the service provider may rapidly dispose a content service, the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. At the same time, the corresponding network QoS may be ensured according to the requirements of a certain content service, thus an overall QoS may be provided, and the market competitive power may be improved.

Brief Description of the Drawings

[0053] Figure 1 is a schematic diagram showing an exemplary system structure according to an embodiment of the invention;

[0054] Figure 2 is a schematic diagram showing the structure of the Policy Server according to an embodiment of the invention;

[0055] Figure 3 is a schematic diagram showing the structure of the content control gateway according to an embodiment of the invention; and

[0056] Figure 4 is a flow chart of the method according to an embodiment of the invention.

Detailed Description of the Embodiments

[0057] To make the principle, characteristics and advantages of the invention clearer, the invention will now be described in detail hereinafter in conjunction with the embodiments and the drawings of the invention.

[0058] As shown in Figure 1, the system for content charging according to an embodiment of the invention includes a Portal Server, a Policy Server, a Content Control Gateway (CCG) and a Content Server. Wherein, the Policy Server is connected with the Portal Server and the content control gateway, for delivering or canceling a service policy message, and performing rating and charging according to the service usage information reported by the CCG, such as traffic flow and time length. The CCG is connected with the Content Server, for controlling the access to the Content Server of the user, counting the service consumption information, and periodically reporting the related data to the Policy Server for charging. The Portal Server provides a portal for user access, and provides the user with functions such as login, service channel, service selection, self-help service. The Content Server is a server through which the ICP provides contents. There may be a plurality of Content Servers connected with a CCG, and various contents may also be issued on a Content Server. The servers on which the contents exist may be different, and the service ports of the contents, i.e. Transmission Control Protocol/User Data Protocol (TCP/UDP) ports may be different. The CCG distinguishes between the content data flows according to the server on which the contents exist or the service port of the content, and controls the content

data flows and collects data respectively for executing the policy.

[0059] The service policy message may be regarded as an indication message for the service data flow rules, which comprises parameters such as the source IP address, destination IP address, destination port, service resource information and traffic flow information of a network packet. For example, when a Content Server provides a game service, if a user wants to access the game server, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth, the Universal Resource Locator (URL), etc. Thus, if the Policy Server delivers the policy and notifies the CCG, the CCG grants the user the right to access the game server after applying the policy. If the Policy Server instructs the CCG to remove the policy, the current user will lose the right to access the game server.

[0060] If the user wants to access a streaming server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the streaming server, the port of the streaming server, the upstream bandwidth, the downstream bandwidth and the URL. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the streaming server after applying the policy and reserves a designated bandwidth for the video/audio stream. If the Policy Server instructs the CCG to remove the policy, then the current user will lose the right to access the streaming server.

[0061] Similarly, if the user wants to access a download server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the download server, the port of the download server, the upstream bandwidth, the downstream bandwidth, and the path of the download file. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the download server after applying the policy and reserves a designated download bandwidth. If the Policy Server instructs the CCG to delete the policy, then the current user will lose the right to access the download server.

[0062] Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy.

[0063] The internal structure of the Policy Server is as shown in Figure 2, which may include a central control module, a charging engine, a portal interface module, a device interface module, a database interface module and a local memory database (Built-in-Memory).

[0064] The central control module is the core module of the Policy Server, and is mainly responsible for scheduling and controlling other modules in the system. The central control module receives a service activation request sent from the portal interface module, converts it into a service policy message corresponding to the service, and sends the service policy message to the CCG via the device interface. If the policy is executed successfully, the CCG will periodically report the user service consumption information (mainly including time length and traffic flow information), and the central control module invokes the charging engine module for performing rating after receiving the original charging information from the device interface module.

[0065] The portal interface is responsible for interconnecting with the Portal Server, sending the service activation request or the service deactivation request to the central control module, and returning the service request execution result to the Portal Server.

[0066] The device interface module is responsible for interconnecting with the CCG, forwarding the policy information delivered by the central control module to the CCG, and reporting the policy execution information and service usage information to the central control module.

[0067] The charging engine is the charging component of the Policy Server. The central control module invokes the charging engine for performing rating and accounting according to the user service consumption record.

[0068] The database interface enables other subsystems to access the database and the memory database.

[0069] The memory database is an optional component, which may be regarded as a buffer for the external database. The memory database is mainly adapted to store policy data, charging data, configuration data and user session data. By using the memory database, the performance of the system may be improved greatly. The central control module periodically sends an instruction to the memory database for reading the policy data, charging data, configuration data from the external database and refreshing the local memory data.

[0070] The CCG is adapted to control the access to the Content Server of the user, count the service consumption information, and periodically report related data to the Policy Server for performing charging. As shown in Figure 3, the internal structure of the CCG includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0071] The central control module is responsible for receiving the policy sent from the Policy Server and interpreting and executing the policy. During the execution of the policy, the central control module needs to interact with and control the flow classification module, the content filtration module and the charging collection module.

[0072] The flow classification module checks, classifies and controls the information such as the source IP, the destination IP, the destination port of the network packet, on the IP layer. The network flow that conforms to the policy may pass.

[0073] The content filtration module checks, classifies and controls the resources to be accessed by the network packet, such as the URL address applied by the HTTP,

the file path applied by the FTP (File Transfer Protocol) and the RTICP (Real-Time Streaming Protocol) path applied by the stream media, on the application layer. The network flow that conforms to the policy may pass.

[0074] The charging collection module collects the time length and the traffic flow information of the network flow, and reports the original charging data to the central control module. The central control module reports the original charging data to the Policy Server.

[0075] In the method according to an embodiment of the invention, Portal Server receives a service request from a user, and sends a service activation request to Policy Server. The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to CCG. The CCG executes the policy message, permits the user to use the service, and periodically reports the user service consumption information to the Policy Server. The Policy Server performs rating and charging according to the consumption information.

[0076] Specifically, as shown in Figure 4, the method includes following steps.

[0077] (1) A user sends a login request to the Portal Server, and the Portal Server authenticates the identity of the user.

[0078] (2) If the authentication is passed, the Portal Server receives the service selection data input by the user.

[0079] (3) The Portal Server sends a service activation request, which carries information such as the user IP, destination IP, service resources, to the Policy Server.

[0080] (4) The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to the CCG. Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy. This table may be stored on the Policy Server or on a third party device. The Policy Server determines the policy corresponding to the service by querying the correlation table according to the activation request, extracts the parameters needed by the policy according to the activation request and the service policy, fills the parameters in the policy message and delivers the policy message. For example, for a game service, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth and the URL.

[0081] (5) The CCG receives the service policy message, executes the service policy according to the instruction of the message, releases the access right from the user IP (which may be a source IP) to the destination IP, destination port or destination URL, and controls the network flow according to the bandwidth parameters in the policy. The CCG sends the policy execution result to the Policy Server after executing the policy.

[0082] (6) The Policy server informs the Portal Server of the service activation result.

[0083] (7) The Portal Server displays the service activation result to the user.

[0084] (8) If the service is activated, the user starts an application client end and performs content consumption, after knowing from the Portal Server that the service is available.

[0085] (9) The CCG periodically reports the service consumption information to the Policy Server during the content service used by the user.

[0086] (10) The Policy Server processes the service consumption information reported by the CCG in real time, and performs rating for the user content consumption.

[0087] (11) The Portal Server receives a request for stopping the service from the user when the user wants to logout the Content Server.

[0088] (12) The Portal Server sends a service deactivation request to the Policy Server.

[0089] (13) The Policy Server delivers a policy cancellation request to the CCG.

[0090] (14) The CCG cancels the policy and returns the policy cancellation result to the Policy server.

[0091] (15) The Policy server informs the Portal Server of the service cancellation result.

[0092] (16) The Portal Server displays the service cancellation result to the user.

[0093] (17) The CCG reports the last service consumption information of the user to the Policy Server.

[0094] (18) The Policy Server processes the service consumption information, performs rating, and settles accounts on the current content consumption according to each rating information.

[0095] In another embodiment of the invention, the content control gateway does not need to periodically report the user service consumption information to the Policy Server. Instead, the content control gateway reports the total service consumption information of the user to the Policy Server at a time after receiving the policy cancellation request delivered by the Policy Server. The Policy Server performs rating and accounting according to the consumption information.

[0096] The invention provides a novel content charging solution, by means of which the interconnection difficulty and the interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. In the meanwhile, the corresponding network QoS may be ensured according to the requirements of a certain content service.

Claims

1. A method for content charging, comprising:

   sending, by a Portal Server, a service activation request to a Policy Server based on a service request from a user;
   responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;
   executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and
   permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

2. The method according to claim 1, wherein the method further comprises:

   sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and
   responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consumption information, by the Policy Server.

3. The method according to claim 1 or 2, wherein the method further comprises:

   reporting, by the content control gateway, the user service consumption information to the Policy Server periodically during the use of the service;
   rating according to the user service consumption information, and accounting on the service consumption of the user according to each rating information after the user stops using the service, by the Policy Server.

4. The method according to claim 1, wherein the method further comprises:

   after responding to the service activation request, querying a preset correlation table between the service and the service policy according to the service activation request, determining the service policy corresponding to the service, extracting the parameters needed for executing the service policy, filling the parameters in the service policy activation message and delivering the service policy activation message to the content control gateway by the Policy Server.

5. The method according to claim 1, 2 or 4, wherein: the service policy activation message comprises the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

6. The method according to claim 5, wherein the method further comprises:

   granting the source IP address of the user network packet a right to access the destination IP address, destination port and destination service resource, and controlling the network flow according to the traffic flow information in the service policy message, by the content control gateway.

7. The method according to claim 1, wherein the method further comprises:

   obtaining the content data flows according to the Content Server or the service port of the content, controlling the content data flow and collecting the consumption information, by the content control gateway.

8. A system for content charging, comprising a Portal Server and a Content Server, wherein the system further comprises a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;
   the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

9. The system according to claim 8, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

   the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a

service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

10. The system according to claim 8, wherein the content control gateway comprises a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass;
the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

11. A Policy Server, for realizing the charging method according to claim 1, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

12. The server according to claim 11, wherein the server further comprises a database interface and a memory database, through the database interface, an external database and the memory database is accessed; the memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

13. A content control gateway, for implementing the charging method according to claim 1, comprising a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass;

the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

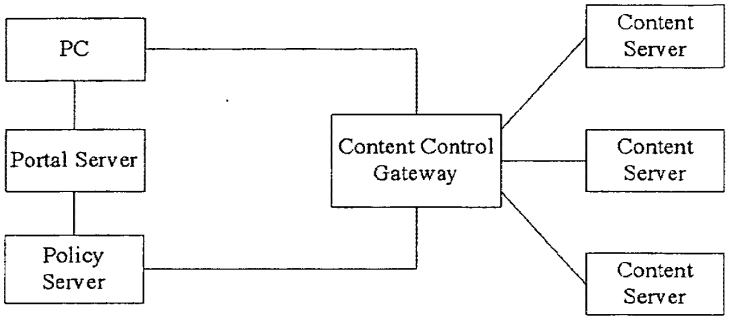

PC
Portal Server
Policy Server
Content Control Gateway
Content Server
Content Server
Content Server

Fig.1

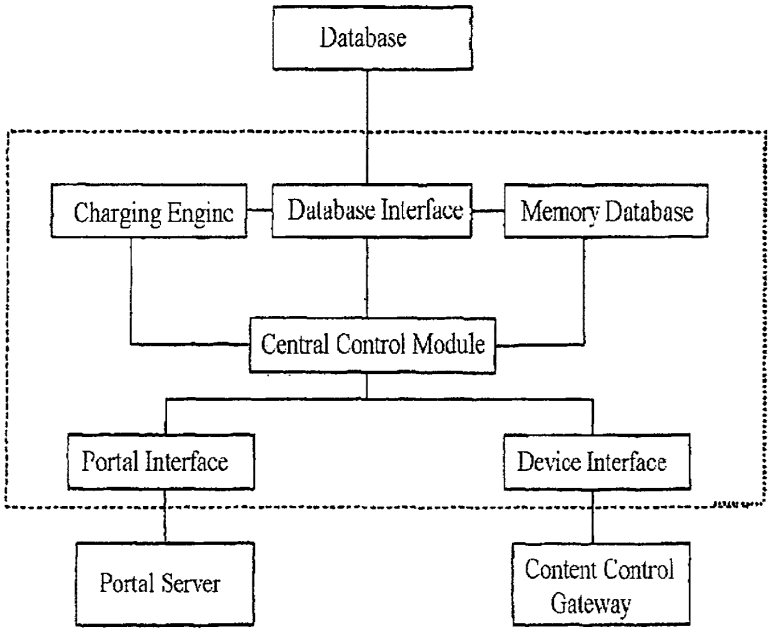

Database
Charging Engine
Database Interface
Memory Database
Central Control Module
Portal Interface
Device Interface
Portal Server
Content Control Gateway

Fig.2

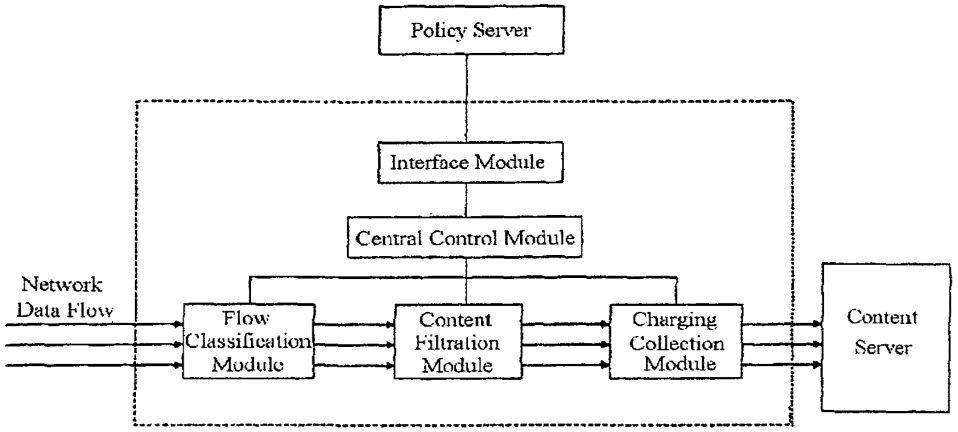

Policy Server
Interface Module
Central Control Module
Network Data Flow
Flow Classification Module
Content Filtration Module
Charging Collection Module
Content Server

Fig.3

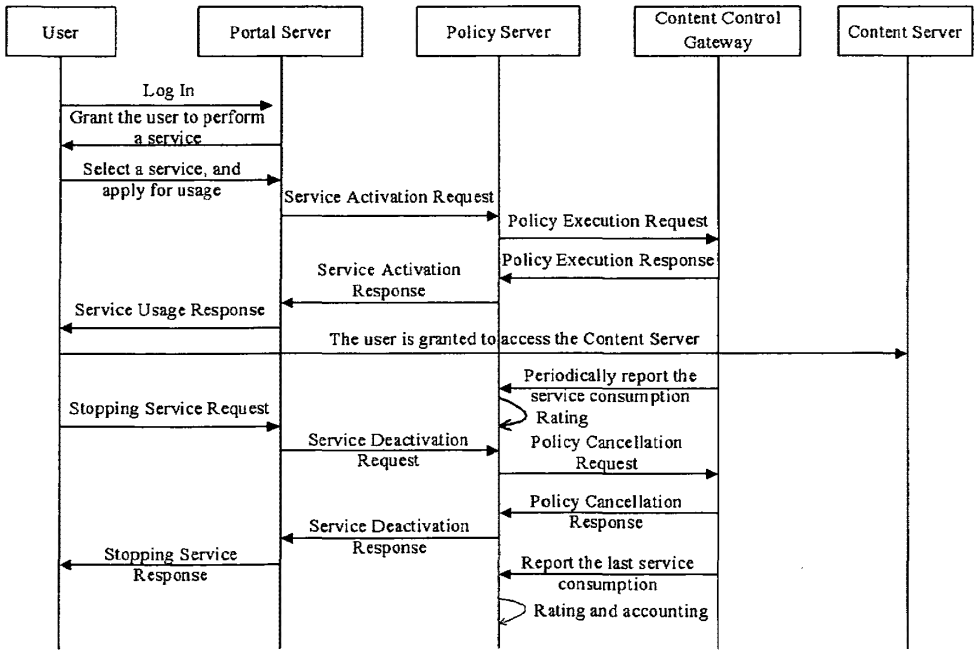

User
Portal Server
Policy Server
Content Control Gateway
Content Server
Log In
Grant the user to perform a service
Select a service, and apply for usage
Service Activation Request
Policy Execution Request
Policy Execution Response
Service Activation Response
Service Usage Response
The user is granted to access the Content Server
Periodically report the service consumption
Rating
Stopping Service Request
Service Deactivation Request
Policy Cancellation Request
Policy Cancellation Response
Service Deactivation Response
Stopping Service Response
Report the last service consumption
Rating and accounting

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/001156

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L (2006.01), G07F (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, PAJ: bill+, charg+, account, content, policy, strategy, request, gateway, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, A1, 0159990 (FUTURE TECH INC) 16.AUG. 2001 (16.08.2001), the whole document.	1-13
A	EP, A1, 1400934 (OPENWAVE SYSTEMS INC) 24.MAR. 2004 (24.03.2004), the whole document.	1-13
A	CN, A, 1556634 (ZHONGXING COMMUNICATION CO LTD SHENZHEN) 22.DEC. 2004 (22.12.2004), the whole document.	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29. AUG. 2006 (29. 08. 2006)	21 · SEP 2006 (21 · 09 · 2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WANG,Hongli Telephone No. (86-10) 62084525

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/001156

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO0159990A1	16.08.2001	JP2003523031T	29.07.2003
		KR2000024368 A	06.05.2000
		AU200136124 A	20.08.2001
		KR331219 B	06.04.2002
		US2003023550 A1	30.01.2003
		CN1397125 A	12.02.2003
EP1400934A1	24.03.2004	NONE	
CN1556634A	22.12.2004	NONE	

Form PCT/ISA /210 (patent family annex) (April 2005)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 007 065 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
24.12.2008 Bulletin 2008/52

(21) Application number: **07720622.5**

(22) Date of filing: **30.03.2007**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2007/001048

(87) International publication number:
WO 2007/112685 (11.10.2007 Gazette 2007/41)

(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 MT NL PL PT RO SE SI SK TR

(30) Priority: **31.03.2006 CN 200610067080**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District, Shenzhen
Guangdong 518129 (CN)

(72) Inventors:
- **WU, Yajuan**
  Shenzhen Guangdong 518129 (CN)
- **LUO, Long**
  Shenzhen Guangdong 518129 (CN)

(74) Representative: **Haley, Stephen**
Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) CHARGING ASSOCIATING METHOD, SYSTEM, CHARGING CENTER, AND DEVICE FOR APPLICATION SERVICE

(57) A method for charging correlation for an application or service is provided. The method may include: receiving a service identifier assigned for an application or service; and correlating Charging Data Records CDRs generated for the application or service based on the service identifier. A system for charging correlation, a billing center and an apparatus for charging correlation are also provided. These method and apparatus may provide a simple charging correlation process for an application or service.

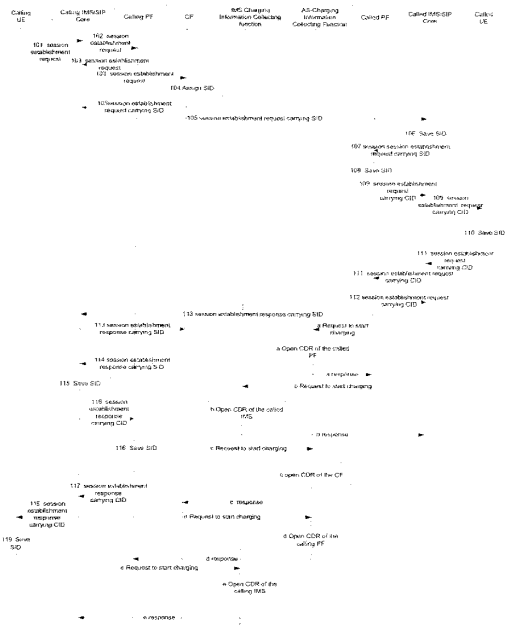


Fig. 1

EP 2 007 065 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to applications and services, and particularly, to a method and system for charging correlation of applications and services, a billing center and an apparatus for generating charging data record.

Background of the Invention

[0002] At present, communication systems have provided applications and services for individual user and/or group users, and communication media employed in these applications and services may include text, audio, video, and varieties combinations of multimedia. A general application or service is mainly oriented to individuals, and there usually is only one or two User Equipments (UEs) communicating with an Application Server or with each other. However, in an application or service in which group users take part, users of one or more groups usually communicate with other users at the same time. In other words, this kind of communication is not a two-party communication including one calling user and one called user, but a communication including a plurality of calling users and a plurality of called users. Such an application or service in which group users take part is also called a multi-party service.

[0003] In a session-based service, a Charging Identifier (CID) is allocated each time when an Application Server (AS) establishes a session with a UE, and all CIDs allocated are saved in the AS and a service bearer network. A billing center retrieves Charging Data Records (CDRs) corresponding to the CIDs from the service bearer network and the AS via a charging function collecting entity, and combines CDRs that correspond to the same CID in order to perform a charging. For applications and services employing an IP Multi-media Subsystem (IMS) as a service bearer network, the CIDs allocated are also called IMS Charging Identifiers (ICIDs). However, the applicant finds out that the CID-based charging method described above has some disadvantages in practical applications and services.

[0004] For example, in a service communication, when a UE establishes a session with an AS for a first time, the UE is given a CID. For some reasons, the UE may exit the service communication temporarily before the service communication is end. Later, the UE re-enters the service communication. In such a case the UE is given a new CID for a session established after re-entering the service communication. From a perspective of a user using the UE, the two sessions, established for the first entering and established for the re-entering, respectively, are two related sessions, and need to be combined for a charging. However, from a perspective of the billing center, the two sessions correspond to different CIDs, thus the two sessions are considered as unrelated sessions. If the two sessions need to be correlated, the billing center needs to analyze CDRs of the two sessions and perform complicated calculation based on user information recorded in the CDRs, yet it is still difficult to guarantee an accurate correlation of the two sessions. Such problem becomes more apparent in multi-party services.

[0005] In a multi-party service, UEs used by users of various parties of this service access a center control server via respective access servers. The center control server provides centralized session handling, which includes session signaling controls, media transmission authorization to communication parties, media data duplication and distribution, etc. One multi-party service has one center control server and at least one access server. The center control server performs controlling function (CF) and the access server performs participating function (PF). Logically, a CF corresponds to a multi-party service. In a multi-party service, the CF establishes one session for each UE, and the sessions of each UE correspond to a PF. Therefore, the center control server is looked as a CF while the access server is looked as at least one PF corresponding to at least one UE connected to the access server.

[0006] Therefore, multi-party services have a common feature that, a multi-party service has at least one session and each session corresponds to a UE of one user and corresponds to its CID. Due to such feature of multi-party services, the billing center needs to correlate a great number of CIDs when performing charging, which leads to poor charging accuracy and difficult implementation. Moreover, for a multi-party service, there is also a need to charge a user by correlating a plurality of sessions of the user in one multi-party service. However, according to the charging technique in the prior art, the billing center needs to generate CDRs based on ICIDs first and make further calculations based on group information in the CDRs, which is still complicated and tends to be inaccurate.

[0007] As discussed above, CID-based charging method in the prior art cannot correlate different sessions of a user in one service communication, but only can correlate actions of the user in one session. Such charging method may easily result in a repeated charging for one action and may omit an action which needs to be charged, thereby threatening security and reliability of charging operations and reducing user satisfaction.

[0008] Furthermore, as new demands emerge, it is becoming more and more difficult to use a single AS to handle a plurality of applications or services. In order to provide more flexible and richer services, operators or service providers are developing multi-services which includes a plurality of sub-services. For a perspective of a multi-service, the above application or service provided by the AS can be called single-service. In a multi-service, each sub-service has a sub-service server e.g. an AS, and an entire multi-service also has a service control function adapted to perform a centralized control of all the sub-service servers. For example, the service control

function controls initiation procedures of the respective sub-services and controls assignment of session identifiers of the respective sub-services, etc. A current typical multi-service has a structure that one of the sub-services is considered as the primary service, and all other sub-services of the multi-service are considered as supplementary services. The sub-service server serves the primary service can be called a primary service server and the sub-service servers serve the supplementary services can be called supplementary service servers. The implementation of the supplementary services depends on the implementation of the primary service in certain degree and provides supplementary functions for the implementation of the primary service. For example, a Presence Server may be configured in a PoC service network and be used to display group status to users during a PoC service session. For another example, a Location Service Server (LCS Server) may also be used in a PoC service network to provide location information of participating users.

[0009] As the development of multi-services, operators or service providers may develop correlating charging policies for multi-services. However, as discussed above, the conventional charging method is based on CIDs corresponding to separate sessions. Therefore the billing center needs to correlate CDRs of a plurality of services in a multi-service charging to perform a charging. Because a CID corresponds to only one session of a sub-service of a user, the billing center needs to analyze each CDR and performs comprehensive calculation by using complicated processes, thereby resulting in low charging accuracy and low feasibility.

[0010] Therefore, the conventional CID-based charging method is only applicable to correlate a plurality of actions of a user in one session, but is not applicable to correlate a plurality of sessions of a user in a single-service and says nothing of correlating a plurality of sessions of a user in a plurality of sub-services of a multi-service.

Summary of the Invention

[0011] Embodiments of a method and a system for charging correlation, a billing center and an apparatus for generating charging data record for implementing a charging correlation for an application or service are provided, which enables a charging correlation process to be easily performed and to greatly improve charging accuracy.

[0012] A method for charging correlation for an application or service may include:

assigning a service identifier by a service control function to an application or service;
sending the service identifier to a charging system; and
correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

[0013] A system for charging correlation for an application or service may include:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate Data Records CDRs generated for the application or service based on the service identifier.

[0014] A billing center may include:

a first module, adapted to receive a service identifier assigned to an application or service and CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

[0015] An apparatus for generating charging data record may include:

a first module, adapted to receive a service identifier assigned to an application or service; and
a second module, adapted to generate Charging Data Records CDRs carrying the service identifier from the first module for the application or service.

[0016] The method for charging correlation, the system for charging correlation, the billing center and the apparatus for generating charging data record for implementing a charging correlation for an application or service provided in accordance with embodiments of the present invention are able to correlate a plurality of CDRs generated during an application or service, thereby implementing a correlated charging of a plurality of users participating in the application or service in a simple way. A plurality of CDRs generated for one user in the application or service may be correlated and the user can be accurately charged. Furthermore, correlated charging for multi-services can also be implemented. The technical solution provided in embodiments of the present invention is easy to be implemented and does not need to make many modifications to the existing networks, and therefore is highly feasible.

Brief description of the drawings

[0017]

Figure 1 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 2 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 3 is a flowchart of a charging correlation process in a session modification in accordance with an embodiment of the present invention.
Figure 4 is a flowchart of a charging correlation proc-

ess when a new user is added in accordance with an embodiment of the present invention.

Figure 5 is a flowchart of a charging correlation process of an on-demand session in accordance with an embodiment of the present invention.

Figure 6 is a flowchart of a charging correlation process of a pre-established session in accordance with an embodiment of the present invention.

Figure 7 is a flowchart of a charging correlation process when a user who established an on-demand session re-enters the session in accordance with an embodiment of the present invention.

Figure 8 is a flowchart of a charging correlation process when a user who established a pre-established session re-enters the session in accordance with an embodiment of the present invention.

Figure 9 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 10 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention.

Detailed Description of the Embodiments

[0018] This invention will hereinafter be described in detail with reference to accompanying drawings and embodiments.

[0019] A charging method for an application or service according to an embodiment of the present invention may include: assigning a service identifier to an application or service session, sending the service identifier to a charging system, and correlating, by the charging system, the CDRs generated in this service based on the service identifier. The charging method is described in detail in the following embodiments.

[0020] The charging system may include a charging information collecting function used to receive CDRs from ASs and bearer control layer entities, a charging gateway, and a billing center used to correlate the CDRs and perform other operations for charging. The charging information collecting function functions as an interface of the charging system, receives CDRs from network nodes e.g., ASs or bearer control layer entities connected to the charging information collecting function, and sends the CDRs to the billing center via the charging gateway. ASs and the bearer control layer entities have respective charging information collecting functions. A charging information collecting function corresponding to ASs is usually called an AS-charging information collecting function and a charging information collecting function corresponding to bearer control layer entities is usually called a bearer control layer-charging information collecting function. For bearer control layer in an IMS network, the bearer control layer-charging information collecting function is also called an IMS charging information collecting function. Embodiments of the present invention mainly concerns about transmission of service identifiers among ASs, bearer control layer entities and charging information collecting functions, therefore the figures and illustrations of the embodiments of the present invention omit the processes that the charging information collecting functions send CDRs and service identifiers to the billing center. In the figures and illustrations of the embodiments of the present invention, the AS-charging information collecting function entities and IMS charging information collecting function entities are referred to as AS-charging information collecting functions and IMS charging information collecting functions.

[0021] A first charging correlation scheme given in an embodiment of the present invention implements charging with a plurality of CDRs generated for one user in a single-service. In this embodiment, a service control function, e.g. an AS of a single-service session, assigns a uniform service identifier for the single-service, generates CDRs of participating users and sends the service identifier and the CDRs to a charging system. The charging system correlates the CDRs of a user in this single-service session.

[0022] In practical applications, a user may establish one or a plurality of sessions in one service and a CDR corresponds to one session of the user. Different ways may be adapted to correlate CDRs based on the service identifier. The CDRs to be correlated may be CDRs corresponding to a plurality of sessions established for one user in one service, or may be CDRs corresponding to a plurality of sessions established for a part of users or all users in one service. The specific way of correlating CDRs is chosen in accordance with an applied correlation policy and will not be described further herein.

[0023] The AS sends the service identifier and the CDRs to a charging information collecting function of a charging system. The charging information collecting function sends the CDRs collected and the service identifier to a billing center which performs charging correlation operations. When this charging correlation scheme is applied to application service layer, the charging information collecting function includes an AS-charging information collecting function corresponding to the service control function entity. The charging correlation scheme may also be applied to bearer control layer, and in such a case the charging information collecting function includes a bearer control layer-charging information collecting function corresponding to a bearer control layer entity that the service control function entity corresponds to, wherein the bearer control layer entity that the service control function corresponds to is used to bear the service control function. At this time, the bearer control layer entity corresponding to the service control function records the service identifier and generates CDRs for the current application or service, and sends the service identifier and the CDRs to the bearer control layer-charging infor-

mation collecting function of the bearer control layer entity. The AS-charging information collecting function and the bearer control layer-charging information collecting function respectively send the CDRs and service identifiers to the billing center. The billing center correlates the CDRs received from the AS-charging information collecting function and correlates the CDRs received from the bearer control layer-charging information collecting function, respectively. Or the billing center may correlates the CDRs received from the AS-charging information collecting function with the CDRs received from the bearer control layer-charging information collecting function. This charging correlation scheme in an embodiment of the present invention may be applied to both the application service layer and the bearer control layer in the embodiments shown in Figures 1 to 8. When the charging correlation scheme is applied only to the application service layer, the charging correlation process involves UE, AS, AS-charging information collecting function and billing center, without involving the bearer control layer entity and the bearer control layer-charging information collecting function. The charging correlation process in which the charging correlation scheme is applied only to the application service layer will not be described in detail herein, yet such process is still covered by the protection scope of the present invention.

[0024] The embodiments of the present invention are mainly oriented to session-based applications or services such as multi-party services. In conventional session-based services, session IDs (SIDs) corresponding to different service sessions are already employed. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers that perform PF of the multi-party service, a server performing CF, and UEs are used to exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement a charging process on the bearer control layer. In such process the AS of each application or service corresponds to a bearer control layer entity that is adapted to bear the AS.

[0025] At present, the mainstream multi-party services include Push-to-Talk over Cellular network (PoC) service, Conference service, etc. In a PoC service session, a server performing CF is a PoC server that performs CF, also called Controlling PoC Server; and the server performing PF is the PoC server that performs PF, also called Participating PoC Server. In a Conference service session, the server that performs CF is the Conference server that performs CF, also called a Controlling Conference Server; and the server performing PF is the Conference server that performs PF, also called a Participating Conference Server. The server performing PF and the server performing CF are logical functions of multi-party service servers, and the server performing PF and the server performing CF may be physically located in different ASs or in one AS. The server performing CF is referred to as the CF and the server performing PF is referred to as PF herein for the sake of simplicity. The embodiments of the present invention are described in detail herein taken a SIP based multi-party service as an example.

[0026] Figure 1 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. The entities involved in this embodiment include a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a present multi-party service, a called UE and a called PF of the called UE, a called IMS/SIP Core corresponding to the called PF and the called UE. The entities involved in this embodiment also include an AS-charging information collecting function corresponding to the calling PF, CF, and the called PF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. The calling UE, the calling PF and the CF correspond to a same bearer control layer entity i.e., the calling IMS/SIP Core, the called UE and the called PF correspond to a same bearer control layer entity i.e., the called IMS/SIP Core. The service control function of the current application or service performs CF of the multi-party service.

[0027] When the calling/called PF and CF are provided by servers in a network of one service provider, the calling/called PF and the CF may correspond to a same AS-charging information collecting function. In this embodiment, suppose that the calling/called PF and the CF correspond to a same AS-charging information collecting function. However, when the calling/called PF and the CF are provided by servers in different networks of different service providers, the calling/called PF and the CF may correspond to different AS-charging information collecting functions respectively, and accordingly, the calling/called PF and the CF send service identifiers and the CDRs to different AS-charging information collecting functions respectively. Similarly, when IMS/SIP Cores of the calling UE and the called UE are provided in a same network of a same operator, the calling/called IMS/SIP Cores may correspond to one IMS charging information collecting function. When the IMS/SIP Cores of the calling UE and the called UE are in different networks provided by different operators, the calling/called IMS/SIP Cores may correspond to different IMS charging information collecting functions and send service identifiers and the CDRs to different IMS charging information collecting functions respectively. In this embodiment, suppose that the calling/called IMS/SIP Cores correspond to one IMS charging information collecting function.

[0028] As shown in Figure 1, the process includes as follows.

[0029] 101-102: The calling UE sends a session es-

tablishment request to the calling PF via a corresponding calling IMS/SIP Core. The session establishment request may be carried in an SIP INVITE message in this embodiment; however, the present invention is not limited to this.

[0030] The application service layer entities such as the UE, PF, CF, etc., and the corresponding bearer control layer entities such as the IMS/SIP Core, etc., may be in a same network or in different networks. The present invention is not limited to this.

[0031] 103: The calling PF sends the session establishment request to the CF via the calling IMS/SIP Core.

[0032] 104: The CF assigns a service identifier (SID) for the current multi-party service session and the followings shall be performed once for each of the called UEs.

[0033] 105: The CF sends the session establishment request to the called IMS/SIP Core corresponding to the called PF via the calling IMS/SIP Core of the CF. The session establishment request carries the SID assigned in 104.

[0034] 106-107: The called IMS/SIP Core saves the received SID and sends the session establishment request carrying the SID to the called PF.

[0035] 108-109: The called PF saves the received SID and sends the session establishment request carrying the SID to the called UE via the called IMS/SIP Core.

[0036] 110-111: The called UE saves the received SID and returns a session establishment response carrying the SID to the called PF via the called IMS/SIP Core. The session establishment response is carried in an SIP 2000K message in this embodiment, however, the present invention does not limit to this.

[0037] 112-113: The called PF sends the session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0038] 114: The CF returns the session establishment response carrying the SID to the calling IMS/SIP Core.

[0039] 115-116: The calling IMS/SIP Core saves the received SID and returns the session establishment response carrying the SID to the calling PF, the calling PF also saves the received SID.

[0040] 117-119: The calling PF returns the session establishment response carrying the SID to the calling UE via the calling IMS/SIP Core, and the calling UE saves the received SID. By now, a session establishment process is completed.

[0041] In this embodiment, after receiving the SID, the service layer entities and bearer control layer entities related to the charging correlation process may insert the SID into or with the CDRs generated for the current application or service and send the CDRs to the corresponding charging information collecting functions. Specifically, the application service layer entities and bearer control layer entities generate CDRs after receiving a session establishment response indicating a successful session set-up or after sending the session establishment request, and the SID is included in the CDRs and the CDRs are sent to the charging information collecting functions. This embodiment describes a process in which the session is successfully established; hence it is supposed that the session establishment response always indicates a successful session set-up. In Figure 1, the application service layer entities related to the charging correlation process include a calling PF, a called PF and a CF; the bearer control layer entities related to the charging correlation process include a calling IMS/SIP Core and a called IMS/SIP Core. The procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities related to the charging correlation process includes the followings.

[0042] The called PF may perform step ***a*** after sending the session establishment request in 109 or after receiving the session establishment response in 111. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing ***a*** and the steps following 111. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during a current multi-party service.

[0043] The called IMS/SIP Core may save the SID when sending the session establishment request or when sending session establishment response that carries the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session establishment response in 112. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and the steps following 112. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE carrying the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0044] The CF may perform step c after receiving the session establishment response in 113. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***c*** and the steps following 113. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0045] The calling PF may perform step ***d*** after receiving the session establishment response in 116. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence

order of performing step ***d*** and the steps following 116. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start charging and sends the CDR of the calling UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0046] The calling IMS/SIP Core may save the SID after sending the session establishment response that carries the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session establishment response in 117. Step ***e*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***e*** and the steps following 117. Step ***e*** may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0047] When the calling UE and the called UE establish a session and start a multi-party service communication, the AS-charging information collecting function or the IMS charging information collecting function starts to record the actions of the calling and called UEs that are performed on the entities during the multi-party service in real-time.

[0048] In the embodiment shown in Figure 1, the calling and the called PFs send the received SID to the calling and the called UEs, respectively. As such, when it needs to modify the session, or to add a new user into a session, or to make a user re-enter into a session, or to make a user exit the session, it is possible for the UEs to send the SID to a server performing PF or a server performing CF, in order to generate partial CDRs corresponding to the SID, or to generate a new CDR corresponding to the SID, or to update the CDR corresponding to the SID, or to close the CDR corresponding to the SID, respectively. However, sending the SID to the calling and the called UEs is not essential. Only when the above factors are taking into consideration, it is necessary to send the SID to the calling and the called UEs. In Figure 1, the calling and called UEs do not negotiate media parameters before establishing a session i.e., the calling and the called UEs establish an on-demand session. When the calling and called UEs negotiate media parameters before establishing a session i.e., the calling and the called UEs establish a pre-established session, the charging correlation process will be different from the process shown in Figure 1, as shown in Figure 2.

[0049] Figure 2 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. In this embodiment, media parameters have been negotiated between the calling UEs and the calling PF that servers the calling UEs before establishing a session, and media parameters have been negotiated also between the called UEs and the called PF that servers the called UEs. The entities involved in the process are the same as the entities in Figure 1. A brief description of the pre-established session is given as follows. Before establishing a session, the UE negotiates session parameters with the server performing PF for the UE. The UE initiates a session establishment process by a session modify request such as a parameter message (REFER message). Therefore in the session establishment process, session parameters negotiation may be omitted and the UE does not need to upload session parameters. The UE just needs to indicate the server performing PF which service is to be joined by the UE. As such, SIP signaling that is exchanged with the UE has fewer bits, and air interface resources may be saved. The server performing PF then initiates a normal session establishment process with the server performing CF according to the indication from the UE, and informs the UE of a successful set-up by sending a media data control protocol message to the UE after the session between the PF and the CF is established. The media data control protocol may be the Talk Burst Control Protocol (TBCP) or the Media Burst Control Protocol (MBCP).

[0050] Figure 2 mainly includes followings.

[0051] 201-202: The calling UE sends a session modify request to the calling PF via the calling IMS/SIP Core corresponding to the calling UE. The calling PF returns a session modify response to the calling UE. The session modify request may be carried in an SIP parameter message (SIP REFER message) and the session modify response may be carried in an SIP accepted message (SIP ACCEPTED message), however, the present invention is not limited to this.

[0052] 203: The calling PF sends a session establishment request to the CF via the calling IMS/SIP Core corresponding to the calling PF.

[0053] 204: The CF assigns a service identifier SID for a current multi-party service and the followings is performed once for each of the called UEs.

[0054] 205: The CF sends the session establishment request to the called IMS/SIP Core via the calling IMS/SIP Core. The session establishment request carries the SID assigned in 204.

[0055] 206-207: The called IMS/SIP Core saves the received SID and sends the session establishment request that carries the SID to the called PF.

[0056] 208-210: The called PF saves the received SID and returns a session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0057] While returning the session establishment response to the CF, the called PF also performs 210'. 210' may include followings. The called PF sends to the called IMS/SIP Core a media data control protocol message

carrying the SID, such as a TBCP Connect message used to notify the called UE to join the current service. The called UE saves the SID and returns an acknowledgment e.g. a TBCP Talk Burst Acknowledge message to the called PF via the called IMS/SIP Core. The called PF sends a confirmation e.g. a TBCP Talk Burst Confirm message to the called UE and then media data streams may be transmitted to the called UE.

[0058] In this embodiment, suppose that the called UE has negotiated parameters with the called PF and an auto-answer mode Has been set. That is, the called PF may send the media data control protocol message to the called UE, and return a session establishment response to the CF, without requesting the called UE in advance. The media data control protocol message, such as a TBCP Connect message or a Talk Burst Confirm message that is sent to the called UE, carries the SID. In another example, the called UE may also be configured to a manual response mode. That is, the called PF first sends a session establishment request e.g. an INVITE message to the called UE and then sends the media data control protocol message to the called UE. The called PF sends a session establishment response to the CF after the called user agrees to join the current service. In such a case, the media data control protocol message such as a TBCP Connect message or Talk Burst Confirm message, or the session establishment request such as an INVITE message that is sent to the called UE, may carry the SID.

[0059] 211-214: The CF returns a session establishment response carrying the SID to the calling IMS/SIP Core. The calling IMS/SIP Core saves the received SID and returns a session establishment response carrying the SID to the calling PF. The calling PF also saves the received SID.

[0060] 215-217: The calling PF sends a media data control protocol message, such as a TBCP Connect message, to the calling UE via the calling IMS/SIP Core to inform the calling UE that it is ready for a service session setup. The calling UE returns an acknowledgment, such as a TBCP Talk Burst Acknowledge message, to the calling PF via the calling IMS/SIP Core. The calling PF sends a confirmation such as a TBCP Talk Burst Confirm message to the called UE and is ready to receive media data streams from the calling UE. After that, the calling PF sends a session setup notification such as a NOTIFY message carrying the SID to the calling UE via the calling IMS/SIP Core. The calling UE saves the received SID and a whole session establishment process is completed.

[0061] In this process, the calling PF sends the SID to the calling UE by carrying the SID in a session setup notification or in a media data control protocol message such as a TBCP Connect message or a Talk Burst Confirm message.

[0062] The procedure of sending the SID and the CDRs received from the application service layer entities and bearer control layer entities that are related to the charging correlation process may include the followings.

[0063] The called IMS/SIP Core may save the SID after sending the session establishment request that carries the SID, the media data control protocol message that carries the SID, or the session establishment response that carries the SID. The called IMS/SIP Core may perform Step ***a*** after receiving the session establishment response, e.g., the response to the session establishment request or the response to the media data control protocol message, from the called UE. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***a*** and other steps. Step ***a*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE to the IMS charging information collecting function, wherein the CDR of the called UE carries the SID. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0064] The called PF may perform step ***b*** after sending the session establishment request or media data control protocol message to the called UE, or after receiving the session establishment response e.g., a response to the session establishment request or a response to the media data control protocol message from the called UE. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and other steps. Step ***b*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during the current multi-party service.

[0065] The CF may perform step c after receiving the session establishment response in 210. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step c and the steps following 210. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs that carry the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0066] The calling PF may perform step ***d*** after receiving the session establishment response in 213. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***d*** and the steps following 213. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start

charging and sends the CDR of the calling UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0067] The calling IMS/SIP Core may save the SID after sending the session establishment response carrying the SID. The calling IMS/SIP Core may further perform step e after receiving the session establishment response in 211. Step e is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step e and the steps following 211. Step e may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0068] During a multi-party service, a UE may modify the session, for example, the UE may modify the session media parameters, which may result that the AS-charging information collecting function or IMS charging information collecting function may generate a partial CDR. The partial CDR and original CDRs belong to the same multi-party service and need to be correlated in the charging correlation process. Therefore, in a session modification process, the UE needs to send the SID saved during the session establishment process to entities such as the server performing PF and the server performing CF which are related to the charging correlation process, so that the entities can generate partial CDRs corresponding to the SID. In this way the partial CDR may be correlated with other CDRs generated for the multi-party service.

[0069] Figure 3 shows a flowchart of a charging correlation process in a session modification process in accordance with an embodiment of the present invention. The entities involved in this embodiment may include: a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a current multi-party service, a called UE and a called PF of the called UE, and a called IMS/SIP Core corresponding to the called PF and the called UE. This embodiment also involves: a AS-charging information collecting function corresponding to the calling PF, the called PF and the CF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. Figure 3 includes the following processes.

[0070] 301: The calling UE sends a session modify request that carries the SID to the calling PF via the calling IMS/SIP Core. The session modify request is carried in an SIP UPDATE message or in an SIP Re-INVITE message in this embodiment, however, the present invention is not limited to this.

[0071] 302: The calling PF sends the session modify request that carries the SID to the calling IMS/SIP Core.

[0072] 303: The calling IMS/SIP Core sends the session modify request that carries the SID to the CF, and the followings is performed once for each of the called UEs.

[0073] 304-305: The CF sends the session modify request that carries the SID to the called IMS/SIP Core via the calling IMS/SIP Core.

[0074] 306: The called IMS/SIP Core sends the session modify request that carries the SID to the called PF.

[0075] 307-308: The called PF sends the session modify request that carries the SID to the called UE via the called IMS/SIP Core.

[0076] 309-310: The called UE returns a session modify response that carries the SID to the called PF via the called IMS/SIP Core. The session modify response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0077] 311-313: The called PF sends the session modify response that carries the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0078] 314-315: The CF returns the session modify response that carries the SID to the calling IMS/SIP Core, the calling IMS/SIP Core returns the session modify response that carries the SID to the calling PF.

[0079] 316-317: The calling PF returns the session modify response that carries the SID to the calling UE via the calling IMS/SIP Core and the session modify process is completed.

[0080] In the above process, the procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities that are related to the charging correlation process includes the followings.

[0081] The called PF may perform step ***a*** after sending the session modify request to the called UE or after receiving the session modify response from the called UE. Step ***a*** is independent from steps following 307 and the present invention does not limit the sequence order of performing step ***a*** and the steps following 307. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the called PF, saves the partial CDR, and starts to record actions that may affect an accounting and are performed by the called UE on the called PF after the session is modified in the current multi-party service.

[0082] The called IMS/SIP Core may save the SID after sending the session modify request or the session modify request response carrying the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session modify response from the called UE. Step ***b*** is independent from steps following 309 and the present inven-

tion does not limit the sequence order of performing step ***b*** and the steps following 309. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the called IMS/SIP Core, saves the partial CDR and starts to record actions that may affect an accounting and are performed by the called UE on the called IMS/SIP Core after the session is modified in the current multi-party service.

[0083] The CF may perform step c after receiving the session modify response in 313. Step c is independent from steps following 313 and the present invention does not limit the sequence order of performing step ***c*** and the steps following 313. Step ***c*** may include followings. The CF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDRs of the calling UEs and the called UEs, that is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the CF, saves the partial CDRs of the calling and the called UEs and starts to record actions that may affect an accounting and are performed by the calling and called UE on the CF after the session is modified in the current multi-party service.

[0084] The calling PF may perform step ***d*** after receiving the session modify response in 315. Step ***d*** is independent from steps following 315 and the present invention does not limit the sequence order of performing step ***d*** and the steps following 315. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDR of the calling UE, which is generated by the calling PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the calling PF, saves the partial CDR of the calling UE and starts to record actions that may affect an accounting and are performed by the calling UE on the calling PF after the session is modified in the current multi-party service.

[0085] The calling IMS/SIP Core may save the SID while sending the session modify response carrying the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session modify response in 314. Step e is independent from steps following 314 and the present invention does not limit the sequence order of performing step e and the steps following 314. Step e may include followings, the calling IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends the partial CDR of the calling user, which is generated by the calling IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the calling IMS/SIP Core, saves the partial CDR of the calling user and starts to record actions that may affect an accounting and are performed by the calling UE on the calling IMS/SIP Core after the session is modified in the current multi-party service.

[0086] In the embodiments shown in Figures 1 to 3, the calling PF, the CF and the called PF are separated entities. In practical applications, any one or any combination of the calling PF, the CF and the called PF may be provided by one entity, in which case the basic processes are the same as the embodiments shown in Figures 1 to 3, and will not be described in detail herein but are still covered by the protection scope of the present invention.

[0087] In Figures 1 and 2, the calling PF and the CF correspond to a same IMS/SIP Core and the called PF corresponds to another IMS/SIP Core. In practical applications, the calling PF, the CF and the called PF may correspond to different IMS/SIP Cores. When the calling UE and a called UE are in one network provided by an operator, the calling PF and the called PF of the called UE may correspond to the same IMS/SIP Core. When the calling UE and a called UE are in different networks provided by different operators, the calling PF and the called PF correspond to different IMS/SIP Cores. When the calling PF and the CF are in one network provided by the same operator, the calling PF and the CF correspond to the same IMS/SIP Core. When the called PF and the CF are in different networks provided by different operators, the called PF and the CF correspond to different IMS/SIP Cores. However, no matter the calling PF, the CF and the called PF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the processes in embodiments of the present invention are essentially the same. In one word, the application service layer entities such as the calling PF, the CF and the called PF send/receive session establishment/modify requests or session establishment/modify responses via corresponding IMS/SIP Cores, and the detailed processes thereof will not be described herein, but are still covered by the protection scope of the present invention.

[0088] During an existing multi-party service, when adding a new user, the control function entity (e.g., the CF) of the multi-party service generates a new CDR for a session of the new user. A service identifier will be adapted to correlate the CDRs of the new user when adding the new user.

[0089] Figure 4 shows a flowchart of a charging correlation process when adding a new user to an existing multi-party service in accordance with an embodiment of the present invention. A process of adding a new user includes: requesting by a UE to add another user (a third party user) into a current multi-party service. The third party user is shown as an added UE in Figure 4. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, an added UE, a CF of the current multi-party service, an

AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, suppose that the UE and the new user added to the current service (the added UE) are served by the same PF, and the UE, the added UE, the PF and the CF correspond to the same IMS/SIP Core.

[0090] As shown in Figure 4, the process includes followings.

[0091] 401-402: The UE sends an adding request that carries an SID to the PF via the IMS/SIP Core. The adding request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0092] 403-404: The PF sends the adding request that carries the SID to the CF via the IMS/SIP Core.

[0093] 405-406: The CF sends the adding request that carries the SID to the PF of the added UE via the IMS/SIP Core, and the PF sends the adding request that carries the SID to the added UE. The added UE returns an adding response that carries the SID to the PF via the IMS/SIP Core after receiving the adding request. The PF returns the adding response that carries the SID to the CF via the IMS/SIP Core. As such, the new UE is added to the current service.

[0094] The adding request may be carried in an SIP INVITE message and the adding response may be carried in an SIP 2000K message, however, the present invention is not limited to this.

[0095] 407: The CF returns the adding response that carries the SID to the PF of the UE via the IMS/SIP Core. The PF informs the UE that the new user has been added to the current service by returning the adding response that carries the SID to the UE via the IMS/SIP Core. The adding response may be carried in an SIP ACCEPTED message in this embodiment; however, the present invention is not limited to this.

[0096] In Figure 4, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the adding response in 406. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the follow-up steps. The PF may perform step ***b*** after receiving the adding response in 406 and step ***b*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***b*** and the follow-up steps.

[0097] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to start charging and sends the CDR of the new user (the added UE) that is generated by the CF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the CF and starts to record actions performed by the new user on the CF during the current multi-party service.

[0098] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the new user that is generated by the PF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the PF and starts to record actions performed by the new user on the PF during the current multi-party service.

[0099] The bearer control layer entity related to the charging correlation process in Figure 4 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the adding response in 406, and step c is independent of other following steps and the present invention does not limit the sequence order of performing step c and the follow-up steps. Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the new user that is generated by the IMS/SIP Core and carries the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the new user from the IMS/SIP Core and starts to record actions performed by the new user on the IMS/SIP Core during the current multi-party service.

[0100] In embodiments shown in Figures 3 and 4, the UE may establish an on-demand session or have a pre-established session, the processes in Figures 3 and 4 may be applied to both cases.

[0101] If a UE exits a session, the AS-charging information collecting function and the IMS charging information collecting function need to close the CDRs of the multi-party service of the UE. In such a case, the SID of the current multi-party service needs to be sent to the AS-charging information collecting function and the IMS charging information collecting function so that the CDRs corresponding to the same SID among all CDRs of the UE may be closed based on the same SID.

[0102] Figure 5 shows a flowchart of a charging correlation process when a UE that has established a pre-established session exits a session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0103] As shown in Figure 5, the process includes followings.

[0104] 501-502: The UE sends a release session request that carries an SID to the PF via the IMS/SIP Core. The release session request is carried in an SIP BYE message in this embodiment, however, the present invention is not limited to this.

[0105] 503: The PF sends the release session request that carries the SID to the CF via the IMS/SIP Core.

[0106] 504: The CF returns a release session response that carries the SID to the PF via the IMS/SIP Core. The release session response may be carried in

an SIP 200OK message in this embodiment, however, the present invention is not limited to this.

[0107] 505-506: The PF sends the release session response that carries the SID to the UE via the IMS/SIP Core.

[0108] In Figure 5, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session response in 503. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 503. The PF may perform step ***b*** after receiving the release session response in 504 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 504.

[0109] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording charging data of the UE.

[0110] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0111] The bearer control layer entity related to the charging correlation process in Figure 5 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 505, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 505.

[0112] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0113] The release session process shown in Figure 5 is suitable to be used for a user who establishes an on-demand session. For a user who establishes a pre-established session, a different release session process shall be used. Figure 6 shows a flowchart of a charging correlation process for a user who establishes a pre-established session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0114] A whole session establishment process for a user who establishes a pre-established session includes two parts: firstly, the UE and the PF negotiate session parameters before establishing a session; then, the PF establishes a session with the CF for the UE when the UE is ready for establishing the session. Therefore this kind of session establishment process shall be ended in two steps: firstly, the session that is pre-established between the UE and the PF is modified; then, the session between the PF and the CF is released. As shown in Figure 6, the process includes followings.

[0115] 601-602: The UE sends a session modify and release request that carries an SID to the PF via the IMS/SIP Core in order to release the session. The session modify and release request may be carried in an SIP REFER BYE message in this embodiment, however, the present invention is not limited to this.

[0116] 603: The PF returns a session modify response to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0117] 604: The PF sends a release session request carrying the SID to the CF via the IMS/SIP Core. The release session request may be carried in a BYE message, however, the present invention is not limited to this.

[0118] 605: The CF returns a release session response to the PF via the IMS/SIP Core. The release session response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0119] 606-607: The PF sends a release session notification to the UE via the IMS/SIP Core to notify the UE of a successful release of the session between the UE and the CF. The UE returns a release session response to the PF. The release session response may be carried in a NOTIFY message, and the release session response may be carried in an OK message, however, the present invention is not limited to this.

[0120] In Figure 6, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session request in 604 and after successful releasing the session. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 604. The PF may perform step ***a*** after receiving the release session response in 607.

[0121] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording the charging data of the UE.

[0122] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0123] The bearer control layer entity related to the

charging correlation process in Figure 6 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 605, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 605.

[0124] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0125] Besides the situations described above, new CDRs may be generated by the entities related to the charging correlation process in two other situation. The charging correlation processes in accordance with the embodiments of the present invention are suitable in such two situations. In the first situation, a user who establishes an on-demand session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. In the other of the two situations, a user who establishes a pre-established session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. The charging correlation processes in the two situations are described with reference to Figures 7 and 8.

[0126] Figure 7 shows a flowchart of a charging correlation process in a case that a user who establishes an on-demand session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to a same IMS/SIP Core. As shown in Figure 7, the process includes followings.

[0127] 701-702: The UE sends a session joining request carrying an SID to the PF via the IMS/SIP Core. The session joining request may be carried in an SIP REFER message or an SIP INVITE message in this embodiment, however, the present invention is not limited to this.

[0128] 703: The PF sends the session joining request carrying the SID to the CF via the IMS/SIP Core.

[0129] 704: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 2000K message or an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0130] 705-706: The PF sends the session joining response carrying the SID to the UE via the IMS/SIP Core.

[0131] In Figure 7, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining response in 703. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 703. The PF may perform step ***b*** after receiving the session joining response in 704 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 704.

[0132] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user who requests to re-enter the session (the UE), which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0133] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0134] The bearer control layer entity related to the charging correlation process in Figure 7 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 705, and step c is independent of following steps and the present invention does not limit the sequence order of performing step ***c*** and the steps following 705.

[0135] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0136] Figure 8 shows a flowchart of a charging correlation process in a case where a user who establishes a pre-established session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of the current multi-party service, an AS-charging information collecting function and an IMS charging information collecting func-

tion. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core. As shown in Figure 8, the process includes followings.

[0137] 801-802: The UE and the PF negotiate session parameters before establishing a session. Then the UE sends a session modify request carrying an SID to the PF via the IMS/SIP Core. The session modify request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0138] 803: The PF returns a session modify response carrying the SID to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment. However, the present invention is not limited to this.

[0139] 804: The PF sends a session joining request carrying the SID to the CF via the IMS/SIP Core to establish a session between the UE and the CF. The session joining request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0140] 805-806: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 200OK or an OK message. However, the present invention is not limited to this.

[0141] 807-809: The PF sends to the UE a session joining notification (e.g., a NOTIFY message) carrying a result of the session setup via the IMS/SIP Core. The UE returns a session joining response (e.g., an OK response) to the PF via the IMS/SIP Core. As such, the session re-entering process is completed.

[0142] In Figure 8, the service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining request in 804 and after successful adding the UE into the session. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 804. The PF may perform step b after receiving the session joining response in 809 and similarly, the bearer control layer entity related to the charging correlation process, i.e., the IMS/SIP Core, may perform step c after receiving the response in 809.

[0143] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user (the UE) who requests to re-enter the session, which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE that is generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0144] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0145] The bearer control layer entity related to the charging correlation process in Figure 8 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 805, and step c is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 805.

[0146] Step c may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0147] In embodiments shown in Figures 4 to 8, the PF and the CF are performed by two separated entities. In practical applications, the PF and the CF may be performed by one entity. In such a case, the essential processes of the embodiments in which the PF and the CF are performed by one entity are similar to the processes shown in Figures 4 to 8 and will not be described in detail herein, but are still covered by the protection scope of the invention.

[0148] Moreover, the PF and the CF correspond to the same bearer control layer entity e.g., the IMS/SIP Core in Figures 4 to 8. In practical applications, the PF and the CF may correspond to different bearer control layer entities. When the PF and the CF are in the same network of an operator, the PF and the CF correspond to the same IMS/SIP Core. When the PF and the CF are in different networks of different operators, the PF and the CF correspond to different IMS/SIP Cores. No matter the PF and the CF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the method in accordance with embodiments of the present invention is applicable. No matter the PF and the CF correspond to the same bearer control layer entity or to different bearer control layer entities, the method in accordance with embodiments of the present invention is applicable. In one word, the application service layer entities such as the PF and the CF send/receive messages comprising session modify requests/responses, session joining requests/responses, release session requests/responses, session modify requests/responses and session modify and release requests via corresponding IMS/SIP Cores. Detailed proc-

esses will not be described herein, but are still covered by the protection scope of the present invention.

[0149] In the flowcharts of the above embodiments, the responses returned by the called UE to the CF carry the SID. However, since the CF has learnt the SID of the current service, the responses from the called UE to the CF may not carry the SID.

[0150] In the above embodiments, the SID is sent to the AS-charging information collecting function and IMS charging information collecting function, thus the application service layer of the AS and the bearer control layer of the IMS can perform a function in accordance with the charging correlation scheme provided by embodiments of the present invention. In practical applications, it may be unnecessary for the application service layer or the bearer control layer to implement the charging correlation process, and in such a case the SID and CRDs needs not to be sent to the AS-charging information collecting function or the IMS charging information collecting function.

[0151] The embodiments of the present invention adopt SIDs as service identifiers, and a description of the SID used in a PoC service is given herein. In a PoC service, SID is assigned by a service control function to a calling/called PoC client. The SID is used to identify a PoC group session in an SIP communication, but is not used in charging data generation processes. A PoC Session Identity (PoC SID) is constructed in a format of a SIP Uniform Resource Identifier (URI) and is sent during a PoC session establishment process to a PoC client in a Contact header field and/or a TBCP CONNECT message. The PoC SID may be assigned and available for a long period, or be assigned temporarily. A long term PoC SID is adapted to a pre-arranged PoC group session. A temporary PoC SID is assigned by a server performing CF in the network to a PoC client when the PoC client establishes a PoC session for a PoC service for a first time, and is remained valid as long as the PoC service is in progress. When the PoC client establishes a session for another PoC service, the new PoC service is assigned a different PoC SID. However, if the PoC client exits a session of a PoC service temporarily and re-enters the same PoC service later, the PoC SID to used in the session will remain the same. It can be seen that the PoC SID may be used to identify a PoC service, therefore the PoC SID can also be used to charge correlation information of the service. Such PoC SID cannot be modified easily in transmission and the PoC client cannot modify the PoC SID after receiving the PoC SID, hence it is safe and reliable to use the PoC SID in a charging correlation process.

[0152] Embodiments of the present invention also propose a second charging correlation scheme to implement a charging correlation for a plurality of CDRs generated for one user in a multi-service that comprises a plurality of sub-services. The charging correlation scheme provides two ways to implement this charging correlation.

[0153] According to a first method, a service control function assigns a multi-service identifier for a current multi-service and assigns a sub-service identifier to each of the sub-services included in the current multi-service. The multi-service identifier and the sub-service identifiers are sent to a charging system. The charging system correlates CDRs of a sub-service based on the sub-service identifier of the sub-service, and correlates CDRs of the plurality of sub-services based on the multi-service identifier.

[0154] According to a second method, a service control function just assigns a multi-service identifier for a current multi-service. The multi-service identifier is sent to a charging system which correlates the CDRs of a plurality of sub-services of the current multi-service based on the multi-service identifier.

[0155] In a multi-service, a user may establish one or a plurality of sessions in each of the sub-services and a CDR is generated for each of the sessions of the user. Different methods may be used to correlate the CDRs based on the multi-service identifier. The CDRs to be correlated based on the multi-service identifier may be: CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) establish for one user in the current multi-service, or CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) established for a part of users or all users in the current multi-service. The method of correlating CDRs may be chosen based on special correlation policy applied. The contents and forms of correlation policies are not the technical problem to be solved by the present invention and will not be described further herein.

[0156] In a multi-service, a sub-service corresponds to a sub-service server. A service control function controls the sub-service servers to initiate, modify and terminate sub-services in order to initiate, modify and terminate the multi-service. According to the first method described above, for a sub-service, after the service control function assigns the multi-service identifier and the sub-service identifiers corresponding to the sub-services, the service control function sends the multi-service identifier and a sub-service identifier corresponding to a sub-service to a sub-service server corresponding to the sub-service. The sub-service server generates CDRs for the sub-service and sends the CDRs, the received multi-service identifier and the sub-service identifier to an AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier, the sub-service identifier and the CDRs to a billing center. The billing center correlates the CDRs generated by one sub-service server based on the sub-service identifier, and further correlates CDRs generated by the sub-service servers based on the multi-service identifier. According to the second method described above, after assigning the multi-service identifier, the service control function sends the multi-service identifier to each sub-service server corresponding to each sub-service. A sub-service

server generates CDRs for each corresponding sub-service and sends the received multi-service identifier and the CDRs generated to the AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier and the CDRs to the billing center. The billing center correlates the CDRs from different sub-service servers based on the multi-service identifier.

[0157] When the charging correlation scheme is applied to the application service layer, the charging information collecting function includes the AS-charging information collecting functions corresponding to the sub-service servers. The scheme can further be applied to the bearer control layer, and in such a case the charging information collecting function includes bearer control layer-charging information collecting functions of the bearer control layer entities corresponding to the sub-service servers. The bearer control layer entities corresponding to the sub-service servers are used to implement the service control functions. The bearer control layer entities corresponding to the sub-service servers are further used to record the multi-service identifier or a combination of the multi-service identifier and a sub-service identifier, and generate CDRs for corresponding sub-services. The bearer control layer entities send the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier, and the CDRs to the bearer control layer-charging information collecting function of the bearer control layer entities. The AS-charging information collecting function and the bearer control layer-charging information collecting function send the received CDRs, and the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier to the billing center. In Figures 9 and 10, the application service layer is taken as an example. When the present invention is applied only to the bearer control layer, charging correlation process involves UEs, service control functions, bearer control layer entities corresponding to sub-service servers, bearer control layer-charging information collecting functions and a billing center, without involving sub-service servers and AS-charging information collecting functions. Embodiments that the bearer control layer is employed are not described in detailed herein, but are still covered by the protection scope of the present invention. When the multi-service identifier or the combination of the multi-service identifier and the sub-service identifier is sent to an AS-charging information collecting function or to bearer control layer-charging information collecting function, the multi-service identifier or the combination of the multi-service identifier and the sub-service identifiers may be carried in CDRs.

[0158] Moreover, a multi-service usually includes a primary service and one or more supplementary services. That is, a multi-service includes a sub-service as the primary service and at least one sub-service as the supplementary service. The sub-service server and sub-service identifier corresponding to the primary service are called primary server and primary service identifier respectively, and the sub-service server and sub-service identifier corresponding to a supplementary service are called supplementary server and supplementary service identifier respectively. The service control function may be performed by a separated entity or be performed by the primary server. The multi-service identifier assigned to the multi-service may be identical with or different from the sub-service identifiers. When the multi-service includes a primary service and at least one supplementary service, the multi-service identifier may be identical with the primary service identifier.

[0159] The embodiments of the present invention are mainly applied to session-based applications or services such as multi-party services, the session IDs (SIDs) corresponding to different service sessions are already applied to conventional session-based services. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers performing PF of the multi-party service, the server performing CF, and the UEs may exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, the network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement the charging correlation process on the bearer control layer. Each sub-service server of a sub-service corresponds to a bearer control layer entity, and the bearer control layer entity is adapted to bear the sub-service server.

[0160] At present, mainstream multi-services include: combinations of a plurality of multi-party services, a combination of a multi-party service and a Location Service or a combination of a multi-party service and a Presence Service. The second charging correlation scheme of the present invention is described hereinafter with reference to a multi-service comprising two multi-party services, e.g. a PoC service and a Conference service. A server performing CF and a server performing PF in the multi-party service are used to provide the services, yet the second charging correlation scheme focuses on the charging correlation of the sub-services, not internal flows of the sub-services. Therefore, for the sake of simplicity, the service processes between the server performing CF and the server performing PF in the multi-party service are omitted, and the server performing CF and the server performing PF are considered as sub-service servers of the multi-party service. A sub-service server corresponding to the PoC service is called a PoC server, and a sub-service server corresponding to the Conference service is called a Conference server. In embodiments of the present invention, the service control function is implemented by a PoC server.

[0161] Figure 9 shows a flowchart of a charging cor-

relation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier. In this embodiment, the SID adapted to an individual PoC service in a conventional PoC service is used as the multi-service identifier. The entities involved in the embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 9, the process includes followings.

[0162] 901: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2, and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier to the current multi-service. The multi-service identifier is the SID assigned to the PoC service. The session establishment request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0163] 902: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 200OK message). The session establishment request carries the information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0164] After 902, both the PoC service and the Conference service are originated and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service and CDRs of the Conference service on the AS-charging information collecting function.

[0165] Step ***a*** may include the followings. The Conference server generates CDRs for the present Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that are generated by the Conference server and carries the SID. The AS-charging information collecting function opens the CDR received from the Conference server, starts to record actions which affect the accountings and, are performed on the Conference server by users of the Conference service, and returns a response to the Conference server.

[0166] Step ***b*** may include the followings. The PoC server generates a CDR for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDR that is generated by the PoC server and carries the SID. The AS-charging information collecting function opens the CDR received from the PoC server, starts to record actions which affect the accountings and are performed on the PoC server by users of the PoC service, and returns a response to the PoC server.

[0167] 903: The PoC server sends a session joining request carrying the SID to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0168] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step c needs to be performed. Step c may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDR carrying the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDR of PoC Client 2 that carries the SID and is received from the PoC server, records the information of PoC Client 2 in the CDR, starts to record actions that affect the accounting and are performed by PoC Client 2 on the PoC server during the current multi-service, and returns a response to the PoC server.

[0169] 904: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 2 into the current Conference service session.

[0170] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, sends the CDRs that carries the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carries the SID and is received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0171] 905-906: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID to the Conference server, and the Conference server returns a session joining response (e.g., a 200OK message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 need to be added into the Conference service. At the same time, the

PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0172] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step e needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client 1 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the PoC server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0173] 907: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 1 into the current Conference service session.

[0174] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client I to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the Conference server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0175] After the processes described above, the CDRs of the sub-services, which are saved in the AS-charging information collecting function, carry the multi-service identifier, therefore, the CDRs of the sub-services can be correlated based on the multi-service identifier.

[0176] Figure 10 shows a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier for the multi-service and assigns a sub-service identifier to each sub-service. In this embodiment, the sub-service identifier of the PoC service adopts the SID assigned for an individual PoC service in the conventional PoC service, called SID1. The sub-service identifier of the Conference service adopts the SID assigned for an individual Conference service in the conventional Conference service, called SID2. The entities involved in this embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 10, the process includes followings.

[0177] 1001: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2 and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier for the current multi-service, assigns one or more sub-service identifiers to the PoC service and assigns one or more sub-service identifiers to the Conference service.

[0178] The sub-service identifier of the PoC service adopts the SID assigned to the PoC service, called SID1; the sub-service identifier of the Conference service adopts the SID assigned to the Conference service, called SID2; and the multi-service identifier adopts the SID assigned to the multi-service, called SID0. The session establishment request may be carried in an SIP INVITE message in this embodiment. However, the present invention is not limited to this.

[0179] 1002: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 2000K message). The session establishment request carries information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0180] After 1002, both the PoC service and the Conference service are originated, and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service session and CDRs of the Conference service session on the AS-charging information collecting function.

[0181] Step ***a*** may include the followings. The Conference server generates CDRs for the current Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the Conference server and carries the SID0 and SID2. The AS-charging information collecting function opens the CDRs received from the Conference server, starts to record actions of the Conference service which are performed on the Conference server by users and affect the accounting, and returns a response from the AS-charging information collecting function to the Conference server.

[0182] Step ***b*** may include the followings. The PoC

server generates CDRs for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the PoC server and carries the SID0 and SID1. The AS-charging information collecting function opens the CDRs from the PoC server, starts to record actions of the PoC service which are performed on the PoC server by users and affect the accounting, and returns a response to the PoC server.

[0183] 1003: The PoC server sends a session joining request carrying the SID0 and SID1 to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0184] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step ***c*** needs to be performed. Step ***c*** may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID0 and SID1 of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID1 and are received from the PoC server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0185] 1004: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 1003 in order to add PoC Client 2 into the current Conference service.

[0186] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 2. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0187] 1005-1006: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server, and the Conference server returns a session joining response (e.g., a 2000K message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 can be added into the Conference service session. At the same time, the PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0188] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service on the AS-charging information collecting function, therefore step ***e*** needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID1 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID1 are received from the PoC server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0189] 1007: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 1003 to add PoC Client 1 into the current Conference service session.

[0190] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0191] After the processes described above, CDRs of the sub-services in the AS-charging information collecting function have the multi-service identifier and the sub-service identifiers corresponding to the sub-services. Therefore the CDRs of a sub-service may be correlated based on the sub-service identifier of the sub-service, and the CDRs of different sub-services, which have al-

ready been correlated based on the sub-service identifiers, are then correlated based on the multi-service identifier.

[0192] Figures 9 and 10 illustrate the second charging correlation scheme of the present invention which is applied to the application service layer. When the charging correlation scheme is applied to the bearer control layer, the entities involved include: a bearer control layer entity corresponding to the sub-service servers, a bearer control layer-charging information collecting function, and UEs. The bearer control layer entities corresponding to the sub-service servers may record the multi-service identifier and/or sub-service identifiers when the multi-service identifier and/or sub-service identifiers are received by the sub-service servers, generate CDRs, and send the received multi-service identifier and/or sub-service identifiers and the CDRs to the corresponding bearer control layer-charging information collecting functions. The processes in which the charging correlation scheme is applied to the bearer control layer is similar to that in Figures 9 and 10 and will not be described in detail herein, but is covered by the protection scope of the present invention.

[0193] Moreover, the charging correlation process may be variable based on different multi-services to be charged for, yet the charging correlation process will always be in accordance with the two methods of implementing the second charging correlation scheme provided in the above embodiments of the present invention. Since different multi-services may include various sub-services, the charging flow may vary in different ways. For example, the service control function may send the multi-service identifier and the sub-service identifiers to the primary server and the supplementary servers in different ways: 1) the service control function may send a primary service identifier when initiating a primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 2) the service control function may send the multi-service identifier when initiating the primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 3) the service control function may send a supplementary service identifier when initiating corresponding supplementary service session, or when setting up corresponding supplementary service session, or when setting up the current multi-service session; 4) the service control function may send the multi-service identifier when initiating each of the supplementary service sessions, or when setting up each of the supplementary service sessions, or when setting up the current multi-service session. Various charging correlation processes for various multi-services will not be listed herein. However, any charging correlation process for multi-service that is in accordance with the principles of the current invention falls in the scope of the present invention.

[0194] In embodiments of the present invention, a sub-service included in a multi-service can be any application or service. A multi-service may include sub-services such as PoC service, Conference service, Location service, Presence service and any combination of the above applications and services.

[0195] A system for charging correlation for an application or service is further proposed. Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention. In an embodiment of the present invention, the system includes a service identifier generating unit, a CDR generating unit and a CDR correlating unit.

[0196] The service identifier generating unit is adapted to assign a service identifier to a current application or service and send the service identifier to the CDR generating unit. The CDR generating unit is adapted to receive the service identifier from the service identifier generating unit, generate a plurality of CDRs for the current application or service and send the received service identifier and the CDRs generated to the CDR correlating unit. The CDR correlating unit is adapted to receive the CDRs and the service identifier from the CDR generating unit and correlate the CDRs of the current application or service based on the service identifier.

[0197] The service identifier generating unit may be a separated entity or be integrated into the service control function of the application or service. When the system is applied to a single-service, the service control function is an AS of the current application or service, e.g., a server performing CF for a multi-party service such as PoC service and Conference service. When the system is applied to a multi-service, the service control function is a service control function of the current multi-service. The service control function may be integrated into an AS of a sub-service (i.e., a sub-service server) of the multi-service or be integrated into a server performing CF for the multi-party service such as the PoC service and the Conference service. The CDR correlating unit may also be a separated entity or be integrated into a charging system.

[0198] Moreover, the CDR generating unit may further add the received service identifier into the CDRs generated so that the CDRs and the service identifier may be sent.

[0199] In the system provided by embodiments of the present invention, the units may function according to the processes described in the preceding embodiments, and detailed functions of the units are not described anymore.

[0200] A system for charging correlation is also proposed by embodiments of the present invention. The system for charging correlation includes a service control function entity and a charging system. The service control function entity is adapted to assign a service identifier to a current application or service and the charging system is adapted to correlate at least one set of CDRs generated for the application or service based on the service iden-

tifier that is assigned by the service control function entity. The charging system may further include a charging information collecting function entity and a billing center. The charging information collecting function entity is adapted to receive the service identifier from the service control function entity and collect at least one set of CDRs, and the billing center is adapted to correlate at least one set of CDRs based on the service identifier.

[0201] The service control function entity may be an AS adapted to generate at least one set of CDRs for the application or service. The system may further include a bearer control layer entity adapted to record the service identifier assigned by the service control function entity, and generate at least one set of CDRs. In such a case the charging information collecting function entity further includes an AS-charging information collecting function entity and a bearer control layer-charging information collecting function entity. The AS-charging information collecting function is adapted to receive the service identifier from the service control function entity (i.e., the AS) and the at least one set of CDRs generated by the service control function entity, and the bearer control layer-charging information collecting function entity is adapted to receive the service identifier from a bearer control entity and the at least one set of CDRs generated by the bearer control layer entity. Therefore the billing center can correlate the at least one set of CDRs received from the bearer control layer-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs received from the AS-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs from the bearer control layer-charging information collecting function entity and the at least one set of CDRs from the AS-charging information collecting function entity based on the service identifier.

[0202] When the application or service is a multi-party service, the service control function entity is a server performing CF. At least one server performing PF may further be included. The bearer control layer entity may include a bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer entity corresponding to the server performing PF. The bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF, and a bearer control layer entity corresponding to a server performing PF is adapted to bear the server performing PF. The AS-charging information collecting function entity may further include an AS-charging information collecting function entity of the server performing CF and at least one AS-charging information collecting function entity of the server performing PF. The bearer control layer-charging information collecting function entity may further include a bearing control layer charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer-charging information collecting function entity of a bearer control layer entity corresponding to a server performing PF.

[0203] When the application or service is a multi-service comprising a plurality of sub-services, the system may further include sub-service servers of a plurality of sub-services. The bearer control layer entity may further include at least one bearer control layer entity corresponding to a plurality of sub-service servers. The bearer control layer entity corresponding to the sub-service servers is adapted to bear the sub-service servers. The AS-charging information collecting function entity may further include AS-charging information collecting function entities of sub-service servers, and the bearer control layer-charging information collecting function entity may further include bearer control layer-charging information collecting function entities of bearer control layer entities of sub-service servers.

[0204] The functions of the components of the system in various cases have been given in the preceding description and will not be explained further herein, but are still covered by the protection scope of the present invention.

[0205] A billing center is also proposed in embodiments of the present invention. The billing center may include a first module adapted to receive a service identifier of the current application or service, and receive at least one set of CDRs generated for the application or service, and a second module adapted to correlate at least one set of CDRs based on the service identifier received by the first module and generate a bill. The CDRs received by the first module may be CDRs generated by an AS and CDRs generated by a bearer control layer entity. The second module may correlate the CDRs generated by the AS based on the service identifier, or correlate the CDRs generated by the bearer control layer entity based on the service identifier, or correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity together based on the service identifier.

[0206] An apparatus for generating charging data record is also proposed in embodiments of the present invention. The an apparatus for generating charging data record may include a first module and a second module. The first module is adapted to receive a service identifier assigned to the current application or service, and the second module is adapted to generate for the application or service at least one set of CDRs carrying the service identifier that is received by the first module and adapted to export the at least one set of CDRs. The an apparatus for generating charging data record may be an AS or a bearer control layer entity in embodiments of the present invention.

[0207] In one word, in embodiments of the present invention, a plurality of CDRs generated for a user in a service session may be correlated for charging, and the CDRs of a plurality of sub-services in a multi-service of the user can also be correlated for charging. Furthermore, the embodiments of the present invention is easy to implement and can improve accuracy of correlated

charging. Therefore the methods and apparatus proposed in the embodiments of the present invention are beneficial in supplementing and improving the conventional application or service charging correlation process (especially the charging correlation process of a multi-party service).

[0208] The previous description of the disclosed embodiments is provided to enable those skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art and generic principles defined herein may be applied to other embodiments without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

Claims

1. A method for charging correlation for an application or service, comprising:

   assigning a service identifier by a service control function to an application or service;
   sending the service identifier to a charging system; and
   correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

2. The method according to Claim 1, wherein the charging system comprises a charging information collecting function entity and a billing center; and the method further comprises:

   sending the service identifier to the billing center via the charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the service control function entity based on the service identifier.

3. The method according to Claim 2, wherein the application or service is a single-service, the service control function entity comprises an Application Server AS and the charging information collecting function entity comprises an AS charging information collecting function entity corresponding to the AS; and the method further comprises:

   assigning a service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier.

4. The method according to Claim 3, wherein the charging information collecting function entity further comprises: a bearer control layer charging information collecting function entity corresponding to a bearer control layer entity that corresponds to the AS, and the method further comprises:

   assigning the service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity;
   recording the service identifier by the bearer control layer entity that corresponds to the AS;
   sending the service identifier to the billing center via the bearer control layer charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier and correlating the at least one CDR generated by the bearer control layer entity based on the service identifier; or correlating the at least one CDR generated by the AS together with the at least one CDR generated by the bearer control layer entity based on the service identifier.

5. The method according to Claim 4, wherein the application or service is a multi-party service, the AS further comprises a server performing Control Function CF and at least one server performing Participating Function PF, and the service control function entity is the server performing CF; the AS charging information collecting function entity further comprises: at least one AS charging information collecting function entity covered by the server performing CF and at least one AS charging information collecting function entity covered by at least one server performing PF; the bearer control layer charging information collecting function entity further comprises at least one bearer control layer charging information collecting function entity covering the bearer control layer entities corresponding to the server performing CF and at least one server performing PF respectively, the bearer control layer entity corresponding to the server performing CF is used for bearing the server performing CF and the bearer control layer entity corresponding to a server performing PF is used for bearing the server performing PF;
   the server performing CF assigns the service identifier to the multi-party service and sends the service identifier to the at least one server performing PF, the server performing CF and the at least one server performing PF send the service identifier to the billing

center respectively via the AS charging information collecting function entity which corresponds to the server performing CF and the AS charging information collecting function entity which corresponds to the server performing PF;
the bearer control layer entities corresponding respectively to the server performing CF and the at least one server performing the PF record the service identifier, and send the server identifier to the billing center via the at least one bearer control layer charging information collecting function entity;
correlating, by the billing center, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier, and correlating the CDRs generated by the bear control layer entities; or, correlating, by the billing center, the CDRs generated by the bear control layer entities, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier.

6. The method according to any one of Claims 1 to 5, wherein sending the service identifier to the charging system comprises:

sending the at least CDR that carries the service identifier to the charging system.

7. The method according to any one of Claims 1 to 5, wherein in the application or service, one user is established at least one session, and one CDR corresponds to one session of one user; and
the at least CDR correlated for the application or service based on the service identifier comprises: CDRs corresponding to a plurality of sessions of one user in the application or service, or CDRs corresponding to a plurality of sessions of a part of or all users in the application or service.

8. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the charging information collecting function entity comprises: at least one AS charging information collecting function entity which respectively corresponds to multiple sub-service server providing multiple sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service and multiple sub-service identifiers of the multiple sub-services;
respectively receiving, by the multiple sub-service servers, the multi-service identifier and the respective sub-service identifier from the service control function entity, and sending the multi-service identifier and the respective sub-service identifier to the billing center via respective AS charging information collecting function entity; and
correlating, the billing center, the CDRs each sub-service server using the respective sub-service identifier, and correlating, the CDRs generated by all sub-service servers using the multi-service identifier.

9. The method according to Claim 8, wherein the charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple sub-service servers are adapted to respectively bear the bear control layers;
recording, by the bear control layer entities that respectively correspond to the multiple sub-service servers, the corresponding sub-service identifier and the multi-service identifier, and sending the corresponding sub-service identifier and the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities;
correlating, by the billing center, the CDRs generated by each bear control layer entity based on the corresponding sub-service identifier, and correlating CDRs generated by all the bear control layer entities based on the multi-service identifier.

10. The method according to Claim 8 or 9, wherein sending the multi-service identifier and the sub-service identifier comprises:

sending the CDRs that carry the multi-service identifier and the sub-service identifier.

11. The method according to Claim 8 or 9, wherein the multi-service identifier is identical to one of the sub-service identifiers, or is not identical to any one of the sub-service identifiers.

12. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service; the charging information collecting function comprises: at least one AS charging information collecting function entity that respectively correspond to the multiple sub-service servers;
receiving, by the multiple sub-service servers, the multi-service identifier from the service charging information collecting function entity, and respectively sending the multi-service identifier to the billing center via respective AS charging information collecting function entity; correlating, by the billing center, the CDRs generated by the multiple sub-service servers based on the multi-service identifier.

13. The method according to Claim 12, wherein the

charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple subservice servers are adapted to respectively bear the bear control layers;
the method further comprises:

recording, by the bear control layer entities that respectively correspond to the multiple subservice servers, the multi-service identifier, and sending the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities; correlating, by the billing center, the CDRs generated by the bear control layer entities based on the the multi-service identifier.

14. The method according to Claim 12 or 13, wherein sending the multi-service identifier comprises: sending the CDRs that carry the multi-service identifier.

15. A system for charging correlation for an application or service, comprising:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate at least one Charging Data Records CDR generated for the application or service based on the service identifier.

16. The system according to Claim 15, wherein the charging system comprises:

a charging information collecting function entity, adapted to receive the service identifier assigned by the service control function entity and collect the at least one CDR; and
a billing center, adapted to correlate the at least one CDR based on the service identifier received from the charging information collecting function entity.

17. The system according to Claim 16, wherein the service control function comprises an Application Server AS adapted to generate at least one CDR for the application or service; and the system further comprises a bearer control layer entity, adapted to record the service identifier and generate at least one CDR for the application or service.
wherein the charging information collecting function entity comprises:

an AS-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the service control function entity;
a bearer control layer-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the bearer control layer entity;

wherein
the billing center is further adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity based on the service identifier, and correlate the at least one CDR from the AS-charging information collecting function entity based on the service identifier respectively, or adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity with the at least one CDR from the AS-charging information collecting function entity based on the service identifier.

18. The system according to Claim 17, wherein the application or service is a multi-party service and the service control function entity is a server performing Controlling Function CF,
the system further comprises at least one server performing Participating Function PF,
wherein the bearer control layer entity comprises a bearer control layer entity corresponding to the server performing CF and at least one bearer control layer entity corresponding to the at least one server performing PF; the bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF and the bearer control layer entity corresponding to the server performing PF is adapted to bear the server performing PF;
the AS-charging information collecting function entity comprises an AS-charging information collecting function entity corresponding to the server performing CF and at least one AS-charging information collecting function corresponding to the at least one server performing PF;
the bearer control layer-charging information collecting function comprises a bearer control layer-charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF and at least a bearer control layer-charging information collecting function of the bearer control layer entity corresponding to the at least one server performing PF;
the server performing CF is adapted to assign the service identifier, send the service identifier to the at least one server performing PF, generate at least one set of CDR and send the service identifier and the CDRs to the AS-charging information collecting function entity of the server performing CF;
each server performing PF is adapted to record the service identifier, generate at least one set of CDR

and send the at least one set of CDR and the service identifier to the AS-charging information collecting function entity of the server performing PF;
the bearer control layer entity corresponding to the server performing CF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
each bearer control layer entity corresponding to a server performing PF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center.

19. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the plurality of sub-services respectively; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities of respective sub-service servers;
the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities of the bearer control layer entities corresponding to respective sub-service servers;
the service control function entity is further adapted to assign sub-service identifiers for the sub-services and send the service identifier and the sub-service identifiers to the sub-service servers;
each sub-service server is adapted to record the service identifier and the sub-service identifiers from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to the sub-service server is adapted to record the service identifier and the sub-service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center;
the bearer control layer-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center; and
the billing center is further adapted to correlate CDRs of each sub-service according to the sub-service identifier corresponding to the sub-service, and correlate CDRs of the plurality of sub-services according to the service identifier.

20. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the sub-services; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities corresponding to the sub-service servers; the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities corresponding to the bearer control layer entities corresponding to the sub-service servers;
the service control function entity is adapted to send the service identifier to the sub-service servers;
the sub-service server is adapted to record the service identifier from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the at least one set of CDRs and the service identifier to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to a sub-service server is adapted to record the service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
an AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center;
a bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the billing center is adapted to correlate the CDRs of the sub-services based on the service identifier.

21. A billing center, comprising:

a first module, adapted to receive a service identifier assigned for an application or service and Charging Data Records CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

22. The billing center according to Claim 21, wherein the CDRs received by the first module comprise CDRs generated by an Application Server AS and CDRs generated by a bearer control layer entity; and
the second module is adapted to correlate the CDRs generated by the AS based on the service identifier and correlate the CDRs generated by the bearer control layer entity based on the service identifier respectively, or adapted to correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity based on the service identifier.

23. The billing center according to any of Claim 21 or 22, wherein the application or service comprises at least one session and each set of the CDRs identified by ICID corresponds to one session; and
the second module is adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of one user in the application or service based on the service identifier, or adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of a part of or all users in the application or service based on the service identifier.

24. A apparatus for generating a charging data record, comprising:

a first module, adapted to receive a service identifier assigned for an application or service; and
a second module, adapted to generate Charging Data Records, CDRs, carrying the service identifier from the first module for the application or service.

25. The apparatus according to Claim 24, wherein the apparatus is an AS or a bearer control layer entity.

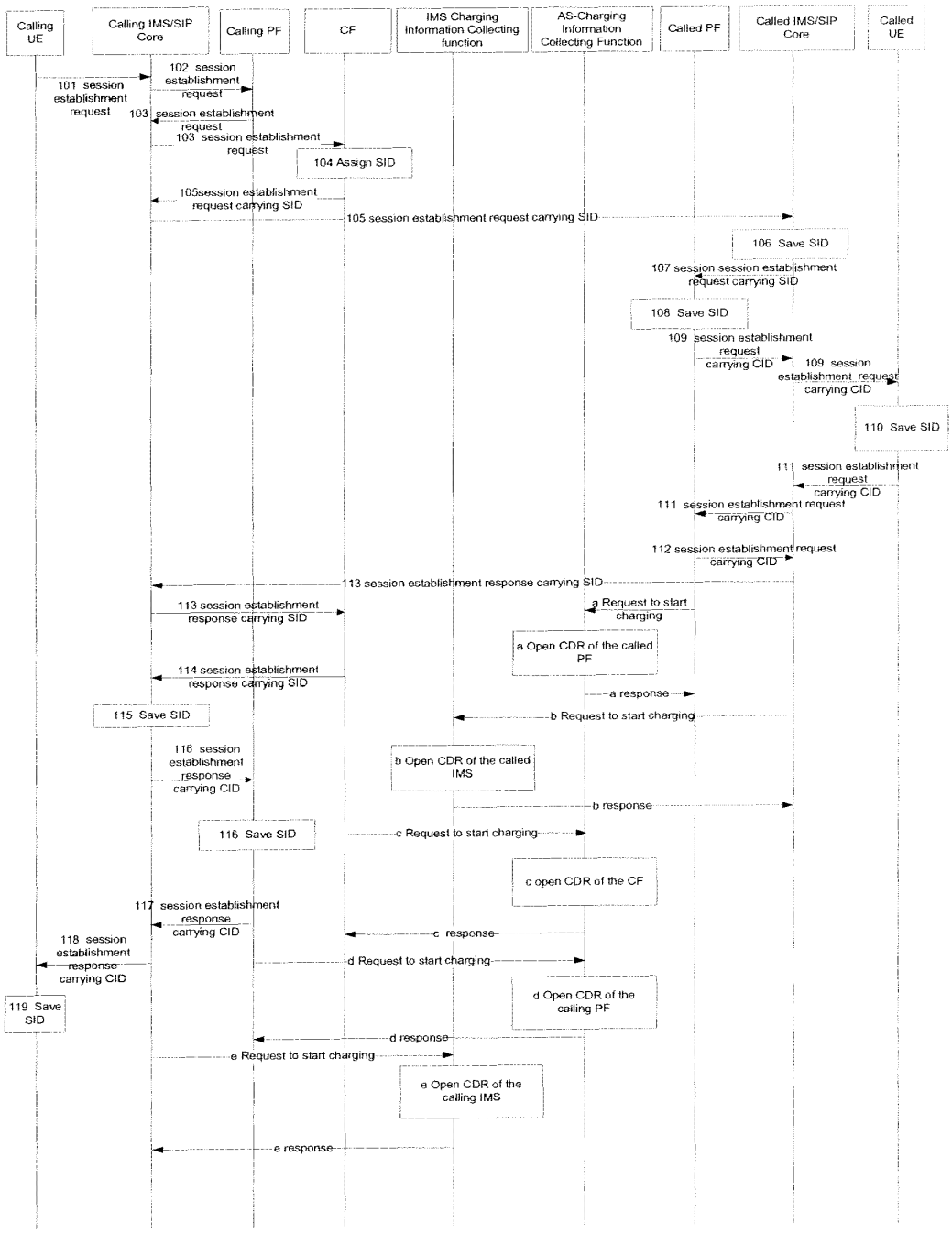

Calling UE
Calling IMS/SIP Core
Calling PF
CF
IMS Charging Information Collecting function
AS-Charging Information Collecting Function
Called PF
Called IMS/SIP Core
Called UE
101 session establishment request
102 session establishment request
103 session establishment request
103 session establishment request
104 Assign SID
105session establishment request carrying SID
105 session establishment request carrying SID
106 Save SID
107 session session establishment request carrying SID
108 Save SID
109 session establishment request carrying CID
109 session establishment request carrying CID
110 Save SID
111 session establishment request carrying CID
111 session establishment request carrying CID
112 session establishment request carrying CID
113 session establishment response carrying SID
113 session establishment response carrying SID
a Request to start charging
a Open CDR of the called PF
114 session establishment response carrying SID
a response
115 Save SID
b Request to start charging
116 session establishment response carrying CID
b Open CDR of the called IMS
b response
116 Save SID
c Request to start charging
c open CDR of the CF
117 session establishment response carrying CID
c response
118 session establishment response carrying CID
d Request to start charging
d Open CDR of the calling PF
119 Save SID
d response
e Request to start charging
e Open CDR of the calling IMS
e response

Fig. 1

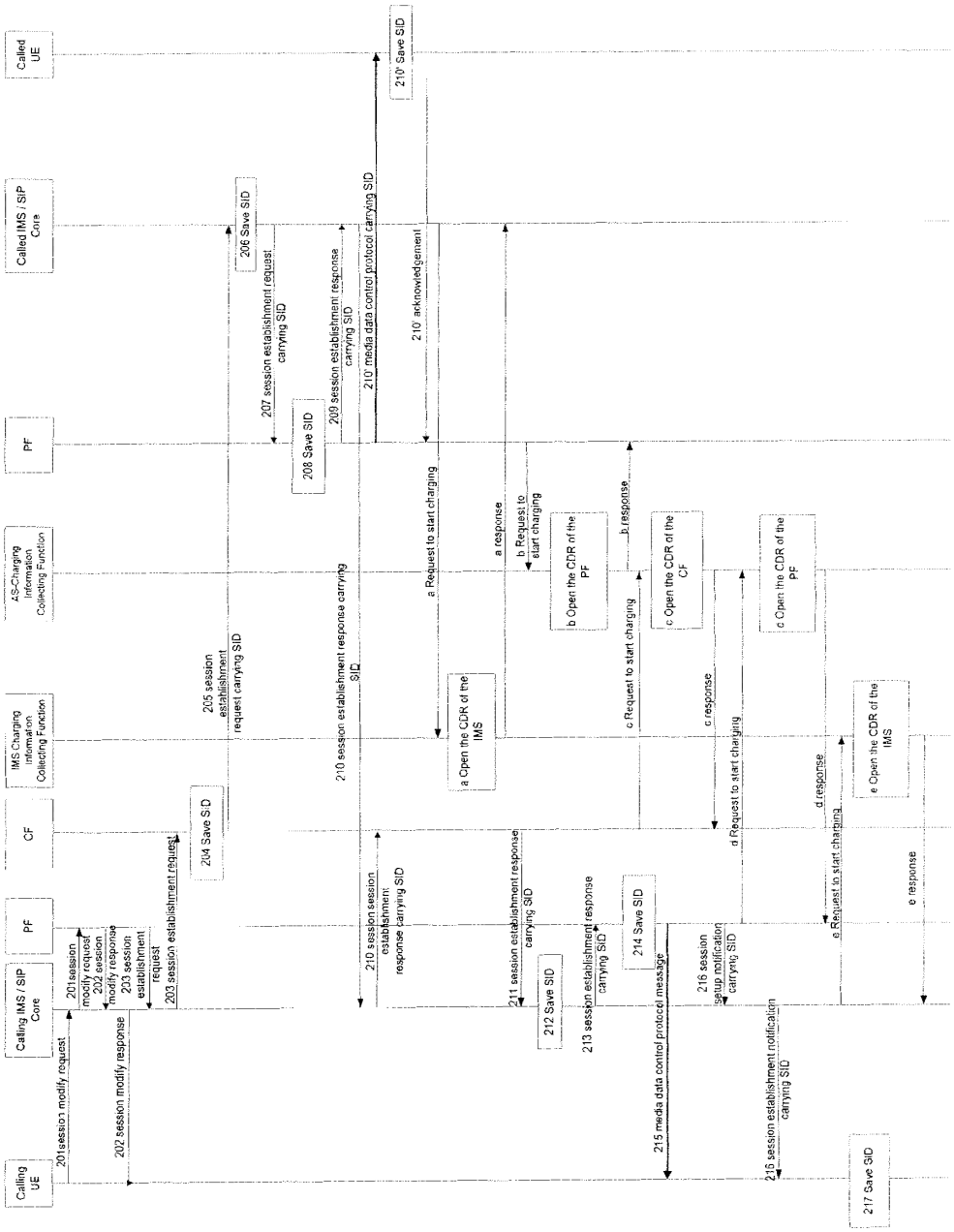

Calling UE
Calling IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
PF
Called IMS / SIP Core
Called UE
201 session modify request
202 session modify response
201 session modify request
202 session modify response
203 session establishment request
203 session establishment request
204 Save SID
205 session establishment request carrying SID
206 Save SID
207 session establishment request carrying SID
208 Save SID
209 session establishment response carrying SID
210' media data control protocol carrying SID
210' acknowledgement
210' Save SID
210 session session establishment response carrying SID
a Request to start charging
a response
b Request to start charging
b response
a Open the CDR of the IMS
b Open the CDR of the PF
c Request to start charging
c response
c Open the CDR of the CF
c Open the CDR of the PF
211 session establishment response carrying SID
212 Save SID
213 session establishment response carrying SID
214 Save SID
d Request to start charging
d response
216 session setup notification carrying SID
e Request to start charging
e response
e Open the CDR of the IMS
215 media data control protocol message
216 session establishment notification carrying SID
217 Save SID

Fig. 2

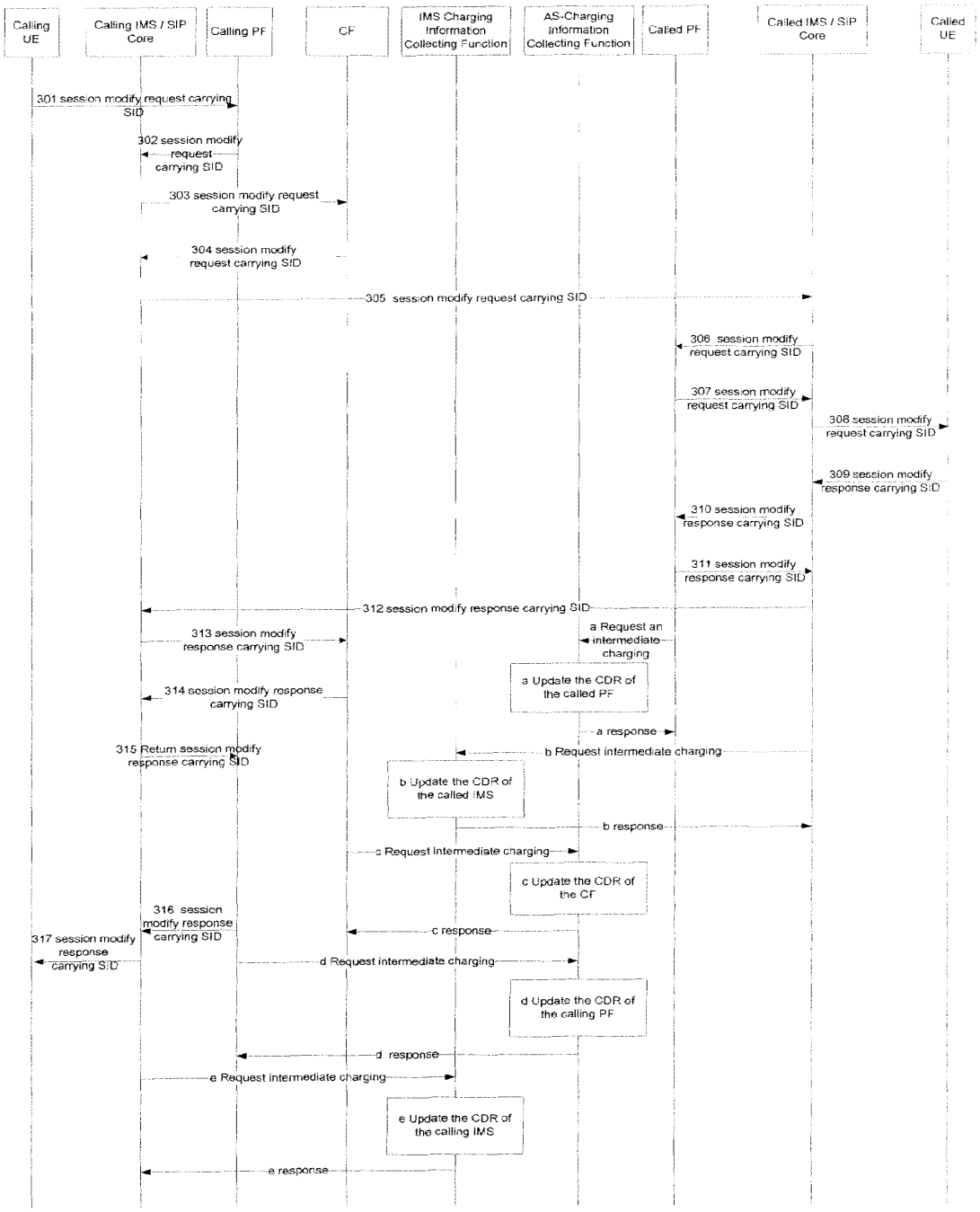

Calling UE
Calling IMS / SIP Core
Calling PF
CF
IMS Charging Information Collecting Function
AS-Charging information Collecting Function
Called PF
Called IMS / SIP Core
Called UE
301 session modify request carrying SID
302 session modify request carrying SID
303 session modify request carrying SID
304 session modify request carrying SID
305 session modify request carrying SID
306 session modify request carrying SID
307 session modify request carrying SID
308 session modify request carrying SID
309 session modify response carrying SID
310 session modify response carrying SID
311 session modify response carrying SID
312 session modify response carrying SID
313 session modify response carrying SID
a Request an intermediate charging
a Update the CDR of the called PF
314 session modify response carrying SID
a response
315 Return session modify response carrying SID
b Request intermediate charging
b Update the CDR of the called IMS
b response
c Request intermediate charging
c Update the CDR of the CF
316 session modify response carrying SID
c response
317 session modify response carrying SID
d Request intermediate charging
d Update the CDR of the calling PF
d response
e Request intermediate charging
e Update the CDR of the calling IMS
e response

Fig. 3

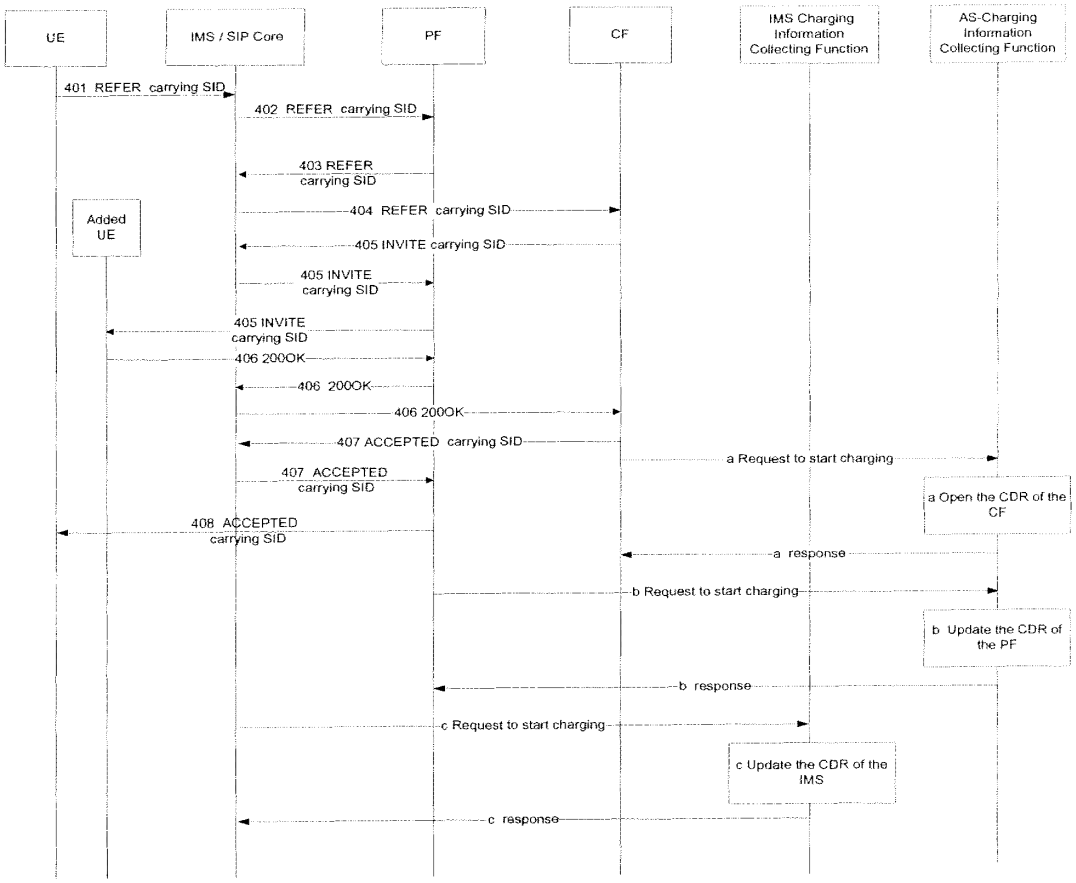

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
401 REFER carrying SID
402 REFER carrying SID
403 REFER carrying SID
404 REFER carrying SID
Added UE
405 INVITE carrying SID
405 INVITE carrying SID
405 INVITE carrying SID
406 200OK
406 200OK
406 200OK
407 ACCEPTED carrying SID
a Request to start charging
407 ACCEPTED carrying SID
a Open the CDR of the CF
408 ACCEPTED carrying SID
a response
b Request to start charging
b Update the CDR of the PF
b response
c Request to start charging
c Update the CDR of the IMS
c response

Fig. 4

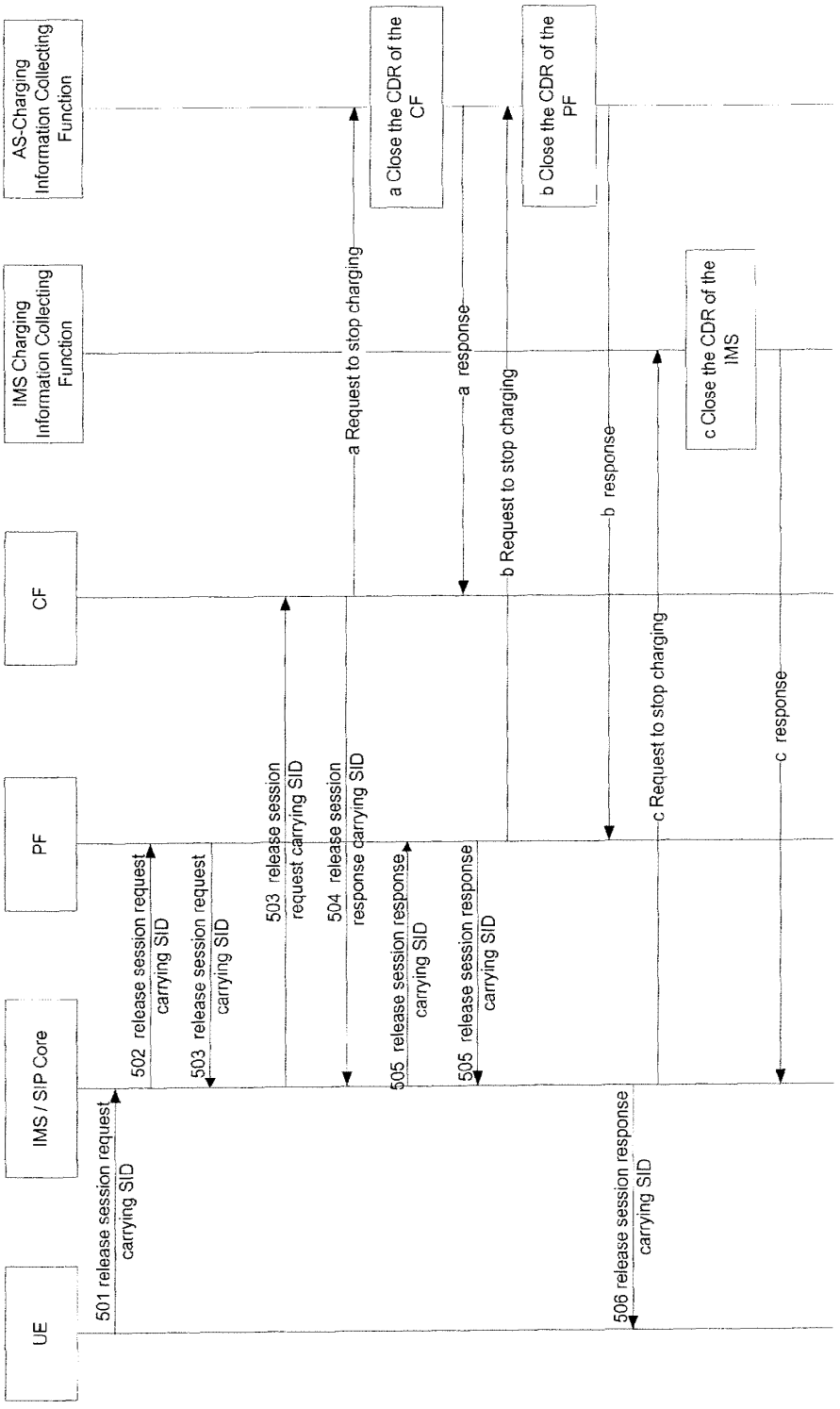

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
501 release session request carrying SID
502 release session request carrying SID
503 release session request carrying SID
503 release session request carrying SID
504 release session response carrying SID
505 release session response carrying SID
505 release session response carrying SID
a Request to stop charging
a response
a Close the CDR of the CF
b Request to stop charging
b response
b Close the CDR of the PF
c Request to stop charging
c response
c Close the CDR of the IMS
506 release session response carrying SID

Fig. 5

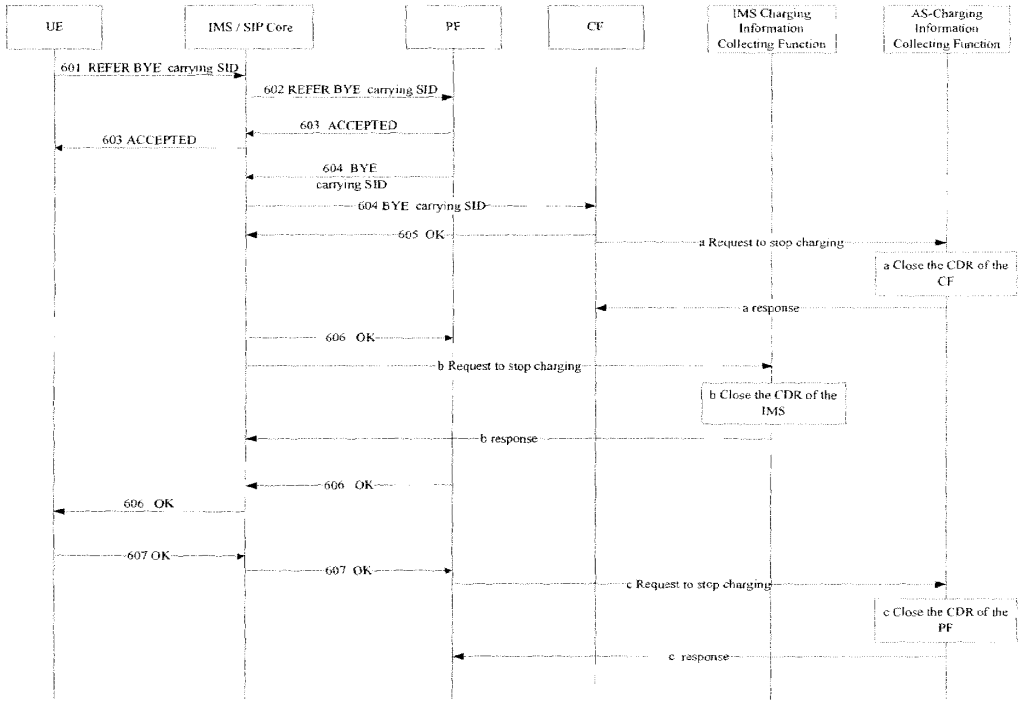

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
601 REFER BYE carrying SID
602 REFER BYE carrying SID
603 ACCEPTED
603 ACCEPTED
604 BYE carrying SID
604 BYE carrying SID
605 OK
a Request to stop charging
a Close the CDR of the CF
a response
606 OK
b Request to stop charging
b Close the CDR of the IMS
b response
606 OK
606 OK
607 OK
607 OK
c Request to stop charging
c Close the CDR of the PF
c response

Fig. 6

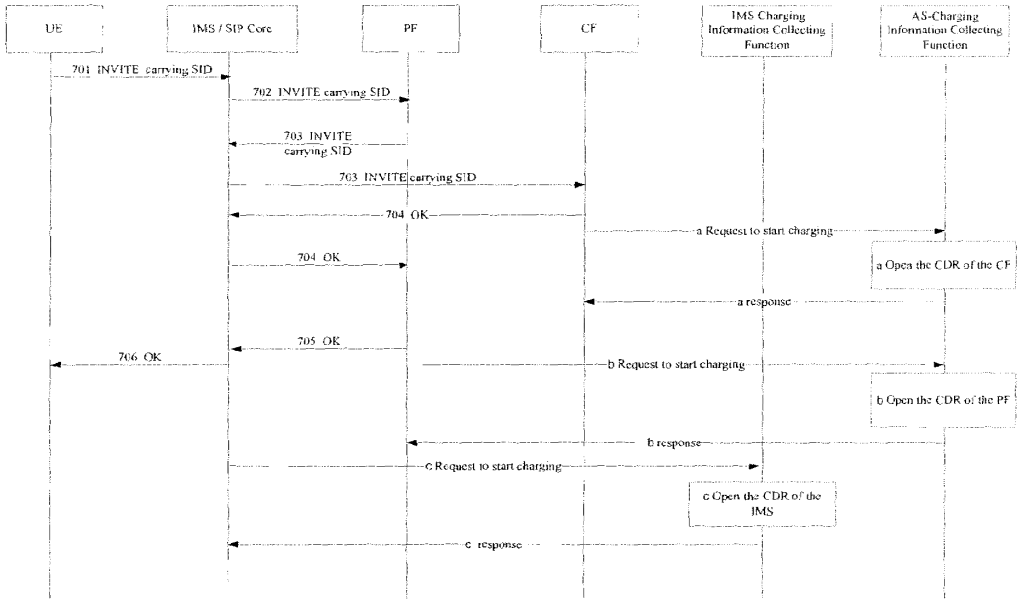

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
701 INVITE carrying SID
702 INVITE carrying SID
703 INVITE carrying SID
703 INVITE carrying SID
704 OK
a Request to start charging
704 OK
a Open the CDR of the CF
a response
705 OK
706 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 7

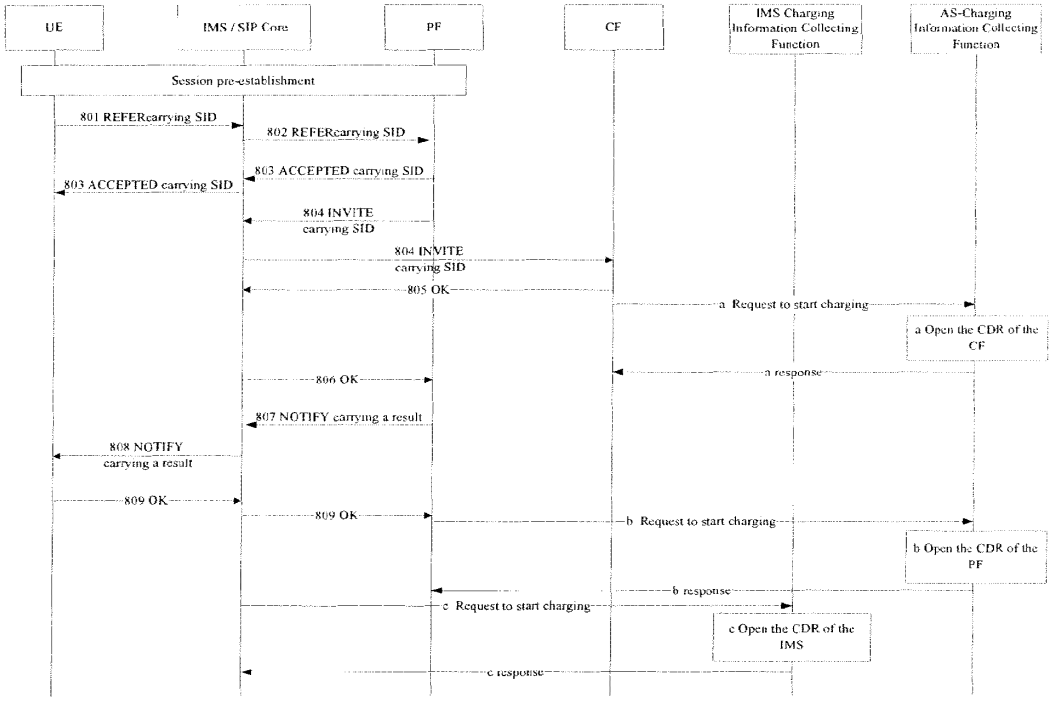

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
Session pre-establishment
801 REFERcarrying SID
802 REFERcarrying SID
803 ACCEPTED carrying SID
803 ACCEPTED carrying SID
804 INVITE carrying SID
804 INVITE carrying SID
805 OK
a Request to start charging
a Open the CDR of the CF
a response
806 OK
807 NOTIFY carrying a result
808 NOTIFY carrying a result
809 OK
809 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 8

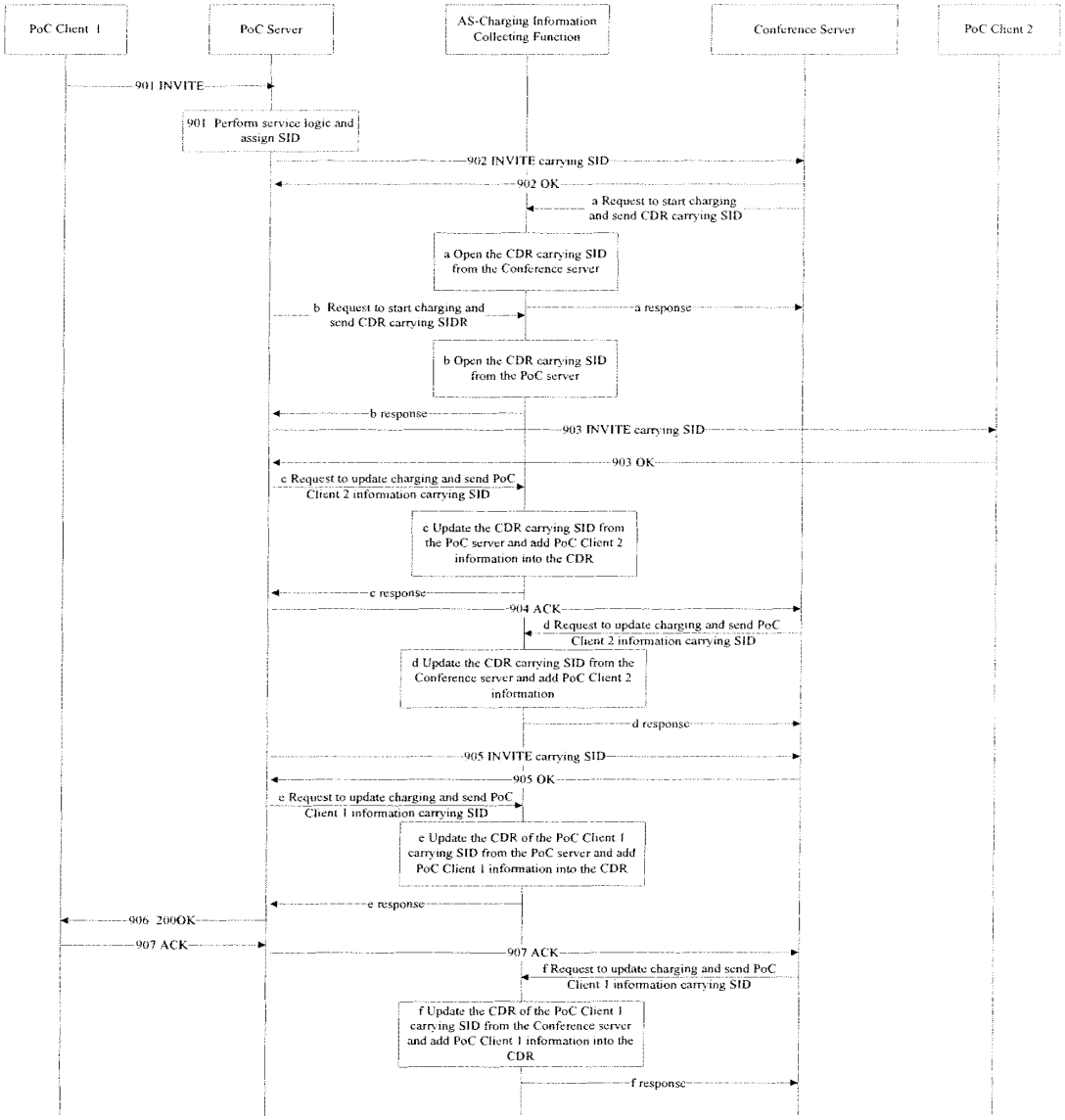

PoC Client 1
PoC Server
AS-Charging Information Collecting Function
Conference Server
PoC Client 2
901 INVITE
901 Perform service logic and assign SID
902 INVITE carrying SID
902 OK
a Request to start charging and send CDR carrying SID
a Open the CDR carrying SID from the Conference server
b Request to start charging and send CDR carrying SIDR
a response
b Open the CDR carrying SID from the PoC server
b response
903 INVITE carrying SID
903 OK
c Request to update charging and send PoC Client 2 information carrying SID
c Update the CDR carrying SID from the PoC server and add PoC Client 2 information into the CDR
c response
904 ACK
d Request to update charging and send PoC Client 2 information carrying SID
d Update the CDR carrying SID from the Conference server and add PoC Client 2 information
d response
905 INVITE carrying SID
905 OK
e Request to update charging and send PoC Client 1 information carrying SID
e Update the CDR of the PoC Client 1 carrying SID from the PoC server and add PoC Client 1 information into the CDR
e response
906 200OK
907 ACK
907 ACK
f Request to update charging and send PoC Client 1 information carrying SID
f Update the CDR of the PoC Client 1 carrying SID from the Conference server and add PoC Client 1 information into the CDR
f response

Fig. 9

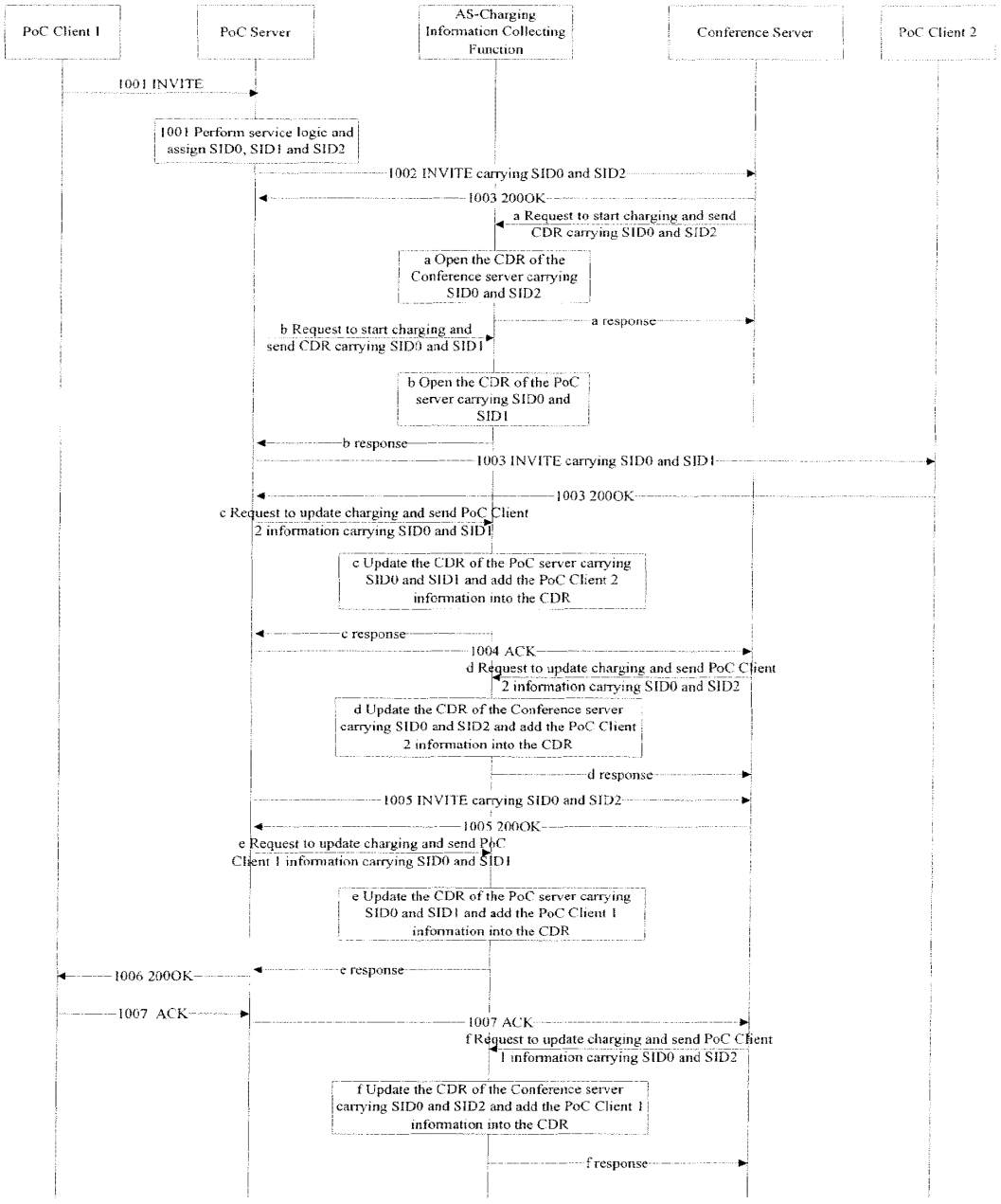

PoC Client 1
PoC Server
AS-Charging Information Collecting Function
Conference Server
PoC Client 2
1001 INVITE
1001 Perform service logic and assign SID0, SID1 and SID2
1002 INVITE carrying SID0 and SID2
1003 200OK
a Request to start charging and send CDR carrying SID0 and SID2
a Open the CDR of the Conference server carrying SID0 and SID2
a response
b Request to start charging and send CDR carrying SID0 and SID1
b Open the CDR of the PoC server carrying SID0 and SID1
b response
1003 INVITE carrying SID0 and SID1
1003 200OK
c Request to update charging and send PoC Client 2 information carrying SID0 and SID1
c Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 2 information into the CDR
c response
1004 ACK
d Request to update charging and send PoC Client 2 information carrying SID0 and SID2
d Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 2 information into the CDR
d response
1005 INVITE carrying SID0 and SID2
1005 200OK
e Request to update charging and send PoC Client 1 information carrying SID0 and SID1
e Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 1 information into the CDR
e response
1006 200OK
1007 ACK
1007 ACK
f Request to update charging and send PoC Client 1 information carrying SID0 and SID2
f Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 1 information into the CDR
f response

Fig. 10

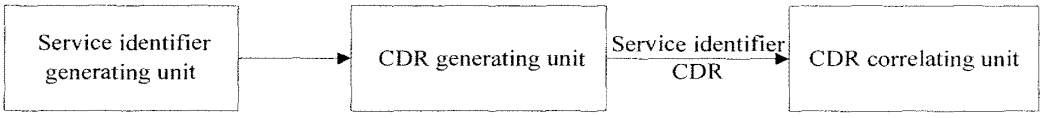

Service identifier generating unit
CDR generating unit
Service identifier
CDR
CDR correlating unit

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001048

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC H04L 12/-; H04M 15/-; G06Q10/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT WPI EPODOC PAJ: service, charg+, money, bill, fee, cost, associat+, relat+, corresponding, flag, ID, identification, indicator, mark, identifier, identity, distribut+, assign, communicat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1267414A (NOKIA NETWORKS OY [FI]) 20 September 2000(20.09.2000) see claims 1,7and figure 3A	1-2, 15-16, 21, 24-25
A		3-14, 17-20, 22-23
A	CN1643888A (ERICSSON TELEFON AB L M [SE]) 20 July 2005(20.07.2005) see whole document	1-25
A	US2004255025A1 (RICAGNI GIUSEPPE [IT]) 16 December 2004(16.12.2004) see whole document	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 June 2007 (26.06.2007)	**12 Jul. 2007 (12.07.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZHAO, Weihua Telephone No. (86-10)62085024

Form PCT/ISA /210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/001048

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1267414A	20.09.2000	FI981031A	15.01.1999
		WO9907108A2	11.02.1999
		AU8443398A	22.02.1999
		NO20000170A	13.03.2000
		EP1005737A2	07.06.2000
		US6240091B1	29.05.2001
		JP2001512926T	28.08.2001
CN1643888A	20.07.2005	EP1345402A1	17.09.2003
		WO03077528A1	18.09.2003
		AU2003210373A	22.09.2003
		EP1483893A1	08.12.2004
		JP2005520405T	07.07.2005
		US2005176404A1	11.08.2005
		AT311719T	15.12.2005
		DE60302559D	05.01.2006
		ES2252682T	16.05.2006
US2004255025A1	16.12.2004	None	

Form PCT/ISA /210 (patent family annex) (April 2007)

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) RALEP032C1
Application Number 14/082,040	Filed November 15, 2013
For Device-Assisted Services for Protecting Network Capacity	
Art Unit 3687	Examiner Rudy, Andrew J.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 505876.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 40013.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James E. Harris/	December 1, 2016
Signature	Date
James E. Harris	903-201-6212
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 1.11 and 1.14. This collection is estimated to take 6 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: Mail Stop PCT, 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 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.

Electronic Acknowledgement Receipt	
EFS ID:	27671387
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
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:	RALEP032C1
Receipt Date:	01-DEC-2016
Filing Date:	15-NOV-2013
Time Stamp:	19:02:16
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	Non Patent Literature	3055.pdf	10370496 db66223e77b303b72c707b13a3bf1588e151bc42	no	20

Warnings:

Information:					
2	Non Patent Literature	3056.pdf	24448035 1be0315565d698a68e100c214709404b6b456701	no	85
Warnings:					
Information:					
3	Non Patent Literature	3057.pdf	1369098 4c887fb7b9fe8033365febea8b25f1275100a8cc	no	6
Warnings:					
Information:					
4	Non Patent Literature	3058.pdf	201178 0bdd69f18a3fd0292aa6cfb96076e8b9ccf310d5	no	4
Warnings:					
Information:					
5	Non Patent Literature	3059.pdf	984650 b3abbccb529e99d2c6635add88044e98852f41b7	no	20
Warnings:					
Information:					
6	Non Patent Literature	3060.pdf	2689325 2571b02a20421247b52538c8c218f2e3c8e6627f	no	336
Warnings:					
Information:					
7	Non Patent Literature	3061.pdf	868379 fd6eb4b7c7f13d4a778a1c80b64403253c0ae145	no	6
Warnings:					
Information:					
8	Non Patent Literature	3062.pdf	369346 69ebce04c86da14ea2d68c910afcd28d7fdf7e6d	no	2
Warnings:					
Information:					

9	Non Patent Literature	3063_Muntermann.pdf	400365 d732f8457b3d7b48773e6de195057acc9b18e201	no	36
Warnings:					
Information:					
10	Non Patent Literature	3064.pdf	944999 f03e4f3963258080c50536b168540d38a4b9eced	no	7
Warnings:					
Information:					
11	Non Patent Literature	3065_Fujitsu.pdf	158718 eee0e740dbe4d1b5db62cc52983988913c995e60	no	13
Warnings:					
Information:					
12	Non Patent Literature	3066.pdf	541057 5087e543fd3bcb9a11a377ef5db4f1c2ca88e720	no	15
Warnings:					
Information:					
13	Non Patent Literature	3067.pdf	2952523 18992a26a8917fcacb584769c943714abeee008d	no	14
Warnings:					
Information:					
14	Non Patent Literature	3068.pdf	749607 9e51f82ae6f112f5983929992b1d151a477fe5f9	no	5
Warnings:					
Information:					
15	Non Patent Literature	3069_OMA.pdf	469668 ea0fe39f7877344efbc29526eb097201b8731e98	no	21
Warnings:					
Information:					
			Total Files Size (in bytes):	47517444	

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.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 06/01/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
06/01/2016	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. 14/082,040	Applicant(s) RALEIGH ET AL.	
	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 *15 November 2013*.

☐ 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) *1-23* 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) *1-23* 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. Claims 1-23 are pending. As noted from the November 27, 2015 communication, the November 17, 2015 Restriction requirement has been vacated.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 1-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed towards non-statutory subject matter because the claim(s) as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea. The claim(s) is/are directed to a system/method which are clearly a machine/process under 35 USC 101 and thus are patent eligible concepts. However, one must further analyze the eligible concepts and determine whether the concepts, in this case, improve the functioning of the computer itself. Applicant's claim(s) is/are directed to the abstract idea of an apparatus that monitor network service usage activity. The additional elements or combination of

elements in the claim(s) amount(s) to no more than using a general purpose computing system, i.e. a processor and memory, to perform generic computer functions, e.g. provide instructions. It is noted that the method claim 22 requires no technology in addition to the recitations claimed. Viewed as a whole, these additional claim elements do not provide meaningful limitation(s) to transform the using computer technology, i.e. a processor and memory, to provide a common abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Therefore, the claims(s) are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. See, Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014).

The technology recited from the claims is deemed common knowledge technology and appears to add no additional technological improvement to the underlying invention. Viewed as a whole, these additional claim elements do not appear to provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Applicant's disclosure does not appear to lend support to anything other than the technology, e.g. a processor, memory, was commonly known. Therefore, the claims(s) are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. See, Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014).

Claim Rejections - 35 USC § 103

5. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-23 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Rados et al., US 8,484,568.

Rados discloses, e.g. Figs. 1-10 and related text, a network communication system comprising: a device e.g. 110 (see claim 18), memory, e.g. 210, 330, a processor, e.g. 200, the device configured to monitor e.g. Figs. 9, 10, the network for service usage activity, a traffic classification information, e.g. 720, and policy, e.g. 150.

Rados does not specifically disclose memory coupled to the processor and configured to provide the processor with instructions input of a user, nor a router.

Official Notice is taken that memory coupled to a processor and configured to provide the processor with instructions input of a user and a router has been common knowledge in the data monitoring art.

To have provided memory coupled to the processor and configured to provide the processor with instructions input of a user for Rados would have been obvious to one of ordinary skill in the art in view of Official Notice. Motivation for providing such would have been to incorporate common knowledge data aggregation used with telecommunication devices used in the data monitoring art.

It is noted Applicant's intended use claim language, e.g. claim 1, line 2, "configured to" does not further limit the positively recited claim language. As is, the claims that contain such language is deemed to be obvious variants of what Rados discloses and is configured to accomplish various policy intiatives for one of ordinary skill in the art in view of common knowledge.

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

8. Applicant's fourteen information disclosure statements (IDS's) have been reviewed. Note the attached IDS's.

9. 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. 14/082,040	Applicant(s)/Patent Under Reexamination RALEIGH ET AL.	
	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	CPC Classification	US Classification
*	A	US-8,634,821 B2	01-2014	Raleigh; Gregory G.	H04L41/0806	455/419
*	B	US-8,503,455 B2	08-2013	Heikens; Heico	H04L47/10	370/395.21
*	C	US-8,484,568 B2	07-2013	Rados; Steven R.	H04L41/5032	715/745
*	D	US-8,023,425 B2	09-2011	Raleigh; Gregory G.	G06Q10/06375	370/252
*	E	US-7,987,496 B2	07-2011	Bryce; Duncan G.	H04L63/0227	726/1
*	F	US-7,849,477 B2	12-2010	Cristofalo; Michael	G06Q30/00	725/105
*	G	US-7,644,151 B2	01-2010	Jerrim; John	G06F21/552	709/212
*	H	US-7,457,870 B1	11-2008	Lownsbrough; Derek Leigh	H04L41/5058	709/217
*	I	US-7,395,244 B1	07-2008	Kingsford; Bryan	G06Q10/06	705/52
*	J	US-6,947,985 B2	09-2005	Hegli; Ronald Bjorn	H04L63/10	709/224
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC 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	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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		2012-09-26	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	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	229	7565141		2009-06-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2010-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	8385896		2013-02-26	Proctor Jr., James A. 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

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]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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)	☐
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	☐
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	☐
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	☐
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	☐
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	☐

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	05/26/2016

*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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	Raleigh, Gregory G.
Attorney Docket Number	RALEP032C1

U.S.PATENTS

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	5774532	A	1998-06-30	Gottlieb et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20040225898	A	2004-11-11	Frost, D. et al.	
	2	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	3	20060114832	A	2006-06-01	Hamilton et al.	
	4	20060156398	A	2006-07-13	Ross et al.	
	5	20060173959	A	2006-08-03	Mckelvie et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

	6	20070033194	A	2007-02-08	Srinivas et al.	
	7	20080070550	A	2008-03-20	Hose, David Alan	
	8	20080201266	A	2008-08-21	Chua et al.	
	9	20100284327	A	2010-11-11	Miklos, Gyorgy	

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

FOREIGN PATENT DOCUMENTS

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]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS

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	"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	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*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.

EFS Web 2.1.17

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	5633868	A	1997-05-27	Baldwin et al.	
	2	6061571	A	2000-05-09	Tamura, Hideo	
	3	6157636	A	2000-12-05	Voit et al.	
	4	6725256	B1	2004-04-20	Albal et al.	
	5	6751296	B1	2004-06-15	Albal et al.	
	6	6792461	B1	2004-09-14	Hericourt, Olivier	
	7	6934751	B2	2005-08-23	Jayapalan et al.	
	8	7027055	B2	2006-04-11	Anderson 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7043225	B1	2006-05-09	Patel et al.	
	10	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	11	7174156	B1	2007-02-06	Mangal, Manish	
	12	7636626	B2	2009-12-22	Oesterling et al.	
	13	7680086	B2	2010-03-16	Eglin	
	14	7720206	B2	2010-05-18	Devolites et al.	
	15	7765294	B2	2010-07-27	Edwards et al.	
	16	7843831	B2	2010-11-30	Morrill et al.	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8131858	B2	2012-03-06	Agulnik et al.	
	19	8160056	B2	2012-04-17	Van der Merwe 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	8180333	B1	2012-05-15	Wells et al.	
	21	8223655	B2	2012-07-17	Heinz et al.	
	22	8315198	B2	2012-11-20	Corneille et al.	
	23	8340678	B1	2012-12-25	Pandey, Vinod	
	24	8385199	B1	2013-02-26	Coward et al.	
	25	8520595	B2	2013-08-27	Yadav et al.	
	26	8523547	B2	2013-09-03	Pekrul, Merton W.	
	27	8621056	B2	2013-12-31	Coussemaeker et al.	
	28	8875042	B2	2014-10-28	LeJeune et al.	
	29	9135037	B1	2015-09-15	Petrescu-Prahova et al.	
	30	9172553	B2	2015-10-27	Dawes 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	9177455	B2	2015-11-03	Remer, David M.	

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	20030028623	A1	2003-02-06	Hennessey et al.	
	2	20050060525	A1	2005-03-17	Schwartz et al.	
	3	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	4	20070061800	A1	2007-03-15	Cheng et al.	
	5	20070255769	A1	2007-11-01	Agrawal et al.	
	6	20070299965	A1	2007-12-27	Nieh et al.	
	7	20080066181	A1	2008-03-13	Haveson et al.	
	8	20080126287	A1	2008-05-29	Cox 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	20080212751	A1	2008-09-04	Chung, Simon	
	10	20090203352	A1	2009-08-13	Fordon et al.	
	11	20100041365	A1	2010-02-18	Lott et al.	
	12	20100121744	A1	2010-05-13	Belz et al.	
	13	20140073291	A1	2014-03-13	Hildner 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	2002045315	WO	A2	2002-06-06	Micromuse		
	2	2009008817	WO	A1	2009-01-15	Ericsson		

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]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	05/26/2016

*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./

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	5131020	A	1992-07-14	Liebesny et al.	
	2	5325532	A	1994-06-28	Crosswy et al.	
	3	6640334	B	2003-10-28	Rasmussen, John H.	
	4	7409447	B	2008-08-05	Assadzadeh, Alireza	
	5	7614051	B	2009-11-03	Glaum et al.	
	6	7668612	B	2010-02-23	Okkonen, Harri	
	7	7756056	B2	2010-07-13	Kim et al.	
	8	8131281	B1	2012-03-06	Hildner 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8160598	B2	2012-04-17	Savoor, Raghvendra	
	10	8223741	B	2012-07-17	Bartlett et al.	
	11	8370483	B	2013-02-05	Choong Jason et al.	
	12	8375136	B2	2013-02-12	Roman et al.	
	13	8396458	B	2013-03-12	Raleigh, Gregory G.	
	14	8645518	B	2014-02-04	David, Scott L.	
	15	8670334	B	2014-03-11	Keohane et al.	
	16	8676925	B	2014-03-18	Liu et al.	
	17	8693323		2014-04-08	McDysan, David E.	
	18	8725899	B	2014-05-13	Short 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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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	20040039792	A1	2004-02-26	Nakanishi, Tomoaki	
	2	20040137890	A1	2004-07-15	Kalke, Catherine	
	3	20040243992	A	2004-12-02	Gustafson et al.	
	4	20050075115	A1	2005-04-07	Corneille et al.	
	5	20050239447	A1	2005-10-27	Holzman et al.	
	6	20070143824	A1	2007-06-21	Shahbazi, Majid	
	7	20070213054	A1	2007-09-13	Han, Seung-Wook	
	8	20070226775	A	2007-09-27	Andreasen et al.	
	9	20070266422	A1	2007-11-15	Germano et al.	
	10	20080032715	A1	2008-02-07	Jia 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20080139210	A	2008-06-12	Gisby et al.		
	12	20080166993	A1	2008-07-10	Gautier et al.		
	13	20080293395	A1	2008-11-27	Mathews et al.		
	14	20090044185	A1	2009-02-12	Krivopaltsev, Eugene		
	15	20090163173	A1	2009-06-25	Williams, Timothy D.		
	16	20090254857	A	2009-10-08	Romine et al.		
	17	20100075666	A1	2010-03-25	Garner, Neil Robert		
	18	20100235329	A	2010-09-16	Koren 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	101127988	CN	A	2008-02-20	ZTE Corporation		☐

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

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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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	05/26/2016

*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	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2013-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-06-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhaguere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8544105		2013-09-24	Mclean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd 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					

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.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.		☐

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	☐
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐

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	05/26/2016

*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.

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	6438575	B1	2002-08-20	Khan et al.	
	2	6578076	B1	2003-06-10	Putzolu, David Matthew	
	3	6697821	B2	2004-02-24	Ziff et al.	
	4	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	5	6982733	B1	2006-01-03	McNally et al.	
	6	6983370	B2	2006-01-03	Eaton et al.	
	7	7084775	B1	2006-08-01	Smith, Michael R.	
	8	7133695	B2	2006-11-07	Beyda, William J.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7222304	B2	2007-05-22	Beaton et al.	
	10	7260382	B1	2007-08-21	Lamb et al.	
	11	7271765	B2	2007-09-18	Stilp et al.	
	12	7318111	B2	2008-01-08	Zhao, Wen	
	13	7561899	B2	2009-07-14	Lee, Changseok	
	14	7627872	B2	2009-12-01	Hebeler et al.	
	15	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	16	7685530	B2	2010-03-23	Sherrard et al.	
	17	7760137	B2	2010-07-20	Martucci et al.	
	18	7843843	B1	2010-11-30	Papp III et al.	
	19	7925778	B1	2011-04-12	Wijnands 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	21	7937450	B2	2011-05-03	Janik, Craig M.	
	22	8010082	B2	2011-08-30	Sutaria et al.	
	23	8019846	B2	2011-09-13	Roelens et al.	
	24	8050705	B2	2011-11-01	Sicher et al.	
	25	8064418	B2	2011-11-22	Maki, Lasse	
	26	8086791	B2	2011-12-27	Caulkins, Jason	
	27	8103285	B2	2012-01-24	Kalhan, Amit	
	28	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
	29	8200200	B1	2012-06-12	Belser et al.	
	30	8229914	B2	2012-07-24	Ramer 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8233433	B2	2012-07-31	Kalhan, Amit	
	32	8249601	B2	2012-08-21	Emberson et al.	
	33	8259692	B2	2012-09-04	Bajko, Gabor	
	34	8406736	B2	2013-03-26	Das et al.	
	35	8489110	B2	2013-07-16	Frank et al.	
	36	8495181	B2	2013-07-23	Venkatraman et al.	
	37	8514927	B2	2013-08-20	Sundararajan et al.	
	38	8522249	B2	2013-08-27	Beaule, Stephane	
	39	8532610	B2	2013-09-10	Manning Cassett et al.	
	40	8571598	B2	2013-10-29	Valavi, John J.	
	41	8631428	B2	2014-01-14	Scott 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8634425	B2	2014-01-21	Gorti et al.	
	43	8701015	B2	2014-04-15	Bonnat, Pierre	
	44	8739035	B2	2014-05-27	Trethewey, Jim	
	45	8804517	B2	2014-08-12	Oerton, Kevin John	
	46	8825109	B2	2014-09-02	Montemurro et al.	
	47	8831561	B2	2014-09-09	Sutaria et al.	
	48	8880047	B2	2014-11-04	Konicek et al.	
	49	8930238	B2	2015-01-06	Coffman et al.	
	50	8949597	B1	2015-02-03	Reeves et al.	
	51	8977284	B2	2015-03-10	Reed, Mark J.	
	52	9014973	B2	2015-04-21	Ruckart, John	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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	20070192460	A1	2007-08-16	Choi et al.	
	5	20070293191	A1	2007-12-20	Mir et al.	
	6	20070294410	A1	2007-12-20	Pandya et al.	
	7	20080050715	A1	2008-02-28	Golczewski et al.	
	8	20080080457	A1	2008-04-03	Cole, Terry L.	
	9	20080282319	A1	2008-11-13	Fontijn 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	10	20090049518	A1	2009-02-19	Roman et al.	
	11	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	12	20100151866	A1	2010-06-17	Karpov et al.	
	13	20100248719	A1	2010-09-30	Scholaert, Hugh	
	14	20110145920	A1	2011-06-16	Mahaffey et al.	
	15	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	101815275A	CN	A	2010-08-25	Yang, Liu		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	4	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐
	5	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	6	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐

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	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	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
	3	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	4	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	☐
	5	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**

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	2	7320029	B2	2008-01-15	Rinne et al.	
	3	7539132	B2	2009-05-26	Werner et al.	
	4	7805606	B2	2010-09-28	Birger et al.	
	5	8175574	B1	2012-05-08	Panda et al.	
	6	8180881	B2	2012-05-15	Seo et al.	
	7	8191124	B2	2012-05-29	Wynn et al.	
	8	8275415	B2	2012-09-25	Huslak, Nicholas S.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8300575	B2	2012-10-30	Willars, Per	
	10	8315593	B2	2012-11-20	Gallant et al.	
	11	8347378	B2	2013-01-01	Merkin et al.	
	12	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	13	8527410	B2	2013-09-03	Markki et al.	
	14	8539561	B2	2013-09-17	Gupta et al.	
	15	8554876	B2	2013-10-08	Winsor, Gerald W.	
	16	8666395	B2	2014-03-04	Silver, Andrew	
	17	8391834	B2	2013-03-05	Raleigh, Gregory G.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	2	20040170191	A	2004-09-02	Guo et al.	
	3	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	4	20050186948	A	2005-08-25	Gallagher et al.	
	5	20070147317	A	2007-06-28	Smith et al.	
	6	20080025230	A	2008-01-31	Patel et al.	
	7	20080056273	A	2008-03-06	Pelletier et al.	
	8	20080270212	A	2008-10-30	Blight et al.	
	9	20100030890	A	2010-02-04	Dutta et al.	
	10	20110110309	A	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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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	1310401	CN	A	2001-08-29	Wang, Di Xing		☐
	2	2466831	EP	A1	2012-06-20	Openet Telecom Ltd. - Mcnamee et al.		☐
	3	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	4	1999027723	WO	A1	1999-06-03	Telefonaktiebolaget LM Ericsson		☐

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	"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	☐
	2	"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	05/26/2016

*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.

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	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	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	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. 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							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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	05/26/2016

*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.

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	6119933	A	2000-09-19	Wong et al.	
	2	7149229	B1	2006-12-12	Leung, Kent K.	
	3	7242668	B2	2007-07-10	Kan et al.	
	4	8095640	B2	2012-01-10	Guingo et al.	
	5	8347104	B2	2013-01-01	Pathiyal, Krishna K.	
	6	8694772	B2	2014-04-08	Kao et al.	
	7	8705361	B2	2014-04-22	Venkataraman et al.	
	8	8719423	B2	2014-05-06	Wyld	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8780857	B2	2014-07-15	Balasubramanian et al.	
	10	8811991	B2	2014-08-19	Jain 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	20050135264	A1	2005-06-23	Popoff et al.	
	2	20050245241	A1	2005-11-03	Durand et al.	
	3	20070165630	A1	2007-07-19	Rasanen et al.	
	4	20080125079	A1	2008-05-29	O'Neil et al.	
	5	20100287599	A1	2010-11-11	He 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1	1503548	EP	A1	2005-02-02	FG Microtec GmbH		☐
	2	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		☐
	3	2008301121	JP	A	2008-12-11	Kyocera Corp.		☐
	4	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		☐
	5	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐
	6	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	7	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.		☐
	8	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐

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		☐

If you wish to add additional non-patent literature 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*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./

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	5974439	A	1999-10-26	Bollella, Gregory	
	2	6038540	A	2000-03-14	Krist et al.	
	3	6058434	A	2000-05-02	Wilt et al.	
	4	6125391	A	2000-09-26	Meltzer et al.	
	5	6393014	B1	2002-05-21	Daly et al.	
	6	6397259	B1	2002-05-28	Lincke et al.	
	7	6735206	B1	2004-05-11	Oki et al.	
	8	6748437	B1	2004-06-08	Mankude 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	7017189	B1	2006-03-21	DeMello et al.	
	11	7024460	B2	2006-04-04	Koopmas et al.	
	12	7047276	B2	2006-05-16	Liu et al.	
	13	7058022	B1	2006-06-06	Carolan et al.	
	14	7149521	B2	2006-12-12	Sundar et al.	
	15	7162237	B1	2007-01-09	Silver et al.	
	16	7200112	B2	2007-04-03	Sundar et al.	
	17	7248570	B2	2007-07-24	Bahl et al.	
	18	7266371	B1	2007-09-04	Amin et al.	
	19	7366654	B2	2008-04-29	Moore, Robert C.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7391724	B2	2008-06-24	Alakoski et al.	
	21	7395244	B1	2008-07-01	Kingsford, Bryan	
	22	7411930	B2	2008-08-12	Montojo et al.	
	23	7454191	B2	2008-11-18	Dawson et al.	
	24	7508799	B2	2009-03-24	Sumner et al.	
	25	7512128	B2	2009-03-31	DiMambro et al.	
	26	7554983	B1	2009-06-30	Muppala, Suresh	
	27	7564799	B2	2009-07-21	Holland et al.	
	28	7627767	B2	2009-12-01	Sherman et al.	
	29	7676673	B2	2010-03-09	Weller et al.	
	30	7817615	B1	2010-10-19	Breau 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7844034	B1	2010-11-30	Oh et al.	
	32	7849161	B2	2010-12-07	Koch et al.	
	33	7849477	B2	2010-12-07	Cristofalo et al.	
	34	7860088	B2	2010-12-28	Lioy, Marcello	
	35	7889384	B2	2011-02-15	Armentrout et al.	
	36	7894431	B2	2011-02-22	Goring et al.	
	37	7899039	B2	2011-03-01	Andreasen et al.	
	38	7966405	B2	2011-06-21	Sundaresan et al.	
	39	7978686	B2	2011-07-12	Goyal et al.	
	40	7987496	B2	2011-07-26	Bryce et al.	
	41	8032168	B2	2011-10-04	Ikaheimo, Jorma	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8073427	B2	2011-12-06	Koch et al.	
	43	8104080	B2	2012-01-24	Burns et al.	
	44	8131840	B1	2012-03-06	Denker, Richard E.	
	45	8150394	B2	2012-04-03	Bianconi et al.	
	46	8190122	B1	2012-05-29	Alexander et al.	
	47	8385964	B2	2013-02-26	Haney, Richard D.	
	48	8407763	B2	2013-03-26	Weller et al.	
	49	8484568	B2	2013-07-09	Rados et al.	
	50	8503455	B2	2013-08-06	Heikens, Heico	
	51	8504032	B2	2013-08-06	Lott et al.	
	52	8504687	B2	2013-08-06	Maffione 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8504690	B2	2013-08-06	Shah et al.	
	54	8522337	B2	2013-08-27	Adusumilli et al.	
	55	8527662	B2	2013-09-03	Biswas et al.	
	56	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	57	8644813	B1	2014-02-04	Gailloux et al.	
	58	8667542	B1	2014-03-04	Bertz et al.	
	59	8793304	B2	2014-07-29	Lu et al.	
	60	8812525	B1	2014-08-19	Taylor III, Buford Leonard	
	61	8863111	B2	2014-10-14	Selitser et al.	
	62	8948726	B2	2015-02-03	Smith et al.	
	63	8966018	B2	2015-02-24	Bugwadia 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	9002342	B2	2015-04-07	Tenhunen et al.	
	65	RE44412		2013-08-06	Naqvi 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	20030134650	A1	2003-07-17	Sundar et al.	
	2	20030159030	A1	2003-08-21	Evans, Junius A.	
	3	20040127208	A1	2004-07-01	Nair et al.	
	4	20040260766	A1	2004-12-23	Barros et al.	
	5	20050041617	A1	2005-02-24	Huotari et al.	
	6	20050096024	A1	2005-05-05	Bicker et al.	
	7	20060075506	A1	2006-04-06	Sanda 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	8	20060095517	A1	2006-05-04	O'Connor et al.	
	9	20060126562	A1	2006-06-15	Liu, Huitao	
	10	20060277590	A1	2006-12-07	Limont et al.	
	11	20060291419	A1	2006-12-28	McConnell et al.	
	12	20070257767	A1	2007-11-08	Beeson, Curt	
	13	20080018494	A1	2008-01-24	Waite et al.	
	14	20080034063	A1	2008-02-07	Yee, Robert	
	15	20090036111	A1	2009-02-05	Danford et al.	
	16	20120108225	A1	2012-05-03	Luna 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]

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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	05/26/2016

*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./

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8339991		2012-12-25	Biswas et al.	
	54	8630314		2014-01-14	York, Frederick John	
	55	8868725		2014-10-21	Samba, Augustine S.	

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	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	
	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20120166604	A1	2012-06-28	Fortier et al.	
	12	20020191573		2002-12-19	Whitehill et al.	
	13	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	14	20090070379		2009-03-12	Rappaport, Theodore R.	
	15	20100318652		2010-12-16	Samba, Augustine S.	

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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	05/26/2016

*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.

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Gart, Matthew S.
Attorney Docket Number	RALEP032C1

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	7805140	B2	2010-09-28	Friday et al.	
	2	8605691	B2	2013-12-10	Soomro et al.	
	3	8655357	B1	2014-02-18	Gazzard et al.	
	4	8706863		2014-04-22	Fadell, Anthony	

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	20020188732	A1	2002-12-12	Buckman et al.	
	2	20080010379	A	2008-01-10	Zhao, Hang	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Gart, Matthew S.
	Attorney Docket Number	RALEP032C1

	3	20080034419	A	2008-02-07	Mullick 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	1878160	CN	A	2006-12-13	Jiang, Yong		☐
	2	2011149532	WO	A1	2011-12-01	Raleigh et al.		☐

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	05/26/2016

*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.

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner
709	203,217, 220,223, 224	5/26/2016	AJR
H 04L	29/08072	5/26/2016	AJR
H 04L	29/06	5/26/2016	AJR
H 04L	43/00	5/26/2016	AJR
H 04L	12/2602	5/26/2016	AJR
H 04L	41/22	5/26/2016	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	5/26/2016	AJR
Inventor name search conducted.	5/26/2016	AJR

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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	6885997	B1	2005-04-26	Roberts, David T.	
	2	7720464	B2	2010-05-18	Batta, Puneet	
	3	7797060	B2	2010-09-14	Grgic et al.	
	4	7853255	B2	2010-12-14	Karaoguz et al.	
	5	7930327	B2	2011-04-19	Craft David et al.	
	6	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	7	8095124	B2	2012-01-10	Balia, Hinal K.	
	8	8229394	B2	2012-07-24	Karlberg, Johan	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8264965	B2	2012-09-11	Dolganow et al.	
	10	8442015	B2	2013-05-14	Behzad et al.	
	11	8495700	B2	2013-07-23	Shahbazi, Majid	
	12	8528068	B1	2013-09-03	Weglein et al.	
	13	8548427	B2	2013-10-01	Chow et al.	
	14	8566236	B2	2013-10-22	Busch, James David	
	15	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	16	8589955	B2	2013-11-19	Roundtree et al.	
	17	8601125	B2	2013-12-03	Huang et al.	
	18	8635164	B2	2014-01-21	Rosenhaft et al.	
	19	8660853	B2	2014-02-25	Robb et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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	20030188006	A	2003-10-02	Bard, Steven R.	
	2	20030188117	A	2003-10-02	Yoshino et al.	
	3	20040255145	A	2004-12-16	Chow, Jerry	
	4	20050055595	A	2005-03-10	Frazer et al.	
	5	20060160536	A	2006-07-20	Chou, Joey	
	6	20060168128	A	2006-07-27	Sistla et al.	
	7	20070259656	A	2007-11-08	Jeong, Jong Woo	
	8	20080263348	A	2008-10-23	Zaltsman et al.	
	9	20080313315	A	2008-12-18	Karaoguz 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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	10	20090282127	A	2009-11-12	Leblanc et al.	
	11	20100167696	A	2010-07-01	Smith, Christopher David et al.	
	12	20110019574	A	2011-01-27	Malomsoky 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	101123553A	CN		2007-09-11	Southeast University		☐
	2	1937511A	CN		2007-03-28	ZTE		☐

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	05/26/2016

*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.

EFS Web 2.1.17

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

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	7809351	B1	2010-10-05	Panda et al.	
	2	8346210	B2	2013-01-01	Balsan et al.	
	3	8355696	B1	2013-01-15	Olding et al.	
	4	8488597		2013-07-16	Nie 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	20050250536	A1	2005-11-10	Deng et al.	
	2	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	20060035631	A1	2006-02-16	White et al.	
	4	20060206709	A1	2006-09-14	Labrou et al.	
	5	20070060200	A1	2007-03-15	Boris et al.	
	6	20090046707	A1	2009-02-19	Smires et al.	
	7	20100311402	A1	2010-12-09	Srinivasan et al.	
	8	20110277019	A1	2011-11-10	Pritchard Jr., John Russell	

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]
	1	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐

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]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	05/26/2016

*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./

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	5633868	A	1997-05-27	Baldwin et al.	
	2	6061571	A	2000-05-09	Tamura, Hideo	
	3	6157636	A	2000-12-05	Voit et al.	
	4	6725256	B1	2004-04-20	Albal et al.	
	5	6751296	B1	2004-06-15	Albal et al.	
	6	6792461	B1	2004-09-14	Hericourt, Olivier	
	7	6934751	B2	2005-08-23	Jayapalan et al.	
	8	7027055	B2	2006-04-11	Anderson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7043225	B1	2006-05-09	Patel et al.	
	10	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	11	7174156	B1	2007-02-06	Mangal, Manish	
	12	7636626	B2	2009-12-22	Oesterling et al.	
	13	7680086	B2	2010-03-16	Eglin	
	14	7720206	B2	2010-05-18	Devolites et al.	
	15	7765294	B2	2010-07-27	Edwards et al.	
	16	7843831	B2	2010-11-30	Morrill et al.	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8131858	B2	2012-03-06	Agulnik et al.	
	19	8160056	B2	2012-04-17	Van der Merwe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	8180333	B1	2012-05-15	Wells et al.	
	21	8223655	B2	2012-07-17	Heinz et al.	
	22	8315198	B2	2012-11-20	Corneille et al.	
	23	8340678	B1	2012-12-25	Pandey, Vinod	
	24	8385199	B1	2013-02-26	Coward et al.	
	25	8520595	B2	2013-08-27	Yadav et al.	
	26	8523547	B2	2013-09-03	Pekrul, Merton W.	
	27	8621056	B2	2013-12-31	Coussemaeker et al.	
	28	8875042	B2	2014-10-28	LeJeune et al.	
	29	9135037	B1	2015-09-15	Petrescu-Prahova et al.	
	30	9172553	B2	2015-10-27	Dawes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	9177455	B2	2015-11-03	Remer, David M.	

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	20030028623	A1	2003-02-06	Hennessey et al.	
	2	20050060525	A1	2005-03-17	Schwartz et al.	
	3	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	4	20070061800	A1	2007-03-15	Cheng et al.	
	5	20070255769	A1	2007-11-01	Agrawal et al.	
	6	20070299965	A1	2007-12-27	Nieh et al.	
	7	20080066181	A1	2008-03-13	Haveson et al.	
	8	20080126287	A1	2008-05-29	Cox et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	20080212751	A1	2008-09-04	Chung, Simon	
	10	20090203352	A1	2009-08-13	Fordon et al.	
	11	20100041365	A1	2010-02-18	Lott et al.	
	12	20100121744	A1	2010-05-13	Belz et al.	
	13	20140073291	A1	2014-03-13	Hildner 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]
	1	2002045315	WO	A2	2002-06-06	Micromuse		
	2	2009008817	WO	A1	2009-01-15	Ericsson		

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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)	2016-03-09
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.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/008817 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04L 12/26* (2006.01)

(21) International Application Number:
PCT/SE2008/050830

(22) International Filing Date: 3 July 2008 (03.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/948,223 6 July 2007 (06.07.2007) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **PELLETIER, Ghyslain**; Bondevägen 57A, S-961 39 Boden (SE). **WÄNSTEDT, Stefan**; Faktorsvägen 15, S-972 51 Luleå (SE). **ENSTRÖM, Daniel**; Hedenslundsvägen 7, S-954 33 Gammelstad (SE).

(74) Agent: **NILSSON, Charlotte**; Ericsson AB, Patent Unit 3G, S-164 80 Stockholm (SE).

(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, ST, 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:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) Title: CONGESTION CONTROL IN A TRANSMISSION NODE

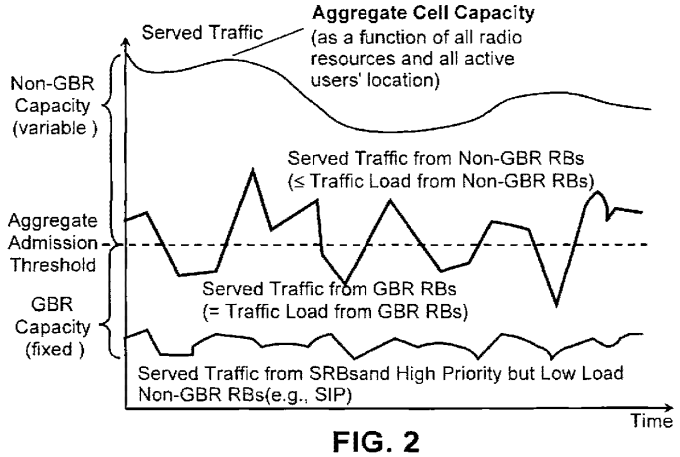


FIG. 2

(57) Abstract: Packets are selectively marked or dropped when congestion of the radio resources is experienced, the selective marking/dropping being related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the present technology takes into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

WO 2009/008817 A1

CONGESTION CONTROL IN A TRANSMISSION NODE

[0001] This application claims the benefit and priority of United States provisional patent application 60/948,223, filed July 6, 2007, entitled "CONGESTION CONTROL ALGORITHM IN A TRANSMISSION NODE", which is incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] This invention pertains to telecommunications, and particularly to the control of congestion in wireless telecommunications.

BACKGROUND

[0003] It is a well-known fact that packet-switched networks utilizing resources shared between the users can experience congestion. Congestion will happen when the sum of traffic of the ingress nodes of the shared resource exceeds the sum of the traffic of the egress nodes of the same shared resource. The most typical example is a router with a specific number of connections. Even if the router has processing power enough to re-route the traffic according to the estimated link throughput, the current link throughput might restrict the amount of traffic the outgoing links from the router can cope with. Hence, the buffers of the router will build up and eventually overflow. The network then experiences congestion and the router is forced to drop packets.

[0004] **Radio resources and congestion**

[0005] Another example of congestion can be found when studying wireless networks with shared channels such as 802.11 a/b/g, High Speed Packet Access (HSPA), Long Term Evolution (LTE), and Worldwide Interoperability for Microwave Access (WiMAX). In these networks, at least the downlink is shared between the users and thus is a possible candidate to experience congestion. In e.g. the case of LTE, the enhanced NodeB (eNB) base station will manage re-transmissions on the Medium Access Control (MAC) layer to the mobile terminal (user equipment, UE) which will have impact on the amount of traffic for which the eNB can provide throughput at any given moment. The more re-transmissions (HARQ and RLC ARQ) required for

successful reception at the UE, the less are the available resources (e.g. transmission power, number of available transmission slots) to provide throughput for other users.

[0006] In, e.g., the case of LTE, the base station (eNB) will also manage how much redundancy is added to protect the data against transmission errors by selecting a proper Modulation and Coding Scheme (MCS) for the physical channel, and then matches the resulting bits to a number of resource blocks (RB). The more conservative the MCS selected for the transmission (e.g. for UEs in bad radio conditions), the less the available resource blocks to provide throughput for users.

[0007] **Congestion and IP transport protocols**

[0008] The normal behavior for any routing node is to provide buffers that can manage a certain amount of variation in input/output link capacity and hence absorb minor congestion occurrences. However, when the congestion is severe enough, the routing node will eventually drop packets.

[0009] Transmission Control Protocol (TCP) is a connection-oriented, congestion-controlled and reliable transport protocol. For TCP traffic, a dropped packet will be detected by the sender since no acknowledgment (ACK) is received for that particular packet and a re-transmission will occur. Further, the TCP protocol has a built in rate adaptive feature which will lower the transmission bit-rate when packet losses occur and re-transmissions happen on the Internet Protocol (IP) layer. Hence, TCP is well suited to respond to network congestion.

[0010] User Datagram Protocol (UDP) is a connectionless transport protocol that only provides a multiplexing service with an end-to-end checksum. UDP is not reliable or congestion-controlled. UDP traffic thus does not have similar mechanisms as TCP to respond to congestion. UDP traffic is by definition non-reliable in the sense that the delivery is not guaranteed. Missing UDP packets will not be re-transmitted unless the application layer using the transport service provided by UDP has some specialized feature which allows this. UDP by itself does not respond in any way to network congestion, although application layer mechanisms may implement some form of response to congestion.

[0011] **Explicit Congestion Notification (ECN)**

[0012] To further increase the performance of routing nodes, a mechanism called "Explicit Congestion Notification for IP" has been developed. See, e.g., RFC 3168, Proposed Standard, September 2001, incorporated herein by reference. This mechanism uses two bits in the IP header to signal the risk for congestion-related losses. The field has four code points, where two are used to signal ECN capability and the other two are used to signal congestion. The code point for congestion is set in, e.g., routers. When the receiver has encountered a congestion notification it propagates the information to the sender of the stream which then can adapt its transmission bit-rate. For TCP, this is done by using two bits in the TCP header. Prior to their definition for use with ECN, these bits were reserved and not used. When received, these bits trigger the sender to reduce its transmission bit-rate.

[0013] The benefit with TCP is dual in this case. As a first benefit, since TCP acknowledges the reception of the incoming packets, all TCP connections automatically have a back-channel (This is not the case with UDP). As a second benefit, TCP has a built-in back-off response to packet losses which also can be used in connection with ECN (This is not available for UDP).

[0014] To summarize, ECN with TCP has all the mechanisms available in standards to enable successful deployment. This is also seen in more modern routers and new PC operating systems.

[0015] The situation with ECN for UDP is quite different. ECN is defined for IP usage with any transport protocol. However, ECN is only explicitly specified in terms of use with TCP traffic. ECN for UDP needs the same generic mechanisms as ECN for TCP: a fast back-channel and some rate control algorithm.

[0016] Within the context of UDP-based real-time communication services such as IMS Multimedia Telephony (MTSI), there is a clear need to manage congestion. Such services are by definition quite sensitive to packet loss. Hence, any means available to avoid such losses should be used. ECN for UDP would be a suitable candidate to alleviate the impact of congestion. It turns out that both requirements for successful ECN usage, fast feedback and rate adaptation, are readily available in many such

services, the lacking part is the connection between the ECN bits and the response of the application.

[0017] Another aspect of the use of ECN is the congestion avoidance algorithm (described below) used in a congested node to either drop or mark packets to signal congestion.

[0018] **Congestion avoidance algorithms**

[0019] Congestion avoidance algorithms include three basic types: Tail Drop, Random Early Detection (RED), and Weighted Random Early Detection (WRED).

[0020] A tail drop congestion avoidance algorithm treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

[0021] The Random Early Detection (RED) congestion avoidance algorithm addresses network congestion in a responsive rather than reactive manner. Underlying the RED mechanism is the premise that most traffic runs on data transport implementations which are sensitive to loss and will temporarily slow down when some of their traffic is dropped. TCP, which responds appropriately - even robustly - to traffic drop by slowing down its traffic transmission, effectively allows RED's traffic-drop behavior to work as a congestion-avoidance signaling mechanism. A typical RED implementation starts dropping or marking packets when the average queue depth is above a minimum threshold. The rate of dropping or marking packets is increased linearly as the average queue size increases, until the queue size reaches the maximum threshold. At this point, all packets are dropped. Whether a packet is ECN-marked or dropped depends on if the ECN bits shows that the mechanism is enabled. However, when applied to traffic that does not respond to congestion or is not robust against losses, RED induces negative impacts on the service.

[0022] A weighted Random Early Detection (WRED) congestion avoidance precedence between IP flows provides for preferential traffic handling of packets with higher priority. WRED can selectively discard or mark lower priority traffic when the average queue depth is above a minimum threshold. Differentiated performance characteristics

for different classes of service can be provided in this manner. By randomly dropping or marking packets prior to periods of high congestion, WRED tells the packet source to decrease its transmission rate.

[0023] Other variants of similar algorithms exist, where the decisional factor is based on queue sizes, traffic classes, resource reservation, and ECN capabilities. In this respect, network nodes interact with the transport protocols in an attempt to mitigate congestion while providing means to the sender to adapt its sending rate consequently and limit the impact of congestion to applications.

[0024] Algorithms to mark or drop packets when congestion is experienced in a network node, henceforth simply referred to as a "marking algorithm", have so far (i.e. in fixed networks) defined congestion as a function of a node's queue depth. The probability that a packet will be "congestion-marked or dropped" in a queue is derived as a function of the average depth of the queue where it lies. Traffic classes and resource reservation (e.g. RSVP) in this respect are essentially a mean to separate one interface's queue into multiple smaller ones, for the purpose of calculating this probability.

[0025] **Congestion in fixed packet data networks**

[0026] For fixed packet-switched networks, a link is typically said to be congested when the offered load on the link reaches a value close to the capacity of the link. In other words, congestion is defined as the state in which a network link is close to being completely utilized by the transmission of bytes. This is largely because the capacity of the link is constant over time, and because the physical characteristics of the ingress and of the egress links are similar.

[0027] **Congestion in wireless networks**

[0028] Defining congestion in wireless network is more complex than simply relating to capacity in terms of the number of bits that can be transmitted. Congestion in wireless networks can be defined as the state in which the transmission channel is close to being completely utilized.

[0029] The total capacity of the transmission channel is distributed between different receivers having different radio conditions. This means that the shared resources are consumed partly by varying levels of redundancy (retransmissions, channel coding) necessary to protect the data that is useful to the user (i.e. IP packets). This tradeoff is conceptually shown in Fig. 1.

[0030] **Managing radio resources and cell capacity**

[0031] The concept of radio bearers is used in LTE to, e.g., support user data services. End-to-end services (e.g. IP services) are multiplexed on different bearers. These different bearers represent different priority queues over the radio interface.

[0032] A bearer is referred to as a GBR bearer if dedicated network resources related to a Guaranteed Bit Rate (GBR) value that is associated with the bearer are permanently allocated (e.g. by an admission control function in the RAN) at bearer establishment / modification. Otherwise, a bearer is referred to as a Non-GBR bearer:

- GBR (Guaranteed Bit Rate – UL + DL)
- MBR (Maximum Bit Rate – UL + DL)

[0033] With respect to how resources are separated between different receivers, there can be a guarantee for some receivers about a specific bit rate, a guaranteed bit rate (GBR). There can also be a part of the cell capacity that is used for data for which no guarantee in terms of bit rate is applicable (non-GBR). Applications, such as real-time applications using codecs that can adapt their bit rate, may fill their allocated GBR and go to a higher rate to fill the non-GBR area, when possible, to increase the application bit rate and hence improve their performance. Fig. 2 shows capacity in terms whether bit rate is guaranteed or not.

[0034] **eNode B Measurements**

[0035] In E-UTRAN, certain types of measurements can be performed internally in the eNode B. These measurements do not need to be specified in the standard; rather they are implementation dependent. The possible measurements serve a number of procedures, such as handovers and other radio resource management.

[0036] In particular, the eNode B can perform measurement related to the amount of transmission power in the cell, antenna branch or per resource block (per UE), as well as received power in the UL per cell, per UE, or per resource block.

[0037] **Measurements and Handover decisions**

[0038] The serving eNode B performs UL measurements on (for instance) the signal-to-interference-ratio (SIR), received resource block power, and the received total wideband power. For a handover (HO) decision, it may also take into account other (downlink) measurements, such as the transmitted (total) carrier power and/or the transmitted carrier power per resource block.

[0039] **Problems with existing solutions**

[0040] When the network node that experiences congestion is at one edge of a wireless network, such as a base station transmitter, congestion can occur due to one or more of the following: (1) the ingress data rate is larger than the downlink available throughput for the entire cell; (2) the ingress data rate is larger than the downlink available throughput, for one receiver (UE); (3) a UE is in bad radio conditions; (4) the cell capacity becomes power limited.

[0041] In other words, the total bit rate exchanged over the air is distributed between user data and coding rate, where the coding rate is adjusted to the radio conditions the receiver is in.

[0042] To make it possible to signal congestion using, e.g., ECN in a manner that is most relevant to quickly efficiently decrease congestion in the radio resources, a mechanism is needed to mark the packets. Packets can (for example) be marked using ECN, even for real-time applications using RTP over UDP.

[0043] Using ECN with UDP traffic requires specialized application behavior: upon reception of a congestion notification, the receiver needs to transmit a request to the sender requiring the sender to reduce its bit-rate. When that request arrives at the sender, it should immediately reduce the transmitted bit-rate. The amount of the reduction is determined by the sender, which in turn can base its decision on a number of parameters.

[0044] In short, current foreseen mechanisms will not provide efficient marking or packet dropping mechanisms that efficiently address congestion of the radio resources.

SUMMARY

[0045] In accordance with an aspect of the technology described herein, packets are selectively marked or dropped when congestion of the radio resources is experienced, the selective marking/dropping being related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the present technology takes into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

[0046] One aspect of the technology concerns a method of operating a communications network. The method comprises detecting congestion of a shared radio resource and, for a user of the shared radio resource, selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

[0047] In one example embodiment the user's share is expressed in terms of cost or amount of resources associated to a user. In one example implementation, the method further comprises determining the cost, or the amount of resources associated to the user, based on transmitter measurements. For example, the transmitter measurements include at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate. Another example implementation, comprises determining the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements. In an example implementation, the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

[0048] An example embodiment further comprises determining the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality indications; handover measurements; and, the type of modulation and coding scheme used for the user.

[0049] An example embodiment further comprises selectively dropping the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

[0050] In another of its aspects, the technology concerns a packet marker which marks or drops packet in accordance with the technique(s) described herein, e.g., selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

BRIEF DESCRIPTION OF THE DRAWINGS

[0051] The foregoing and other objects, features, and advantages of the invention will be apparent from the following more particular description of preferred embodiments as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout the various views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

[0052] Fig. 1 is a diagrammatic view of tradeoff between "useful bits" and channel coding using the same amount of resource blocks.

[0053] Fig. 2 is a diagrammatic view showing operation-controlled partitioning of cell capacity.

[0054] Fig. 3 is a diagrammatic view showing layered functional view of functional components of an example LTE eNB node and a user equipment unit (UE).

[0055] Fig. 4 is a diagrammatic view showing downlink scheduler input, output and interactions according to an example embodiment.

DETAILED DESCRIPTION

[0056] In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular architectures, interfaces, techniques, etc. in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details. That is, those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are included within its spirit and scope. In some instances, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of the present invention with unnecessary detail. All statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0057] Thus, for example, it will be appreciated by those skilled in the art that block diagrams herein can represent conceptual views of illustrative circuitry embodying the principles of the technology. Similarly, it will be appreciated that any flow charts, state transition diagrams, pseudocode, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0058] The functions of the various elements including functional blocks labeled or described as "processors" or "controllers" may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared or distributed. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may include, without limitation, digital signal processor (DSP) hardware, read only memory (ROM) for storing software, random access memory (RAM), and non-volatile storage.

[0059] Fig. 3 shows various example functions involved in transmission (eNB) and reception (UE) in a Long Term Evolution (LTE) version of a telecommunications network 20. While LTE is used to exemplify concepts related to radio transmission such as the packet marking technique described herein, similar concepts apply also to other wireless technologies and the technology is thus equally applicable to systems other than LTE.

[0060] The telecommunications network 20 includes both base station node 28 (also known as a NodeB, eNodeB, or BNode) and wireless terminal 30 (also known as a user equipment unit [UE], mobile station, or mobile terminal). The wireless terminal 30 can take various forms, including (for example) a mobile terminal such as mobile telephones ("cellular" telephones) and laptops with mobile termination, and thus can be, for example, portable, pocket, hand-held, computer-included, or car-mounted mobile devices which communicate voice and/or data with radio access network. Alternatively, the wireless terminals can be fixed wireless devices, e.g., fixed cellular devices/terminals which are part of a wireless local loop or the like.

[0061] Typically base station node 28 communicates over wireless interface 32 (e.g., a radio interface) with plural wireless terminals, only one representative wireless terminal 30 being shown in Fig. 3. Each base station node 28 serves or covers a geographical area known as a cell. That is, a cell is a geographical area where radio coverage is provided by the radio base station equipment at a base station site. Each cell is identified by an identity, which is broadcast in the cell. The base stations communicate over the air interface (e.g., radio frequencies) with the user equipment units (UE) within range of the base stations.

[0001] The base station node 28 comprises a radio access network (RAN). If the radio access network is a "flat" type network as occurs in LTE, the base station node 28 essentially performs most of the radio access network functionality and connects to core networks. If, on the other hand, the radio access network is of a more conventional type (such as a Universal Mobile Telecommunications (UMTS) Terrestrial Radio Access Network (UTRAN), one or more base station nodes are connected to the core network through a controller node such as a radio network controller (RNC). The UMTS is a third generation system which in some respects builds upon the radio access technology known as Global System for Mobile communications (GSM) developed in

Europe. UTRAN is essentially a radio access network providing wideband code division multiple access (WCDMA) to user equipment units (UEs). The Third Generation Partnership Project (3GPP) has undertaken to evolve further the UTRAN and GSM-based radio access network technologies, the LTE being just one version of evolution.

[0062] As those skilled in the art appreciate, in W-CDMA technology a common frequency band allows simultaneous communication between a user equipment unit (UE) and plural base stations. Signals occupying the common frequency band are discriminated at the receiving station through spread spectrum CDMA waveform properties based on the use of a high speed, pseudo-noise (PN) code. These high speed PN codes are used to modulate signals transmitted from the base stations and the user equipment units (UEs). Transmitter stations using different PN codes (or a PN code offset in time) produce signals that can be separately demodulated at a receiving station. The high speed PN modulation also allows the receiving station to advantageously generate a received signal from a single transmitting station by combining several distinct propagation paths of the transmitted signal. In CDMA, therefore, a user equipment unit (UE) need not switch frequency when handoff of a connection is made from one cell to another. As a result, a destination cell can support a connection to a user equipment unit (UE) at the same time the origination cell continues to service the connection. Since the user equipment unit (UE) is always communicating through at least one cell during handover, there is no disruption to the call. Hence, the term "soft handover." In contrast to hard handover, soft handover is a "make-before-break" switching operation.

[0063] Fig. 3 shows an Internet Protocol (IP) packet 40_B received at base station node 28, e.g., from a core network or another base station node. Fig. 3 further shows various layer handlers or functionalities comprising base station node 28 and wireless terminal 30. In particular, for base station node 28 and wireless terminal 30, respectively, Fig. 3 shows: PDCP functionality 42_B and 42_W; radio link control functionality 44_B and 44_W; medium access control (MAC) functionality 46_B and 46_W; and physical layer functionality 48_B and 48_W.

[0064] Fig. 3 illustrates that IP packets for plural users are typically in-coming on SAE bearers to base station node 28 from other radio access network nodes or from the core

network. "SAE" stands for "System Architecture Evolution", and an SAE bearer supports a flow and provides Quality of Service (QoS) end-to-end (both over radio and core network). Typically there is a one-to-one mapping between an SAE Bearer and an SAE Radio Bearer. Furthermore there is a one-to-one mapping between a Radio Bearer and a logical channel. It then follows that an SAE Bearer, i.e. the corresponding SAE Radio Bearer and SAE Access Bearer, is the level of granularity for QoS control in an SAE/LTE access system. Packet flows mapped to the same SAE Bearer receive the same treatment. Fig. 3 further illustrates that an instance of each of the aforementioned functionalities can exist for each user (such as user #i depicted as one of the plural users in Fig. 3).

[0065] Fig. 3 further illustrates various sub-units of the layer handlers or functionalities for base station node 28 and wireless terminal 30. For example, in base station node 28 PDCP functionality 42_B comprises header compressors 50_B and ciphering units 52_B, and in wireless terminal 30 the PDCP functionality 42_W comprises header decompressors 50_W and deciphering units 52_W. In base station node 28, the radio link control functionality 44_B comprises segmentation/automatic repeat request (ARQ) unit 54_B, while in wireless terminal 30 the radio link control functionality 44_W comprises concatenation/automatic repeat request (ARQ) unit 54. In base station node 28 the medium access control (MAC) functionality 46_B comprises MAC scheduler 56; MAC multiplexing units 58_B; and Hybrid ARQ units 60_B. In wireless terminal 30 the medium access control (MAC) functionality 46_W comprises MAC demultiplexing units 58_W and Hybrid ARQ units 60_W. In base station node 28 the physical layer functionality 48_B comprises coding units 62_B; modulators 64_B; and antenna and resource mapping units 66_B which ultimately connect to or comprise transceivers 68_B. Conversely, in wireless terminal 30 the physical layer functionality 48_W comprises decoding units 62_W; demodulators 64_W; and antenna and resource mapping units 66_W (which connect to or comprise transceiver(s) 68_W).

[0066] The MAC scheduler 56 is connected to or interacts with various units of functionalities of base station node 28. For example, a payload selection signal is applied from MAC scheduler 56 to segmentation/automatic repeat request (ARQ) unit 54_B; priority handling and payload selection signals are applied from MAC scheduler 56 to MAC multiplexing units 58_B; retransmission control signals are applied from MAC scheduler 56 to Hybrid ARQ units 60_B; modulation scheme signals are applied

from MAC scheduler 56 to modulators 64_B; and, antenna and resource assignment signals are applied from MAC scheduler 56 to antenna and resource mapping units 66_B.

[0067] Fig. 3 thus shows how user data in an IP packet 40_B is processed by the various layers or functionalities of base station node 28, and is carried to PDCP functionality 42_B in a SAE bearer; from PDCP functionality 42_B to radio link control functionality 44_B by a radio bearer; from radio link control functionality 44_B to medium access control (MAC) functionality 46_B by a logical channel; and from medium access control (MAC) functionality 46_B to physical layer functionality 48_B by a transport channel; and is then transported over air interface 32 to wireless terminal 30.

[0068] On the side of wireless terminal 30, Fig. 3 also shows how the information received over air interface 32 is handled by physical layer functionality 48_W; and then handed over transport channels to medium access control (MAC) functionality 46_W, and then handed over logical channels to radio link control functionality 44_W; handed over radio bearers to PDCP functionality 42_W; and then realized over SAE bearers as a received packet 40_W.

[0069] In LTE, a shared channel (the DL-SCH) is used for downlink transmissions of user data. As can be seen in Fig. 3, MAC scheduler 56 is the process, functionality, or unit that determines what receiver will be served using the shared resources. The MAC scheduler 56 also determines what resource block (in time and frequency) will be used as well with the proper modulation and coding scheme. User and data rate on the DL-SCH is based on instantaneous channel quality. For the uplink and in other wireless channels where dedicated radio bearers are used, the shared resource in the amount of interface that can be generated for each UE; this is referred to as an interference limited system.

[0070] As indicated previously, congestion is typically experienced in a radio network when the shared resources become utilized beyond a certain threshold. For a fixed amount X of radio resources, the amount of user data that is transmitted varies based on radio link conditions.

[0071] The present technology marks or drops packets selectively when congestion of the radio resources is experienced. In the illustrated embodiment, the selective

marking/dropping of packets during congestion according to the criteria/techniques described herein can be implemented in or realized by in a suitable functionality in a node such as a base station (eNB). The functionality which makes the decision to mark or drop a packet according to the foregoing criteria is termed a "packet marker" and can be, for example, a downlink scheduler (e.g., MAC scheduler 56), or a separate process that monitors the queues of the scheduler, or separate process with its own queues prior to the scheduler.

[0072] The selective marking/dropping technique of the present technology is related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and/or fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the packet marker and the techniques of the present technology take into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

[0073] As used herein, the term "user" refers to a user of radio resources, and thus may be an IP flow (service) [even a packet itself], a radio bearer, a UE, or a group of UEs. Which of those is marked may be based on relative priority between each other, such as using QoS classes, UE subscription information, or the like.

[0074] The technology thus encompasses at least two ways of apportioning a user's share: the first way is based on the cost or amount of resources associated to a user; the second way is based on "fairness".

[0075] A user's share of the total costs can be derived in terms of radio resources. The cost, or the amount of resources associated to the user, may be determined based on different measurements, independently or not, such as transmitter measurements and receiver feedback and/or measurements.

[0076] As used herein, "fairness" means that both the share of radio resources and QoS and other guarantees provided by the system are used in the decision to mark or drop.

On the other hand, in a system with high congestion where QoS targets cannot be reached for several UEs, the eNB can use each UE's share of the resources and use the QoS agreements relative to each other to decide how to mark/drop packets, until congestion levels come back to normal. Thus, "fairness" encompasses a combination of radio resource usage and QoS agreements (bitrate, delay, loss rate, etc) and/or priorities relative to each other, in periods of congestion of the radio resources.

[0077] In particular, measurements similar to those for handover (HO) decision can be used to measure a degree of fairness between UEs with respect to their respective resource utilization in the cell, for the purpose of congestion marking and or dropping at the IP transport level. UE measurements that indicate that the UE is getting closer to the threshold used to decide to make a HO means that the UE is in a non-favorable locations, and that radio conditions are deteriorating. In this case, more radio resources (power, retransmissions, etc) are needed to "reach" this UE. In other words, a strong received signal means that the UE does not require as many DL resources to receive the signal, but a weakly received signal means that the UE requires or wants more DL resources. Congestions (and thereby marking) may also occur somewhere in the cell where is not possible to do a handover, hence other measures for congestion marking can also be implemented.

[0078] The decision whether or not a packet is marked (or dropped) can also include whether the radio resources consumed by the user exceed the allocated guaranteed bit rate or not, in the case where congestion is experienced or a certain utilization threshold is reached.

[0079] For example, capacity gains (or the effect of marking on overall congestion in the cell) may be bigger if flows targeted at UEs in bad radio conditions are marked first - those are using more resources than others because of their poor radio situation. Fairness can be achieved by targeting traffic in the Non-GBR area for such UEs.

[0080] Fig. 4 shows the inputs to a MAC scheduler 56 which, in an example embodiment, performs the role of packet marker and thus performs the decision for packet marking and canceling according to the criteria described herein. In an example embodiment, the packet marker or scheduling function can be implemented by a processor or controller.

[0081] Fig. 4 shows that HARQ feedback and CQI reports from representative wireless terminal UE_k 30 are used as input to the MAC scheduler 56 for reporting the allocation of the shared resources to the receiver. This can be another type of input to the assessment of how much congestion is generated by a UE (relative to others).

[0082] The packet marker illustrated as MAC scheduler 56 also receives input regarding the logical channels for the representative wireless terminal 30_k, e.g.,, from the buffer/queue or buffer/queue manager for the logical channels 70_k for the representative wireless terminal 30_k. For each such channel/queue, the packet marker receives an indication of wireless terminal weight (UE weight); label, GBR/MBR status, and ARP (allocation/retention priority), queue delay, and queue (buffer) size. "Label: is also called QoS class identifier (qci) [see, e.g., 3GPP TS 23.203], and can be a scalar that is used as a reference to a specific packet forwarding behavior (e.g., packet loss rate, packet delay budget) to be provided to a SDF.

[0083] The packet marker illustrated as MAC scheduler 56 also receives input from a functionality or unit 72 that monitors the system frame number (SFN) flow and apprises the MAC scheduler 56 of the number of radio bearers required for the representative wireless terminal 30_k.

[0084] The packet marker illustrated as MAC scheduler 56 can also receive input from a suitable unit 74 regarding a multicast logical channel in the event that the representative wireless terminal 30_k participates in a multicast transmission. The information received by the packet marker from unit 74 regarding the multicast transmission basically pertain to the buffer for the multicast transmission and include label; GBR/MBR status; buffer/queue delay; and queue (buffer) size.

[0085] The packet marker illustrated as MAC scheduler 56 also receives other restriction information inputs such as those depicted as ICIC/RRM restrictions; UE capability restrictions; and other restrictions (e.g., DRX, TN, ...).

[0086] The packet marker illustrated as MAC scheduler 56 also receives input from link adaptor 76, particularly a number of bits input. The packet marker illustrated as MAC scheduler 56 outputs to link adaptor 76 a resource indication [which is a request for resources given the inputs from the data queue, e.g., for an uplink scheduling request

and for a downlink scheduling assignment. The link adaptor 76 in turn outputs an indication of the transport format for each scheduled transport channel.

[0087] The packet marker illustrated as MAC scheduler 56 outputs the number of resource blocks for each scheduled transport channel.

[0088] As indicated above, the selective marking/dropping technique of the present technology is related to or dependent the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and/or fairness.

[0089] Examples of transmitter measurements that can be used to determine a user's share of the total cost include the following:

DL total Tx power: Transmitted carrier power measured over the entire cell transmission bandwidth.

DL resource block Tx power: Transmitted carrier power measured over a resource block.

DL total Tx power per antenna branch: Transmitted carrier power measured over the entire bandwidth per antenna branch.

DL resource block Tx power per antenna branch: Transmitted carrier power measured over a resource block.

DL total resource block usage: Ratio of downlink resource blocks used to total available downlink resource blocks (or simply the number of downlink resource blocks used).

UL total resource block usage: Ratio of uplink resource blocks used to total available uplink resource blocks (or simply the number of uplink resource blocks used).

DL resource block activity: Ratio of scheduled time of downlink resource block to the measurement period.

UL resource block activity: Ratio of scheduled time of uplink resource block to the measurement period.

UL received resource block power: Total received power including noise measured over one resource block at the eNode B.

UL SIR (per UE): Ratio of the received power of the reference signal transmitted by the UE to the total interference received by the eNode B over the UE occupied bandwidth.

UL HARQ BLER: The block error ratio based on CRC check of each HARQ level transport block.

[0090] Examples of receiver feedback and/or measurements that can be used to determine a user's share of the total cost include, e.g. CQI/HARQ feedback as described above. In particular, handover measurements and CQI/HARQ feedback can be used in an example mode.

[0091] Examples of calculations would include the user's fraction of total power, the user's fraction of total interference, the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost), Channel quality indications (CQI, i.e. the UEs measurements of reception quality), handover measurements (where the logic that determines how close to the threshold for performing a handover the UE is, e.g. how close the UE is to getting out of coverage), the type of Modulation and coding scheme used for the user (where lower modulation and higher amount of redundancy indicates higher cost). All these can be used individually or in combination with each other.

[0092] Using LTE as a non-limiting example, measurements that can be used to determine a user's share of the total cost include:

- Measurements from the serving eNB: Received total WB power, SIR, transmitted (total) carrier power, Transmitted carrier power per resource block (per UE).
- Measurements from the UE, reported to the eNB: Reference symbol receiver power, reference symbol received quality, carrier received signal strength indicator.

[0093] Some of the layer handler/functionalities or units involved and/or illustrated in Fig. 3 are elaborated below.

[0094] In a first step of the transport-channel processing, a cyclic redundancy check (CRC) is calculated and appended to each transport block by ciphering units 52_B. The CRC is used to detect transmission errors in the receiver.

[0095] For channel coding as performed by coding units 62_B, only Turbo-coding can be applied in case of downlink shared channel (DL-SCH) transmission. Channel coding

adds redundancy (similar to Forward Error Correction - FEC) to the bits to be transmitted, to compensate for possible transmission errors. The amount of redundancy added depends on the channel quality as estimated by the eNB.

[0096] The task of the downlink physical-layer hybrid-ARQ functionality 60 is to extract the exact set of bits to be transmitted at each transmission/retransmission instant from the blocks of code bits delivered by the channel coder. Thus, it is also implicitly the task of the hybrid-ARQ functionality to match the number of bits at the output of the channel coder to the number of bits to be transmitted. The latter is given by the number of assigned resource blocks and the selected modulation scheme and spatial-multiplexing order. In case of a retransmission, the HARQ functionality will, in the general case, select a different set of code bits to be transmitted (Incremental Redundancy).

[0097] The downlink data modulation performed by modulators 64_B maps blocks of scrambled bits to corresponding blocks of complex modulation symbols. The set of modulation schemes supported for the LTE downlink includes QPSK, 16QAM, and 64QAM, corresponding to two, four, and six bits per modulation symbol respectively.

[0098] As indicated above, the base station node 28 can also receive Channel Quality Indicator (CQI) reports from the UE, which measures the quality of the DL reception based on a reference signal either per resource block or per group of resource blocks. The UE can also measure and report the observed DL HARQ BLER, which is the block error rate based on CRC check of each HARQ level transport block. The eNB also can receive HARQ ACKs and NACKs for every downlink transmission.

[0099] Functions that determine QoS in shared channel access networks (not only radio) are the following:

(1) Scheduling (UL + DL)

(2) Traffic Conditioning (UL + DL)

- Admission control for GBR bearers
- Rate policing/shaping for GBR and Non-GBR bearers

[00100] Another relevant function that can be implemented in an eNode B is queue management which can be optimized for either real-time or non-real-time traffic.

[00101] Advantageously the technology solves a problem of how to mark (or drop) IP packets in a radio transmitter (e.g. eNB) so that the radio receiver that contributes the most to the congestion can be signaled that the radio network is experiencing congestion.

[00102] In at least some example embodiments, a mechanism such as ECN (marking) or detection or packet losses (dropping) is assumed to be available and to reach the application. It also assumed that the application in the receiver as the means to propagate back feedback to the IP application in the sender. It can be expected that such mechanisms will get deployed in a foreseeable future.

[00103] The technology advantageously handles the logic for marking dropping packets, and is thus a component in a broader solution where congestion can be handled with as little packet losses as possible by enabling the sender of IP packets to adjust its send rate to the radio conditions along the path, as well as to adjust to the usage their IP packets are consuming.

[00104] Without this functionality, there is a fair risk that the impact on the quality of the session media, when congestion occurs, is distributed randomly in an unfair manner and to a larger number of receivers, resulting in a more drastic drop in media quality and user experience.

[00105] With this functionality, on the other hand, the impact of congestion is redistributed to the receivers most responsible for the congested state, in a manner that is fairer than by randomly marking or dropping packets based on e.g. queue state in the transmitter.

[00106] Although the description above contains many specificities, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments. Therefore, it will be appreciated that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art. Reference to an element in the singular is not intended to mean "one and only one" unless explicitly so

stated, but rather "one or more." All structural, chemical, and functional equivalents to the elements of the above-described preferred embodiment that are known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed hereby. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved or described herein.

WHAT IS CLAIMED IS:

1. A method of operating a communications network comprising:
detecting congestion of a shared radio resource;
characterized by:
for a user of the shared radio resource, selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

2. The method of claim 1, wherein the user's share is expressed in terms of cost or amount of resources associated to a user.

3. The method of claim 2, further comprising determining the cost, or the amount of resources associated to the user, based on transmitter measurements.

4. The method of claim 3, wherein the transmitter measurements include at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate.

5. The method of claim 2, further comprising determining the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements.

6. The method of claim 5, wherein the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

7. The method of claim 1, further comprising determining the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality

indications; handover measurements; and, the type of modulation and coding scheme used for the user.

8. The method of claim 1, further comprising selectively dropping the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

9. A node (28) of a communications network comprising:

a transceiver (68B) configured to transmit a shared radio resource to a user;

characterized by:

a packet marker (56) configured, upon detection of congestion of the shared radio resource, to selectively drop packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

10. The node (28) of claim 9, wherein the user's share is expressed in terms of cost or amount of resources associated to a user.

11. The node (28) of claim 10, wherein the packet marker (56) is configured to determine the cost, or the amount of resources associated to the user, based on transmitter measurements.

12. The node (28) of claim 11, wherein the node (28) is configured to use transmitter measurements including at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate.

13. The node (28) of claim 10, wherein the packet marker (56) is configured to determine the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements.

14. The node (28) of claim 13, wherein the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

15. The node (28) of claim 9, wherein the packet marker (56) is configured to determine the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality indications; handover measurements; and, the type of modulation and coding scheme used for the user.

16. The node (28) of claim 9, wherein the packet marker (56) is configured to selectively drop the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

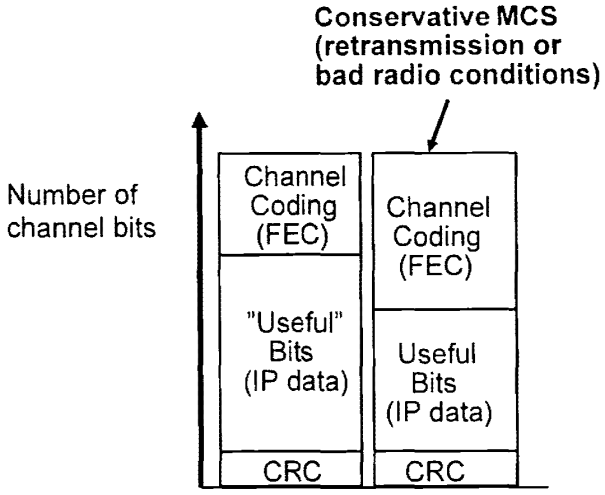

Conservative MCS
(retransmission or
bad radio conditions)
Number of
channel bits
Channel
Coding
(FEC)
"Useful"
Bits
(IP data)
CRC
Channel
Coding
(FEC)
Useful
Bits
(IP data)
CRC

FIG. 1

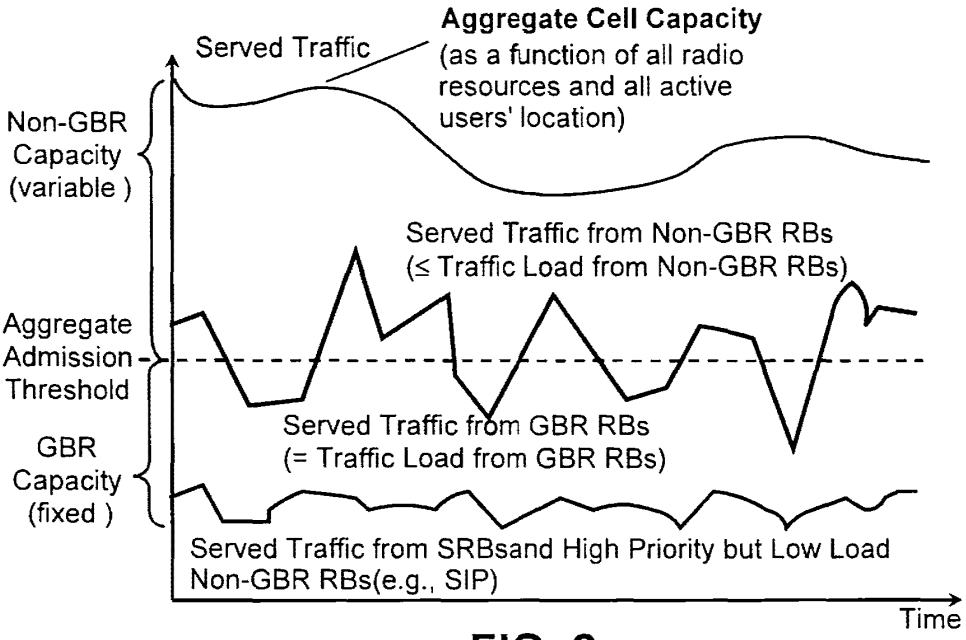

Served Traffic
Aggregate Cell Capacity
(as a function of all radio
resources and all active
users' location)
Non-GBR
Capacity
(variable)
Served Traffic from Non-GBR RBs
(≤ Traffic Load from Non-GBR RBs)
Aggregate
Admission
Threshold
GBR
Capacity
(fixed)
Served Traffic from GBR RBs
(= Traffic Load from GBR RBs)
Served Traffic from SRBsand High Priority but Low Load
Non-GBR RBs(e.g., SIP)
Time

FIG. 2

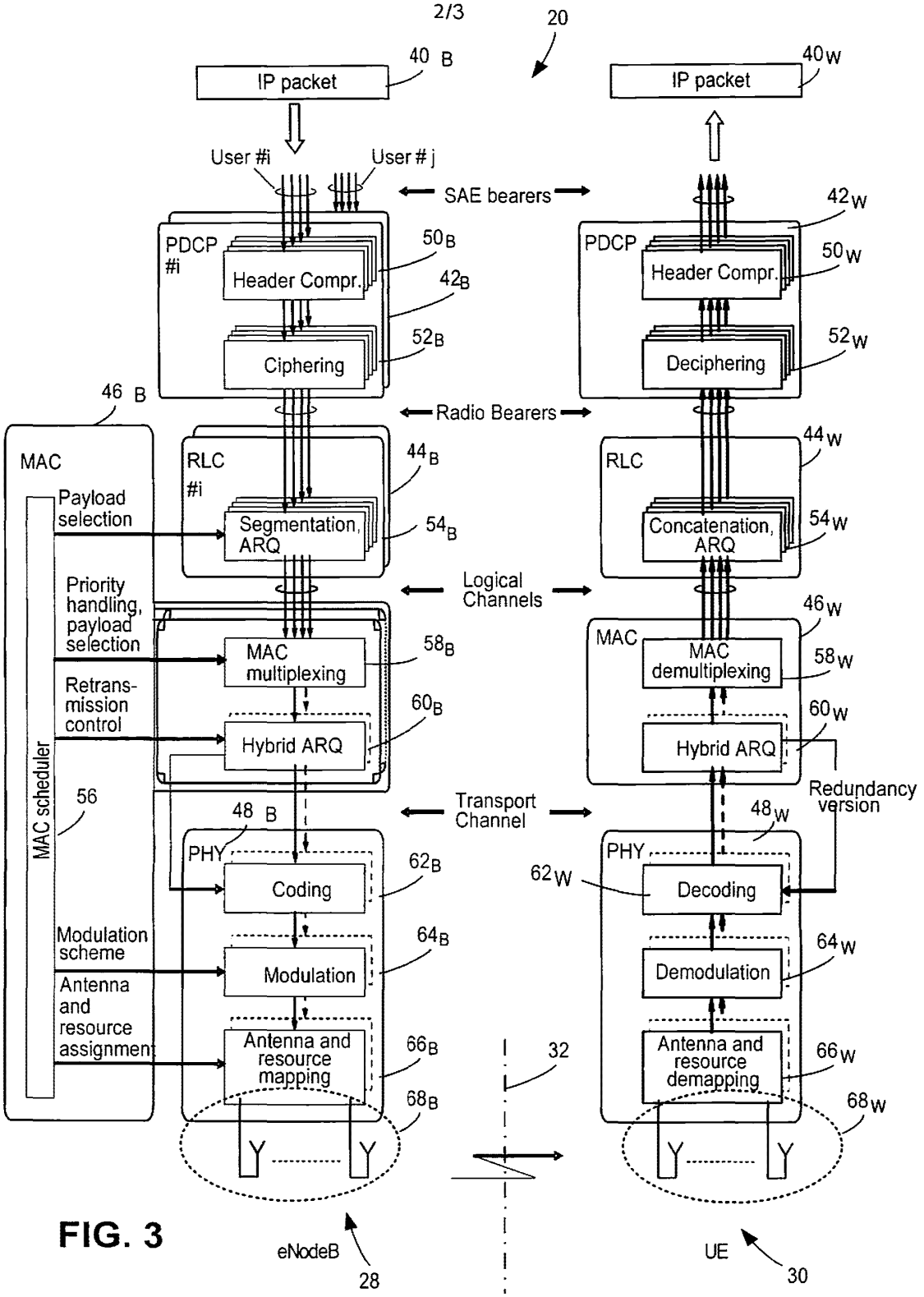

20
IP packet
40 B
IP packet
40W
User #i
User # j
SAE bearers
42W
PDCP
#i
50B
Header Compr.
42B
PDCP
50W
Header Compr.
52B
Ciphering
52W
Deciphering
46 B
Radio Bearers
MAC
RLC
#i
44B
RLC
44W
Payload selection
Segmentation, ARQ
54B
Concatenation, ARQ
54W
Priority handling, payload selection
Logical Channels
46W
MAC
MAC multiplexing
58B
MAC demultiplexing
58W
Retrans-mission control
Hybrid ARQ
60B
Hybrid ARQ
60W
Redundancy version
MAC scheduler
56
Transport Channel
48 B
48W
PHY
PHY
62B
Coding
62W
Decoding
Modulation scheme
64B
Modulation
64W
Demodulation
Antenna and resource assignment
Antenna and resource mapping
66B
32
Antenna and resource demapping
66W
68B
68W
eNodeB
28
UE
30

FIG. 3

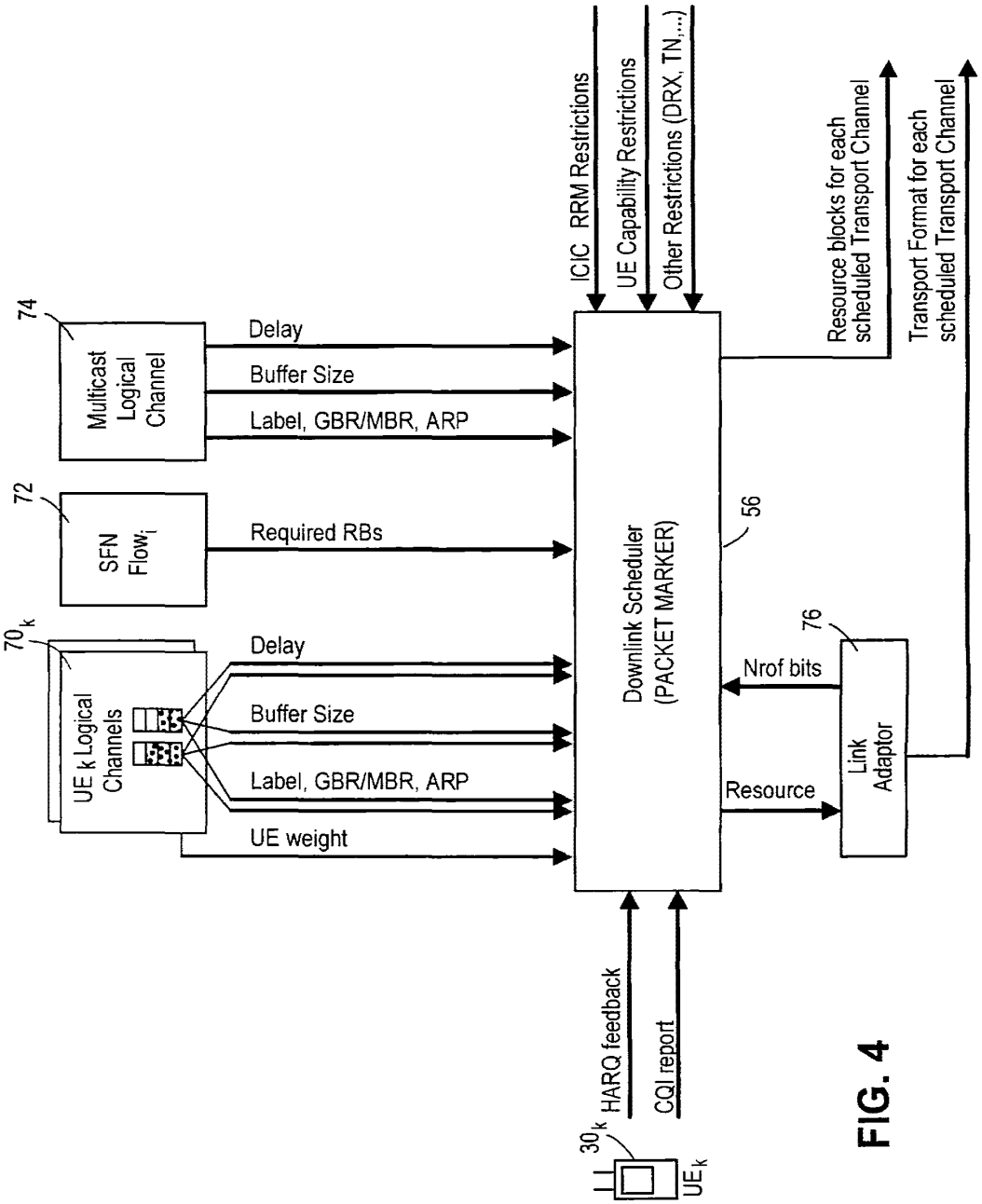

ICIC RRM Restrictions
UE Capability Restrictions
Other Restrictions (DRX, TN,...)
Resource blocks for each scheduled Transport Channel
Transport Format for each scheduled Transport Channel
74
Multicast Logical Channel
Delay
Buffer Size
Label, GBR/MBR, ARP
72
SFN Flow$_i$
Required RBs
70$_k$
UE k Logical Channels
Delay
Buffer Size
Label, GBR/MBR, ARP
UE weight
Downlink Scheduler (PACKET MARKER)
56
76
Nrof bits
Resource
Link Adaptor
HARQ feedback
CQI report
30$_k$
UE$_k$

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050830

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20030086413 A1 (TARTARELLI, S ET AL), 8 May 2003 (08.05.2003), claims 1-28, abstract, paragraphs [0005]-[0047]	1-7,9-15
Y		8,16
	--	
P,X	US 20080101354 A1 (ARNDT, M R), 1 May 2008 (01.05.2008), figure 4, claims 1-21, abstract, paragraphs [0021]-[0029]	1-16
	--	
Y	EP 1365545 A1 (SIEMENS AG), 26 November 2003 (26.11.2003), abstract, paragraphs [0118]-[0124]	8,16
A		1-7,9-15
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2008	19 -11- 2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Elisabet Åselius /LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050830

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02098153 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 5 December 2002 (05.12.2002), page 7, line 13 - page 13, line 5; page 20, line 1 - page 23, line 15, claims 1-29, abstract -- --------	1-16

Form PCT/ISA/210 (continuation of second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.

International patent classification (IPC)
H04L 12/56 (2006.01)
H04L 12/26 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **OVTXPKETAA**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

Form PCT/ISA/210 (extra sheet) (July 2008)

US	20030086413	A1	08/05/2003	DE	10220213	A	27/03/2003
				JP	4032231	B	16/01/2008
				JP	2003087316	A	20/03/2003
US	20080101354	A1	01/05/2008	NONE			
EP	1365545	A1	26/11/2003	NONE			
WO	02098153	A1	05/12/2002	AT	410892	T	15/10/2008
				EP	1391128	A,B	25/02/2004
				EP	1876779	A	09/01/2008
				GB	0113214	D	00/00/0000
				GB	2372172	A,B	14/08/2002
				US	20040218617	A	04/11/2004

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/45315 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US01/43140

(22) International Filing Date:
21 November 2001 (21.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/724,025 28 November 2000 (28.11.2000) US

(71) Applicant: **MICROMUSE INC.** [US/US]; 139 Townsend Street, 5th Floor, San Francisko, CA 94107 (US).

(72) Inventors: **HERRING, David**; 45 Church Road East Crowthorne, Berkshire RE45 7ND (GB). **CARROLL, John, D.**; 4543 North O'Connor Road, Apt. 1249, Irving, Texas 75062 (US). **O'GRADY, Rehan**; Basement Flat, 32 Addison Avenue, Hollamd Park, London W11 4QR (GB). **COLEMAN, Neil**; 40 Belle Vue Road, Quary Bank, West Midlands DY5 1AD (GB). **MARKS, Felix**; 251 Mayall Road, London SE24 OPQ (GB).

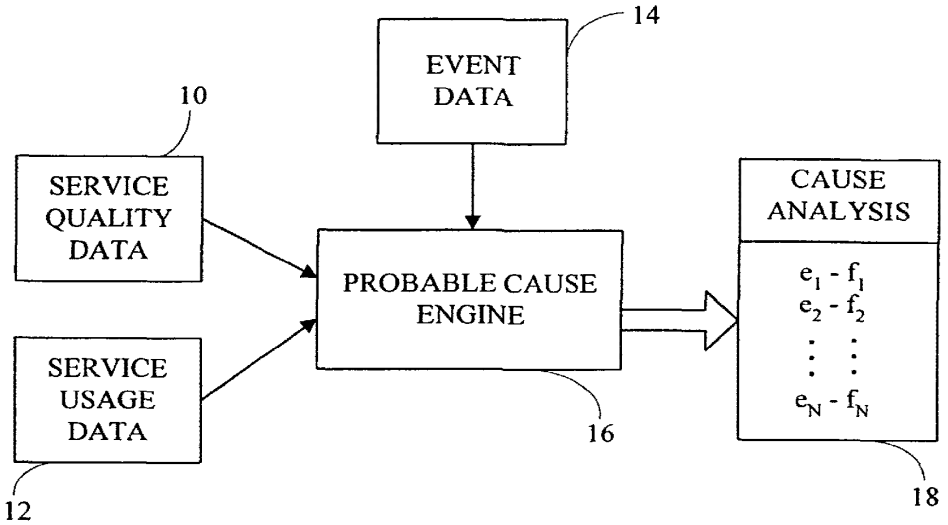
(74) Agent: **OSTROW, Seth. H.**; Brown Rausman Millstein, Felder & Steiner LLP, 900 Third Avenue, New York 10022 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PREDICTING CAUSES OF NETWORK SERVICE OUTAGES USING TIME DOMAIN CORRELATION



(57) Abstract: Method and system are described for predicting the likely causes of service outages using only time information, and for predicting and the likely costs of service outages. The likely causes are found by defining a narrow likely cause window around an outage based on service quality and/or service usage data, and correlating service events to the likely cause window in the time domain to find a probability distribution for the events. The likely costs are found by measuring usage loss and duration for a given point during anoutage and using cost component functions of the time and usage to extrapolate over the outage. These cause and cost predictions supply service administration with tools for making more informed decisions about allocation of resources in preventing and correcting service outages.

WO 02/45315 A2

GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (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.

METHOD AND SYSTEM FOR PREDICTING CAUSES OF NETWORK SERVICE OUTAGES USING TIME DOMAIN CORRELATION

COPYRIGHT NOTICE

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND OF THE INVENTION

The invention disclosed herein relates to the field of fault event correlation and assessment in computerized services such as telecommunications networks or application programs. More particularly, the invention relates to methods, systems, and software for determining likely causes of service outages and assessing the costs of the service outages. The invention described herein is useful in correcting service outages, preventing future occurrences of similar service outages, and determining the appropriate level of resources which should be allocated to correct and prevent such outages.

Maintaining the proper operation of various types of computerized services is usually an important but difficult task. Service administrators are often called upon to react to a service failure by identifying the problem which caused the failure and then taking steps to correct the problem. To avoid wasting resources investigating the wrong problems, administrators must make accurate assessments as to the causes of failures. Because substantial time and resources are often required, administrators must also make accurate decisions as to when to allocate resources to the tasks of identifying problems and fixing them.

A number of tools are available to assist administrators in completing these tasks. One example is the NETCOOL® suite of applications available from Micromuse Inc., assignee of the present application, which allows network administrators to monitor activity on networks such as wired and wireless voice communication networks, intranets, wide areas networks, or the Internet. The NETCOOL suite logs and collects network events, including network occurrences such as alerts, alarms, or other faults, and then reports them to network administrators in graphical and text based formats. Administrators are thus able to observe network events on a real-time basis and respond to them more quickly. The NETCOOL suite

also includes network service monitors of various types which measure performance of a network so that, among other things, network resources can be shifted as needed to cover outages.

Even knowing that events are occurring in real time, however, administrators must still make judgments as to which events are responsible for causing service failures or outages and which service outages are worth the expenditure of resources to fix. Although experienced administrators can usually make reasonably accurate judgments, it is desirable to provide additional application tools which improve the chances that these judgments are accurate.

A number of existing systems attempt to correlate events with service failures. For example, U.S. Patent No. 5,872,911 to Berg describes a system that monitors a telecommunications network for faults and assesses fault data to determine the likely cause of the fault. The system accomplishes this by filtering and reducing the full set of fault data based on a correlation of various faults or alarms. The correlation is performed using a rules-based engine or knowledge base which determines or defines relationships among types of faults. The system then uses the filtered and reduced fault data to determine actual service impact on the network by determining whether a network outage occurred as a result of the fault. The system further determines which customers or equipment are affected by the network outage using conventional mechanisms which track network traffic.

As another example, U.S. Patent No. 5,748,098 to Grace describes a system which uses stored historical data concerning alarms and when they occur to determine the probability of a relationship between events occurring within a window of time. The window of time is either fixed or determined with reference to the nature of the network or the stored historical data. Additional patents, including U.S. Patent No. 5,646,864 to Whitney, U.S. Patent No. 5,661,668 to Yemini, and U.S. Patent No. 6,049,792 to Hart, describe still further schemes for attempting to correlate and relate network faults or alarms using expert systems, logic models, or complex causality matrices.

These patents, which are hereby incorporated by reference herein, describe systems which monitor and attempt to correlate faults in a network. However, among other things, these systems fail to take full advantage of available performance or usage data in correlating events. That is, the inventors have found that a more careful analysis of the level of usage of a service improves the correlation of events to service outages. There is therefore

a need for methods and systems for accounting for service usage information among other data to improve correlation between events and service failures.

Furthermore, there is a need for improved methods and systems for helping administrators make decisions about how to prioritize outages and allocate resources in the correction or prevention of service failures. Commonly assigned application serial no. 09/476,846 and U.S. Patent No. 5,872,911, discussed above, describe different systems for determining the impact of a service failure on customers or users. However, these systems do not quantify the impact in a way to provide the administrator with the ability to compare the effects of outages in different, unrelated services in order to prioritize the allocation of resources, or to perform a strict cost/benefit analysis for the allocation of the resources. Improved methods and systems are thus needed to quantify the cost of a service outage in such a way as to allow the cost to be compared to costs of other service outages in services or systems which may differ in type or use.

SUMMARY OF THE INVENTION

It is an object of the present invention to solve the problems described above with existing network analysis systems.

It is another object of the present invention to improve correlation between events and outages in computerized services.

It is another object of the present invention to improve the correlation without requiring substantive knowledge of the nature of the event and its effect on the service.

It is another object of the present invention to help service administrators make better decisions about how to apply resources to correct service failures.

It is another object of the present invention to quantify the overall cost of a service outage.

It is another object of the present invention to quantify the cost in a way which allows outages in different types of services or systems to be easily compared with one another.

It is another object of the present invention predict the cost of an outage during the outage.

Some of the above and other objects are achieved by a method for analyzing a potential cause of a service change, such as a service outage or service recovery. The method involves monitoring service quality of the service and usage amount of the service, and

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state as well as upon a change in service usage amount. The service change time window encompasses at least part of a service outage, such as the onset or completion of the outage. As used herein, a service outage or failure is intended to include not only total failures and complete losses of service but also reductions in level of a service to a level considered to be unacceptable or requiring corrective action. The method further involves detecting an event and a time in which the event occurred, and computing a probability that the detected event caused the service change based at least in part on a relation between the event time and the service change time window.

The present invention provides a significant improvement over prior attempts to correlate faults or alarms in a number of ways. For example, in certain aspects of the present invention, three items of information are taken - service quality, service usage, and events - and they are correlated in the time domain, based only on their times. In addition, using both the service quality and service usage data to define a service change time window which is likely to contain or near the cause of a service outage the correlation between the detected event and the service outage.

The method is applicable to various types of computerized services, including: telecommunication networks such as voice or data telephony systems, wired or wireless telephony, email, or instant messaging; computer networks such as intranets, extranets, local or wide area networks, or the Internet; and application programs such as web server software, operating systems, financial system software, etc. The method may be implemented in a computer program which is stored on a computer readable medium such as a magnetic or optical disk and is executed to cause the computer to perform the method.

In some embodiments, the service quality is monitored by a service monitor which regularly polls the service to determine a binary classification of the service as either good or bad. Alternatively, the service quality monitor may identify a number of discrete states of the service, and the administrator selects which combination of the states represents a working state versus a non-working state. The service usage amount is measured by a usage meter, which may be part of the service monitor or another component, and which tracks the level of traffic, performance or usage of the service on a substantially continuous basis.

Since in these embodiments the service quality is monitored by polling, a finding of bad service at some point indicates that an outage occurred at some prior point in time after the last monitored level of good. In some embodiments, the service change time window is determined by first defining a service failure time window bounded by successive readings of good and bad service levels, and then narrowing the service failure time window based upon the service usage amount measured during that service failure time window. This combination provides a more accurate time window encompassing the outage and which more likely encompasses or correlates to the event causing the outage.

The probability that the detected event caused the service change may be computed in a number of ways. In some embodiments, one or more weighting functions are used to compute a probability distribution covering events occurring during the service change time window and within a given time period prior to the window. Although the probability distribution could include events occurring a relatively long time prior to the outage, the likelihood that these older events are responsible for the outage exponentially decreases with distance from the time window and at some point are too negligible to be considered. The weighting functions may be combined to produce a combined weighting function. Exemplary weighting functions used in various embodiments of the invention include:

- a time weighting function for each detected event which decreases exponentially with the distance between the detected event occurrence time or times and the service outage time window;
- a false occurrence weighting function for each event which decreases the probability of the event as the cause of the service outage for instances in which an event of the same type occurred outside the service change time window;
- a positive occurrence weighting function for each detected event which increases the probability of the detected event as the cause of the service change based on instances stored in a historical database in which a detected event of the same type occurred within a prior service change time window; and
- a historical weighting function for each detected event which increases the probability of the detected event as the cause of the service outage based

on instances in the historical database in which a detected event of the same type was identified as having caused a prior service change, perhaps by a user or some automated mechanism.

Some of the above and other objects are achieved by method for analyzing potential causes of a service change. The method involves determining a service change time window encompassing a change of service between a first working state and a service outage, the service change being determined at least in part based on measured service usage levels. For example, a service change may be detected by detecting a step change in service usage, without the need to resort to separate service quality data. A set of events occurring within a given time prior to and during the service change time window are detected, each occurrence of an event being associated with a time at which the event occurred. A probability distribution is computed for the set of events, which probability distribution determines for each event in the set the probability that the detected event caused the service change, the probability distribution being based at least in part on relations between the time of each event occurrence and the service change time window.

Some of the above and other objects of the invention are achieved by a network monitoring system having a service monitor for monitoring quality of service on the network, a usage meter for monitoring usage of the network, an event detector for detecting network events and times at which the network events occur, and a probable cause engine, coupled to receive data from the service monitor, usage meter, and event detector. The probable cause engine sets a service outage time window based upon data received from the service monitor and usage meter, the service outage time window encompassing an occurrence of a service outage in the network. The probable cause engine further determines which of the network events detected by the event detector is the most likely cause of the service outage based at least in part on the relation between the detected network event times and the service outage time window.

Some of the above and other objects of the invention are achieved by a method for quantifying the effect of a service outage over a first period of time. The method involves monitoring or measuring levels of service usage over time, defining a cost of outage time window. The cost of outage time window includes the first time period and a second time period following the first time period. The method further involves computing a cost of the outage as the difference between the measured service usage during the cost of outage time

window and service usage measured in a comparison window. The comparison window is substantially equal in time to the time of the cost of outage window and reflects a similar period of service activity as the cost of outage window, but has no service outage.

In some embodiments, the second period of time is the time in which the service usage returns or recovers from the outage to within a given percentage of a normal service usage level. This recovery should last for more than a mere instant to reflect a return to a state of relative equilibrium, as the service usage is likely to fluctuate following the restoration of service. For example, in an email system, a large number of messages may accumulate in the queue while the email system is down, and a this larger number of messages may be conveyed in a short period of time once the system is returned, resulting in very high volumes. In some embodiments, the second period of time is bounded by a maximum time, e.g., a multiple of the time of the outage.

In some embodiments, the cost of outage is computed in units of service usage. What constitutes a unit of usage depends upon the nature of the service. For example, if the service is a communication service conveying messages, such as telephony or email, the unit of usage is one or more messages. If the service is a network server providing data items such as web pages in response to requests such as from clients, the unit of usage may be a received request or data item provided by a server.

Units of usage may be normalized across different services by converting them to a value such as a monetary value, number of users, time value, or other value representing a loss resulting from not receiving the unit of usage. This may be accomplished by multiplying the units of usage by an assigned value of usage per unit. The normalized value of the service outage cost may then be used by administrators or an automated decision making program to compare costs of difference services and prioritize the allocation of resources across the services to prevent or repair service outages.

In some embodiments, the service usage is continuously monitored, including after the end of cost of outage window, and is used to measure the long term effects of the service outage. This is accomplished by computing the difference between the service usage following the cost of outage time window and a normal service usage level. If the service usage is substantially below or above the normal level following the outage, this is an indication that the outage is of the type that causes loss of use of the service, including loss of users.

Some of the above and other objects of the invention are achieved by a method for predicting a cost of an outage of a service such as during the outage itself. The method involves measuring the time duration for and service usage during the outage, and comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs, to thereby determine a usage loss amount. This usage loss amount is used to compute a predicted cost of the outage based at least upon a cost component, the cost component comprising a function of the measured time of the outage and measured usage loss amount. The predicted cost of service outage may be compared to a second predicted cost of outage value for a different service so that outages in the two services may be prioritized based on the compared costs.

In some embodiments, the cost components include a service demand cost component representing an affect on service usage based upon the duration of an outage, a customer retention cost component representing a number or percentage of customers lost due to the outage, an agreement penalty component representing penalties arising under one or more service agreements due to a service outage, and a trust loss component representing empirically collected assessments of cost due to loss of trust in the service. The service demand cost component may be computed by multiplying the measured usage loss by a usage loss curve which is a function of time duration of an outage and represents a predicted percentage usage due to an outage based on time duration of the outage. The usage loss curve may be generated using historical data derived from prior service outages.

The methods and systems of the present invention thus provide a service administrator with the ability to more accurately assess what events are likely to have caused a service outage, without the need to know very much about the nature of the events, and to make a more well informed prioritization of service outages and allocation of resources in correcting or preventing the events and corresponding outages.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like references are intended to refer to like or corresponding parts, and in which:

Fig. 1 is a data flow diagram showing a time-based event correlation methodology in accordance with one embodiment of the present invention;

Fig. 2 is a block diagram showing a service with service level and usage monitors in accordance with one embodiment of the present invention;

Fig. 3 is a block diagram showing a network event correlation system in accordance with one embodiment of the present invention;

Fig. 4 is a flow chart showing a process of correlating events with a service outage in accordance with one embodiment of the present invention;

Fig. 5 is a graphical representation of an exemplary set of service quality data;

Fig. 6 is a graphical representation of an exemplary set of service usage data;

Figs. 7-9 are graphical representations of techniques for defining a likely cause window using service level or service usage data in accordance with embodiments of the present invention;

Fig. 10 is a graphical representation of an exemplary time weighting function in accordance with one embodiment of the present invention;

Fig. 11 is a graphical representation of exemplary outages and events;

Fig. 12 is a table showing a probability distribution for the events shown in Fig. 11 to have caused one of the outages shown in Fig. 11;

Fig. 13 is a graphical representation of a technique for defining a likely cause window for a service recovery using service level or service usage data in accordance with one embodiment of the present invention;

Fig. 14 is a flow chart showing a process of predicting the cost of an outage in accordance with one embodiment of the present invention;

Figs. 15A-15B contain a flow chart showing a process of quantifying the cost of a completed outage in accordance with one embodiment of the present invention;

Figs. 16-19 are graphical representations of techniques for quantifying outage costs in accordance with one embodiment of the present invention;

Figs. 20-22 are graphical representations of exemplary cost of outage analyses performed in accordance with embodiments of the present invention;

Figs. 23-34 are graphical representations of techniques for predicting the cost of an outage during the outage in accordance with embodiments of the present invention;

Fig. 25 is an exemplary usage loss curve as a function of time for use in predicting the cost of an outage in accordance with one embodiment of the present invention; and

Figs. 26-28 are graphical representations of exemplary usage loss scenarios for use in generating a usage loss curve in accordance with one embodiments of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention are now described with reference to the drawings in the Figures.

One goal of these embodiments is to discover the likely cause of a service outage or service recovery by identifying which event or events occurring in the service are most likely to have caused the outage or recovery. For the sake of simplicity, the following description will focus on predicting costs of service outages, but the techniques and system described herein can be applied to service recovery, as explained further below.

Referring to Fig. 1, three sources of data are used to achieve this goal - service level or quality data 10, service usage data 12, and events and timestamps associated with the events 14. A probable cause engine 16 receives these three sources of data and processes them using various heuristics as described herein to build a probability distribution 18 over the events in the system, based on which events are most likely to have caused the outage. In some embodiments, the probable cause engine uses the service level data 10 and service usage data 12 to define a time window, sometimes referred to herein as a Likely Cause Window (LCW), which has a high probability of containing the event which caused the outage. The events 14 are then related to the outage based upon a time domain correlation. By virtue of the probability distribution, the probable cause engine 16 orders the events and assigns a discrete probability to each event, so that a service administrator may more accurately assess which event caused the outage.

Event data 14 consists of a timestamp and identifier for each event. In some embodiments, the probabilistic analysis performed by the probable cause engine 16 relies only on the time and type of an event, and does not involve or require any further knowledge of what a particular event consists of or the nature of the event. For purposes of the description below, an event is often distinguished from an event type. An event generally refers to a single alarm, alert, or fault generated in or detected by the system monitoring the service. The same happening in the service may generate multiple events. An event type, on the other hand, generally refers to the network happening that generated the events. Events 14 having the same identifier all come under the umbrella of a single event type.

In addition, a specific terminology is used herein in which a set, E, is a set of events. Members of this set are referenced with double subscript notation. Several events may, for example, have the same identifier and hence all represent alarms generated by a single event type. An event type is referred to by a single subscript. Different events of a particular type are distinguished with the second subscript. For example, events e_{11} and e_{12} would refer to two events of type e_1. These events have the same identifier but different timestamps. Event e_{11} represents the first chronological event of type e_1 in the set E, event e_{12} represents the second chronological event of type e_1, event e_{21} represents the first chronological event of type e_2 in the set E, and so on.

The service level or quality data and service usage data are collected through any conventional devices depending upon the particular service. For example, referring to Fig. 2, in one embodiment of the invention, a service accessed by a number of end users 22 is monitored by service level monitors 24 as well as usage meter(s) 26. As shown, the usage meter or meters measure the total amount in which the service is used. This measurement will depend upon the nature of the service. For example, in a telecommunication service, the usage meter 26 measures the number of messages being conveyed by the service in an hour or other time period. Such a telecommunication service may include a wireless telephony system using the smart message service protocol, in which the usage meter measures the number of messages conveyed over the system. Similarly, in a computer network, the amount of traffic may be measured over a given period. For a service consisting of an application software program, the usage may be measured in any appropriate manner, such as time spent, number of memory calls over time, number of documents accessed over time, etc.

The service level monitors 24 monitor the status of the service on a polled basis. That is, they poll the service on a regular basis to determine whether the service is working. In some embodiments, this inquiry is binary in nature, resulting in a status of either working or non-working, sometimes referred to herein as a status of good or bad service. Alternatively, the service level monitors 24 may detect several types of service status, and an outage would be defined as desired as a transition from one status in which the service is considered to be working properly to a second status in which it is not providing an acceptable level of service. Multiple discrete service monitors 24 may be used to monitor the quality of service from different locations. For example, for a network accessible from several remotely located sites, each site would have a service monitor 24 to monitor the

quality of service being received at that site, while the traffic on the entire network would be measured by usage meters 26.

As explained further below, the service quality and service usage data are singly or jointly used to detect when an outage has occurred in the service. As used herein, an outage of a service is generally a period or window of time during which positive affirmation of the service being good or acceptable can not be obtained. When an outage is detected by a service monitor 24, for example, an outage time window contains one or more bad polls and is bounded at each end by two good polls. This guarantees that the outage window encompasses the entire outage incident.

One embodiment of the present invention implemented in a computerized network environment is shown in Fig. 3. In this embodiment various activity on a network 30 is monitored by a network monitoring system 32, such as the NETCOOL suite available from Micromuse Inc., as described above. Other commercially available network monitoring systems 32 may be used, as would be understood by one skilled in the art. The network monitoring system 32 works in conjunction with one or more service quality monitors 24, such as Internet Service Monitors, a set of active monitors which work with the NETCOOL suite to provide availability information on Internet service elements including DNS, HTTP, LDAP, POP3, RADIUS, SMTP, and TCP Port Monitoring, or NT Service Monitors, which work with the network monitoring system 32 to collect management events from a network operations center regarding Windows NT environments.

Further, a set of service usage meters 26A, 26B, and 26C work with the network monitoring system 32 to track the amount of activity seen at different locations on the network 30. In particular, in some embodiments service specific usage meters 26A track activity on different services 34 available within the network, including, for example, a cache server, an email server, Radius, HTTP/HTML, LDAP, and other applications and services available to end users over the network 30. Other, network edge usage meters 26B measure activity in and out of the network, including, for example, a usage meter 26B detecting activity at a firewall monitoring application which collects security information, a usage meter 26B at Cisco Net Flow, a usage meter 26B at a PIX firewall, and others as known to those skilled in the art.

Furthermore, network sniffing usage meters 26C, sometimes referred to as snooping agents, capture and listen to packets on the network received at a network interface.

Examples of conventional network sniffing usage meters include Snoop, Etherreal, and Etherfind. Etherfind, for example, examines packets traversing a network interface and outputs a text file describing the traffic. In the file, the text describing a single packet contains values such as protocol type, length, source, and destination. Further packet filtering can be done on the basis of protocol, e.g., IP, ARP, RARP, ICMP, UDP, TCP, and filtering can also be done based on the source, destination addresses as well as TCP and UDP port numbers.

Events are detected by the network monitoring system 32 through probes or similar conventional mechanisms and are stored in an event object server 40. The object server is an object-oriented data repository where information on events is stored, viewed and managed. Events are stored as objects on the server 40 which can be more easily manipulated for processing. A gateway 42 allows a mediator program suite 44 to share the event data stored in the object server 40. The mediator program suite 44 includes the probable cause engine 16 as well as a cost of outage engine 46 for quantifying the effect of an outage, as described in greater detail below. An administrator desktop and user interface 48 allows a network administrator to interact with the mediator 44 and execute the probable cause engine 16 and cost of outage engine 46.

The operation of one embodiment of the probable cause engine 16 is now described with reference to the flow chart in Fig. 4 and the graphical diagrams in Fig. 5-13. Referring to Fig. 4, the probable cause engine receives service quality data from service quality monitors and service usage data from the service usage meters, step 60. This received data is used to detect the occurrence of an outage, step 62. When an outage is detected, the probable cause engine defines a time window, sometimes referred to herein as the likely cause window or LCW, using the service quality data, service usage data, or preferably both, step 64. The probable cause engine then retrieves event data from the event object server for events which occurred during the defined likely cause window and for a period prior to the LCW, step 66. The events retrieved are each assumed to have a non-zero probability of having caused the outage, and it is further assumed that at least one of the retrieved events caused the outage. The engine then computes a probability distribution for the events which maps the probabilities that each event caused the detected outage, step 68. These probabilities are then associated with the events and output to the administrator in a suitable form.

Particular implementations of steps in this methodology are now described with reference to the graphs shown in Figs. 5-12. Figs. 5 and 6 illustrate sample data sets for service quality and service usage, respectively. As shown in Fig. 5, service quality data consists of a series of points 80 regularly spaced at points in time. As shown, the service quality is monitored at one of two levels or states - good and bad - although a number of quality states might be detected. The classification of a quality state as good or bad is defined in the service monitor configuration by its discrete measurement classification. For purposes of simplicity in this application, it is understood that a transition from one of such states to another of such states is considered to represent a failure or outage in the service, with the definition of what loss of service constitutes an outage being a design consideration.

Fig. 6 shows service usage data consisting of a greater number of points measured on a significantly more continuous basis. The service usage data points may be measured on an entirely continuous basis, e.g., every email message conveyed or every HTTP request is counted, or sufficient samplings of usage may be taken to accurately represent the actual usage of the service.

As explained above, the service quality and service usage data are used to detect outages and define the likely cause window. For purposes of this discussion, time windows are understood to generally cover continuous subsets of the time line. In the notation used below, square brackets denote inclusion of endpoints in the subset, while round brackets mean the end point is not included. For example, given two times a and b, a window (a,b] denotes a time window starting but not including time a and ending at and including time b. In addition, for an event e, and a window, W, the notation $e \in W$ indicates that the timestamp associated with event e falls within the window W.

Figs. 7 and 8 illustrate two ways in which outages are detected and the likely cause window is defined. One method of detecting an outage is through the service quality data received from a service monitor. As illustrated in Fig. 7, when a poll of the service monitor registers as bad for the first time following one or more pollings of good quality, the probable cause engine interprets that the service went bad at some stage between the current bad poll and the previous good poll. The time window between these two polls is defined as the service failure window or SFW. In the diagram in Fig. 7, the SFW is the set (b,c]. The time period between two readings of good in the service quality data in which one or more bad quality readings are monitored is defined as the outage window. In Fig. 7, the outage

window is the set (b,e). As described in greater detail below, the outage window is used among other things by the cost of outage engine to predict the cost of the outage and to quantify the cost of the outage in terms which may be compared to other service outages for purposes of prioritizing the application of resources in response to the outages.

In the absence of further information, the probable cause engine defines the LCW as the SFW plus a small, preset time tolerance consisting of the windows [a,b] and [c,d]. The LCW thus represents [a,d] in the diagram in Fig. 7. Alternatively, the time tolerances are set to zero, in which case the LCW = the SFW.

Alternatively, the probable cause engine detects an outage using only the service usage data, without necessarily resorting to the service quality data. In this embodiment, illustrated in Fig. 8, the engine detects a usage step change and verifies based on the step change whether the service has gone bad. To detect a usage step change, the probable cause engine detects a changepoint in a univariate time series, the time series consisting of the discrete measurements of units of usage. If a change in the service quality has already been detected by a service monitor, the SFW is defined as explained above as the period during which the service outage started. The usage step change is found in this window using an offline changepoint detection algorithm. Some such algorithms are described in Booth, N.B. and Smith A.F.M. *A Bayesian approach to Retrospective Identification of Change Points*, J. Econ., 19, (1982), which article is hereby incorporated herein by reference. If service quality data is not available, the probable cause engine analyzes the service usage data itself to detect an outage. This analysis employs an online changepoint detection algorithm. Some online changepoint detection algorithms are described in Basseville, M and Nikiforov, I.V., *Detection of abrupt Changes, Theory and Applications*, Prentice Hall, Englewood, New Jersey (1993), which article is also incorporated by reference herein.

As with an outage detection based on service quality change alone, the LCW may be defined by the probable cause engine as the time window from briefly before the usage step change up to and including the step change. However the outage is detected, clearly getting a tight bound on when the actual outage occurred is important to determining which event caused the outage. The smaller the LCW, the more likely it is that the probable cause engine will be able to pinpoint the event which caused the outage. Preferably, the

LCW should be the smallest time window that can reasonably be specified in which the data indicates the outage occurred.

In some embodiments, then, the probable cause engine uses the usage step change to provide a tighter bound on a SFW previously established using service quality data. As above, a service monitor detects that the service quality has gone bad. With the addition of usage data, however, the probable cause engine puts a much tighter bound on the SFW to produce a narrower LCW. This is illustrated in Fig. 8, in which the service quality data of Fig. 7 is shown in conjunction with usage data. It will be recognized by one skilled in the art that, for purposes of comparing the two types of data and graphing them together in Fig. 8 and later drawings, either or both of the service quality data and service usage data have been normalized. The probable cause engine analyzes the usage data for the time period within the SFW found through the service quality data and detects a usage data step change. The LCW is then defined as the period of the step change plus time tolerances.

As a result, in some embodiments the definition of the likely cause window is based on the service quality and service usage data received regarding a specific service. In other embodiments, the probable cause engine considers outages in other services to achieve a more refined definition of the service failure window and ultimately the likely cause window. This is based on a theory that the cause of an outage under consideration often causes outages in other, related services. Thus, referring to Fig. 9, the engine identifies related services as services experiencing an outage whose service failure window overlaps with the service failure window for the outage under consideration. Alternatively, the engine can use stored information about the relatedness of various services, e.g., a knowledge base or expert system. The engine then superimposes the service failure window for the main or principle service with service monitor or usage meter data received regarding the related services. This results in a smaller composite service failure window, as shown in Fig. 9, and thus improves the probable cause analysis. If the probable cause engine is performing the analysis on a service which has recovered, as described below, then a similar condition can be applied to the corresponding service recovery window.

Once the probable cause engine identifies a likely cause window, it retrieves event data defining a set of events and builds a discrete probability distribution function, P, such that for any event, e, the probability that this event caused the service outage is $P(e)$. The probability distribution, P, is based on heuristic observations of cause and effect. While

many suitable heuristics will accomplish the task, four heuristics are described below, one for each criterion included in the model. In some embodiments, each heuristic can be considered on its own. Alternatively, two or more of these four heuristics are incorporated by means of mathematical weighting functions. A probability is assigned to each event type, rather to each individual event.

A first heuristic is a time weighting function T(e). This function reflects the heuristic that events in the outage window are much more likely to have caused the service outage than events outside it. Indeed, the probability assigned to events outside the outage window should decay as we move further away from the outage window.

A second heuristic is a false occurrence weighting function FO(e). This function reflects the heuristic that if an event appears many times in the retrieved set of events E, while the service was good, this event is less likely to have caused the outage. The more times an event has occurred outside of any outage window, the less probability is assigned to it.

A third heuristic is a positive occurrence weighting function PO(e). This function reflects the heuristic that the more previous outage windows an event has appeared in, the greater the probability that it has caused the current outage. The use of this heuristic requires the storage of event and outage data for reuse in later analyses.

A historic or user input weighting function U(e) reflects information provided by users of the system in the past, as stored in a database. If a user of the system has, in the past, associated a previous outage with a particular event, then this event is assigned a much higher probability. The more times an event has been associated with previous outages (by a user), the higher the probability is assigned to it.

An overall weighting function F(e) is defined as follows:

$F(e) = T(e) * FO(e) * PO(e) * U(e)$

In building the distribution, the probable cause engine computes the distribution such that the sum of all the probabilities for each of the different events is 1, i.e., if the set of events, E, contains n events, $e_1, \ldots, e_n$, then Sum(P(e1), ... , P(en)) = 1. The engine accomplishes this by discounting each of the individual weights by the sum of all the weights. Thus an event, e, has probability

$$P(e) = \frac{F(e)}{\sum_{i=1}^{n} F(e_i)}$$

And as required,

$$\sum_{i=1}^{n} P(e_i) = 1$$

Exemplary weighting functions used by the probable cause engine are now described. As will be understood by one skilled in the art, other weighting functions may be used within the spirit of the present invention to achieve a probabilistic time domain correlation of events and outages.

For the time weighting function, a certain constant weighting, K, is assigned to events inside the LCW. The function models an exponential decay in the weighting assigned to events, decreasing as events occur further away from the LCW. Let e_{ij} be an event, and let [a,d] define the LCW on a timeline. Let *t* be the minimum absolute distance from the event e_{ij} to an endpoint of the LCW. If e_{ij} is in the LCW, then t =0. $T(e_{ij})$ is thus defined as follows:

$T(e_{ij}) = K$ If $a \leq \text{timestamp}(e_{ij}) \leq b$

$T(e_{ij}) = K*2^{-t/(d-a)}$ If $\text{timestamp}(e_{ij}) < a$

$T(e_{ij}) = K*2^{-2t/(d-a)}$ If $\text{timestamp}(e_{ij}) > b$

This choice of $T(e_{ij})$ assigns a weighting of K/2 to an event occurring at time a - |LCW|, and a weighting of K/4 to an event occurring at time b + |LCW|. The time weighting function for an event of a given type is then defined as the maximum over all the events of that event type, or

$T(e_i) = \max_j (T(e_{ij}))$

A resulting time weighting function having exponential decay is illustrated in Fig. 10.

For the positive occurrence weighting function, defining posOcc(e) as the number of previous occurrences of events of this type inside LCWs, the function may be defined as follows:

PO(e) = 1 if posOcc(e) = 0

PO(e) = 2 if posOcc(e) = 1

PO(e) = 4 if posOcc(e) ≥ 2

An alternative definition of this function is:

PO(e) = 1 if posOcc(e) = 0

PO(e) = posOcc(e)*1.5 if posOcc(e) > 0

For the false occurrence weighting function, defining negOcc(e) as the number of previous occurrences outside any outage windows, i.e., during periods of good service uninterrupted by outages, the false occurrence weighting function can be defined as:

$FO(e) = 1$ if $negOcc(e) = 0$

$FO(e) = 1/2$ if $negOcc(e) = 1$

$FO(e) = 1/4$ if $negOcc(e) \geq 2$

An alternative definition of this function is:

$FO(e) = 1$ if $negOcc(e) = 0$

$FO(e) = 1/(negOcc(e)*1.5)$ if $negOcc(e) > 0$

For the historic or user input weighting function, defining userPrevSelected(e) as the number of times events of this type have previously been selected by a user as having caused an outage of this service, the function may be defined as

$U(e) = 1$ if $userPrevSelected(e) = 0$

$U(e) = userPrevSelected(e)*4$ if $userPrevSelected(e) > 0$

Thus, using these exemplary weighting functions, the probability distribution is performed in the time domain, relying only on the temporal relation of events to the likely cause window containing the outage. The invention thus advantageously avoids the need to take into account of the nature of an event, but only needs to consider its timestamp and identifier. As will be recognized by one skilled in the art, this information and previous user knowledge may be incorporated to add more sophisticated weighting to the probability distribution performed by the probable cause engine. For example, the engine may account for where on the network an event occurred or on which type of device.

The understanding of the invention will be enhanced through an example. The service quality data and event data for the example is illustrated in the diagram in Fig. 11. The probable cause engine is concerned with the second of the two service outages shown in the Figure, and is trying to find the most probable cause for this second outage. The set of events, E, contains eight event types (event types e_1-e_8) and fourteen instances of events. The engine retrieves stored data showing that a user previously nominated event type e_2 as the cause of a previous outage of this service. Applying the functions provided above, the probable cause engine determines a probability distribution as shown in the table in Fig. 12, where the event types are ordered on the probability of having caused the outage. The table

in Fig. 12 also shows how the different weighting functions have influenced the probability assigned to each event type.

The probable cause engine can also be used in a similar manner to that previously described to identify the resolution of a service and predict its likely cause. To predict service resolution a service quality change is detected by a service monitor and/or a usage change showing the service changing from a non-working state such as an outage to a good status. From this, a service recovery window (SRW) is defined, as illustrated in Fig. 13. A likely recovery window (LRW) is initially defined as the SRW plus a small preset time tolerance, or using any of the other techniques for leveraging service usage data as described above. Then, in a similar manner as previously described for service failure, the LRW can be refined based upon current usage data for the service and sympathetic services which have overlapping LRW's. A series of weighting functions can similarly be applied to the events to assign probabilities as to which event caused the service to recover.

This service recover analysis is useful, among other things, within systems which have auto-correction with discrete devices or in which changes are being made to devices independent of the knowledge of the service outage - which nevertheless are service effecting.

Using these algorithms, the probable cause engine identifies the most likely cause(s) of a service outage or service recovery. This helps network administrators identify these events as ones which should be prevented or more quickly fixed to minimize the likelihood of future outages, or to identify events which work towards correcting outages sooner to enhance the chances of a quicker service recovery. However, when outages in different services, or the events that are likely to cause them, occur at around the same time, administrators need to prioritize the outages or events to properly allocate resources. The cost of outage engine in the mediator assists the administrator in this evaluation.

The cost of outage engine, sometimes referred to herein as a costing engine, relies on historical service usage data for a service stored in a database accessible to the mediator. The cost of outage engine analyzes the usage which takes place over a window of time which incorporates a service outage with comparison to the usage which has taken place during a similar comparison window of time without a service outage. This comparison is used to predict or calculate a loss in service usage due to this outage. This is then recalculated as a monetary loss by applying a value to the usage of the service. This

quantifies the motivational factor for fixing a current outage and the motivational factor for ensuring a previous outage is not repeated. The cost of outage engine performs its analysis during a service outage and retrospectively for a previous service outage.

Referring to Fig. 14, as explained above the service quality monitors regularly poll the service for quality level and the service usage meters continuously measure the activity in a service, step 84. If a service outage is detected, step 86, based on the service quality or service usage data using techniques described above, the costing engine predicts the cost of the outage based on the current outage window length, for current outages, and including various extended outage windows for completed outages, step 88. The use of window lengths to predict and compute outage costs is described in greater detail below. Once a predicted cost is computed, it is compared to the outage costs determined for other services, step 90. This comparison may then be used to prioritize outages and allocate resources to the service outages, step 92.

As a result, the costing engine both predicts costs of ongoing outages and computes costs for completed outages which have at least partially recovered. Because the prediction of outages is based in part on historical computations of outage costs, specific techniques for computing outage costs for completed outages are described first, followed by specific techniques for predicting costs of an outage during the outage.

Turning first to computing outage costs, and referring to Figs. 15A-15B, the service quality monitors regularly poll the service for quality level and the service usage meters continuously measure the activity in a service, step 100. For purposes of this aspect of the invention, the usage meters preferably measure the usage in units of usage. The unit of usage varies according to the service being measured, and is typically measured over a timed interval. For example, a unit of usage for a web server is the number of hits on the web server in a minute; for an email server, the number of emails sent and received by a company per hour; for a mobile telephone service, the number of mobile phone calls made by an individual per hour.

If a service outage is detected as completed, step 102, using techniques described above for detecting the onset of an outage and its at least partial recovery, an outage window is defined using the service quality data and/or service usage data, step 104. For example, as described above, the outage window may be defined as the period between two service quality readings of good service with one or more bad quality readings in between.

The cost of outage engine then defines an extended window which includes the outage window and a second time window, step 106. This extended window is referred to herein as a cost of outage window. The cost of outage window is the time span over which the usage data is considered for any given outage, with the goal being to analyze the usage data over a period corresponding to that which incorporates all the effects of the outage on usage patterns. The cost of outage window thus extends beyond the bounds of the outage window to pick up the recovery in usage, subsequent to the outage.

The cost of outage window is limited to a time frame around the outage, and in some embodiments is initially defined in terms of a time span equal to a multiple of outage windows in duration, starting at the same time as the outage. In one embodiment, the cost of outage window is set equal to four times the outage window in length, starting at the same time the outage window begins and continuing for three outage windows duration past the end of the outage window. This is illustrated in Fig. 16.

In accordance with the invention, the cost of outage window can be reduced from the full window if the time to recover occurs within this window. Thus, returning to Fig. 15A, the cost of outage engine determines whether the service recovered during the extended cost of outage window, step 108. The cost of outage engine determines a recovery as the return to "normal" service usage, with normal service varying and being service specific. In some embodiments, a recovery occurs when the units of usage are within 75% - 90% of the same units of usage for the comparison window, explained further below. In other embodiments, a recovery is considered to occur when the units of usage remain within a range of plus or minus 20% of the comparison window's usage value for a sustained period equal to 1/4 the outage window in length, as illustrated graphically in Fig. 17.

If the service usage does not recover within the cost of outage window, the cost of outage window is defined as the full, extended cost of outage window, e.g., four times the outage window, step 110. If the service usage recovers during the cost of outage window, the cost of outage window is shrunk to end at the recovery time, step 112, i.e., the cost of outage window is set at the outage window plus the time to recover. This shortening of the cost of outage window to the time to recover is illustrated in Fig. 18.

Once the cost of outage window is set, the cost of outage engine defines a comparison window, step 114, as having a time period equal in length to the cost of outage window and chosen to reflect a similar period of activity as would have occurred during the

cost of outage window, had there not been an outage. The definition of the comparison window typically takes into account the cyclic nature of service access, and is typically the same period of time for the previous day/week/month or year. In most corporate services this is the previous week. The cost of outage engine then retrieves the service usage data collected and stored for the defined comparison window, step 116.

The measured usage data for the current cost of outage window is then compared to the retrieved usage data for the comparison window, step 118. This comparison yields several important items of information. For example, the cost of outage engine uses this comparison to compute a percentage peak usage, as the highest percentage units of usage recorded during the cost of outage window when calculated as a percentage against the comparison window. This can be used as a measure of demand for a service after an outage has occurred, i.e., a service usage overshoot. In addition, the cost of outage engine can compute a percentage minimum usage as the minimum units of usage recorded during a cost of outage window, computed in one embodiment as a percentage based upon the previous service usage in the comparison window. This computed comparison can be used as a measure of how complete the service outage was. These two computed values are illustrated on the usage data shown in Fig. 19.

A primary purpose of comparing the service usage data in the cost of outage window is to determine the effect of the outage on overall service and users. Thus, returning to Fig. 15B, the cost of outage engine compares the usage data in the two windows to determine whether any loss of usage occurred, step 120. This comparison is performed as the difference over the cost of outage window compared the comparison window. If the difference is zero or negligible, the cost of outage engine determines that loss of service usage occurred, and that the service made a full recovery, step 122. Otherwise, the engine computes the loss of service, step 124.

In addition, the cost of outage engine analyzes the usage data at the instance at the end of the cost of outage window to normal levels as represented in some embodiments by the levels depicted in the comparison window, step 126, and determines the difference, step 128. This difference in actual and expected service usage at the end of the cost of outage window, sometimes referred to herein as percentage churn, is considered as a measurement of the long term effect of this outage. For example, this computed difference may be used as an indication of the loss of users to the service, perhaps because of the increased difficulty in

accessing the service or lost opportunity. The units of usage in the percentage churn is converted to a number of users by dividing the usage units by a conversion factor representing a number of usage units per user. This calculated number of users may then be converted to cost by multiplying the number of users by a factor representing a set cost per user.

In order to make the loss of usage valuable as a tool to compare various types of service outages, the loss of usage and related computed values must be normalized against different services. This is accomplished by applying a value of usage weighting, where the value of usage represents, for example, the monetary loss to an organization for not achieving a given unit of usage. This may vary as a function of time, the individual or group attempting that unit of usage, etc. The cost of usage is computed, step 130, by multiplying the loss of usage by a set value of usage represents the monetary cost of the outage. Once the usage values are normalized, the cost of outage engine can compare the costs of two or more outages, for example, outages which may be overlapping, and prioritize them based on cost.

This aspect of the invention would be better understood by the application of this methodology to several examples of service failure. In the first example, a momentary (e.g., less than one minute) loss of service is detected for a corporate email service. As shown in Fig. 20, the time to recover defines and shortens the cost of outage window, and there is a service overshoot as a result of the pent up demand caused by a small time of outage. One can infer a stickiness for different services in the likelihood of a user returning to use the service after a service outage. Many factors effect the stickiness of a service, such as alternative options, importance of service to user, etc. Ideally, from a service usage perspective, a service overshoot should equal the loss of usage area, meaning that effectively there was zero loss in service usage as a result of this small service outage. There is no percentage churn as the time to recover defines the cost of outage window.

In a second example, a corporate web service fails for a medium period (e.g., less than three hours). As illustrated in Fig. 21, the cost of outage engine finds a definite loss in usage of the service, showing that any intended usage of the service during the outage has not been carried forward to when the service was restored. However the usage has recovered to show no overall percentage churn.

In a third example, an e-commerce web service fails for a relatively long period (e.g., one day). As illustrated in Fig. 22, the cost of outage engine finds effects of the

outage lasting beyond the cost of outage window, giving a percentage churn value of approximately 50%.

As described herein, the cost of an outage is thus determined based on three basic factors - the type of service, the length of the outage window, and the time the outage occurred.

The description turns now to techniques used by the cost of outage engine for predicting the total cost of an outage during the outage based on a given outage length. This cost prediction may be used, among other things, to assess the priority of allocating resources to fix this outage. In some embodiments, the prediction of service outage cost is based on the results of a combination of outage costing components. Each costing component is a function that returns a cost when given an outage length among other possible variables. Each costing component model a particular way an outage can cost money.

In some embodiments, the costing components include the following:

- a component modeling service demand behavior in relation to the length of service outage, covering the short to medium term effects of a service outage and derived from empirical observation, represented herein as C_d;
- a component modeling level of customer retention in relation to the length of outage, represented herein as C_r;
- a component modeling penalty clauses in service level agreements (C_p); and
- a component modeling loss of trust in the service or the company providing the service, based upon historical or empirical data, represented herein as C_t.

Each costing component produces a monetary cost using some or all of the following data: length of outage, usage levels at time of outage, historical usage trends, and empirical knowledge. The total monetary cost C is a sum of the component costs:

$$C(\text{outage}) = C_d(\text{outage}) + C_r(\text{outage}) + C_p(\text{outage}) + C_t(\text{outage})$$

The Service Demand component embodies how the length of outage affects the short to medium term usage of a service. The two diagrams in Figs. 23 and 24 illustrate the anatomy of an outage. The measured usage during an outage determines the severity of the outage. A complete outage results in no measured usage. Usage measured during an outage is treated as fulfilled demand, and the usage loss is measured as the difference

between expected or normal usage as determined, for example, by service usage during a comparison window, and the measured usage, as shown in Fig. 23. The service demand component aims to derive a cost for all usage loss attributable to the given, current outage. The loss of usage includes usage lost in the outage window as well as predicted usage lost and regained during the recovery period, as shown in Fig. 24.

The costing engine computes the service demand cost component using a Usage Loss Curve. For purposes of this discussion, it should be understood that usage loss refers to the absence of usage, either measured or projected, as compared to usage measurements for a comparable period, and total usage loss for an outage refers to the combined usage loss from both the outage window and the recovery period.

An example Usage Loss Curve is shown in Fig. 25. The horizontal axis represents outage window length, that is, the measured duration of the outage. The vertical axis represents total usage loss as a percentage of usage loss in the outage window. In Fig. 25, the vertical axis plots 100 * (total usage loss / usage loss in outage window). This allows the predicted total usage loss for an outage in progress to be derived from the measured loss in usage and the current length of the outage. For this prediction the final outage length is taken to be the current outage length. This method is also used to predict the costs of an outage when the outage is not expected to finish at the time the prediction is made. Modeling such a scenario relies on the assumption that level of usage in the outage window will remain constant from the last measured usage value to the projected end of the outage window.

In the exemplary, typical service demand curve shown in Fig. 25, the letters A-E on the length of outage axis denote inflection points and are used to illustrate some of the features of a Usage Loss curve. To point A, outage length is zero, and no outage has occurred. From points A - B - 0% usage loss – all usage missed during outage is regained post outage. From points B-C – 0-100% usage loss – outage affected usage – some usage lost during outage is not recovered. From points C-D – 100% usage loss – all usage missed during outage is lost. From points D-E – 100-200% usage loss– all usage missed during outage is lost and outage causes post usage to be affected.

During an outage, the costing engine estimates cost of the outage using the service demand curve and the Usage Loss curve. In some embodiments, the engine uses the following formula:

C_d(outage) = (usage lost in comparative usage window up to time O_L) x F_U (O_L) x (cost unit multiplier),

Wherein

O_L is the length of the outage, which may be the length of the outage to date or the length of the outage at some future point; and

F_U is the function represented by the Usage Loss Curve.

Usage Loss Curves for service instances and types may be derived from previous outage analyses. For each previous outage of a service two variables are extracted: total usage loss as a percentage of usage loss during the outage window, and length of the outage window. Outage data from a series of outages may be transformed into a Usage Loss Curve using a local regression model such as Lowess, as described in W. S. Cleveland, *Visual and Computational Considerations in Smoothing Scatterplots by Locally Weighted Regression*, Computer Science and Statistics: Eleventh Annual Symposium on the Interface, pages 96-100, Institute of Statistics, North Carolina State University, Raleigh, North Carolina, 1978, which is incorporated herein by reference.

In some embodiments the transformation of outage information into a Usage Loss Curve is improved by applying usage patterns to the outages. These are used to better determine the amount of usage lost. Usage patterns have two components:

- Method to identify pattern – expressed as a set of rules.
- Method to calculate usage loss percentage, i.e., total usage lost as a percentage of the usage lost during the outage, which is expressed as a equation.

Both methods make use of the following set of functions and values:

- OW- outage window length
- T_S – outage start
- T_E – outage end
- C_{USAGE} (T_1,T_2) – the expect usage between points T_1 and T_2 based on comparative usage data
- S_{USAGE} (T_1,T_2) – the usage between points T_1 and T_2 seen in the current usage data.

A number of usage patterns are identified and defined on the basis of observations of human interaction with a service during the outage recovery period. These

usage patterns are described with reference to Figs. 26-28. In other embodiments patterns may be used that model the behavior of Internet protocols and hardware during outages.

A first such usage pattern, a blip outage, has the characteristics of a short length outage, that usage lost during outage is regained post outage, and that users are typically unaware of the outage. An exemplary blip outage is a one minute POP3 outage, in which emails not served during the outage are served when the outage completes. Fig. 26 graphically represents this usage pattern, in which overshoot usage during recovery makes up for lost usage during the outage. This pattern may be defined by the rule that greater than 75% of the usage loss in the outage window is recovered within one outage window past end of outage. The usage loss during this usage pattern is zero, and the identification rule for this usage pattern is:

$$[S_{USAGE}(T_E,T_E+|OW|) - C_{USAGE}(T_E,T_E+|OW|)] > 0.75 * [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

A second usage pattern, a loss outage, has the characteristics of a medium length outage in which usage that would have occurred during the outage period is not regained when outage ends, and that users are aware of the outage. An example of a loss outage is a one hour POP3 outage, during which the telephone is used as an alternative to email during outage period. The usage graph of a loss outage is shown in Fig. 27, in which the usage loss during the outage exceeds the usage gained during recovery. A loss usage may be defined as one in which less than 25% of the usage loss during outage is recovered within 3 outage windows past end of outage. The identification rule for this usage pattern is:

$$0 \le [S_{USAGE}(T_E,T_E+3*|OW|) - C_{USAGE}(T_E,T_E+3*|OW|)] < 0.25 * [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

The usage loss calculation is:

$$100*[S_{USAGE}(T_S,T_E+3*|OW|) - C_{USAGE}(T_S,T_E+3*|OW|)] / [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

A third usage pattern, a suppressant outage, has the features of a long outage in which usage that would have occurred during the outage period is not regained when the outage ends, and usage does not return to pre-outage levels quickly after the outage, and in which a user's short term confidence in the service is lost and alternatives are sought. An example of a suppressant outage is a one day POP3 outage, in which the telephone is used as an alternative to email even when the outage ends. Fig. 28 graphs this usage pattern, showing that, usage continues to be below normal levels well after the outage has recovered. A suppressant outage may be characterized in that, for some value *n*, usage levels in each of the

n subsequent outage window lengths past the end of the outage are less than 90% of the *n* corresponding comparison windows. A suitable value for *n* is 5.

The identification rule for a suppressant outage is:

for all $i \in \{0,1,\ldots,n\}$, the following must hold true:

$(S_{USAGE}(T_E + i * |OW|, T_E + (i+1)*|OW|) / (C_{USAGE}(T_E + i * |OW|, T_E + (i+1)*|OW|)) < 0.9$

The usage loss percentage calculation is:

$100 * [C_{USAGE}(T_S,T_E + n*|OW|) - S_{USAGE}(T_S,T_E+n*|OW|)] / [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$

The level of customer retention component models the cost of an outage in terms of the long term loss of customers. This relationship is be represented by a function that linearly maps the percentage of existing customers lost to the outage length, the mapping being based upon historical or empirical data for the service or upon a relationship of number of customers lost to measured usage loss amount:

C_r(outage) =(customer lost) x (cost per customer)

The service level agreement penalty component derives financial penalties based on the outage details. This financial penalty could be fixed ($x per outage), time linear ($x per minute of outage) or usage linear ($x per byte of usage missed).

While the invention has been described and illustrated in connection with preferred embodiments, many variations and modifications as will be evident to those skilled in this art may be made without departing from the spirit and scope of the invention, and the invention is thus not to be limited to the precise details of methodology or construction set forth above as such variations and modification are intended to be included within the scope of the invention.

WHAT IS CLAIMED IS:

1. A method for analyzing a potential cause of a change in a service, wherein service quality of the service is monitored, usage of the service is measured, and service events are detected, the method comprising:

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state, and upon a change in service usage amount, the service change time window encompassing at least part of a service outage;

retrieving data representing a detected event and a time in which the event occurred; and

computing a probability that the detected event caused the service change based at least in part on a correlation between the event time and the service change time window.

2. The method of claim 1, wherein determining the service change time window comprises determining a service failure time window based upon the change in service quality and narrowing the service failure time window to the service change time window based upon the service usage amount measured during that service failure time window.

3. The method of claim 2, wherein the service quality is monitored through periodic polling of the service quality, and comprising determining the service failure time window as bounded by a polled point of the first working state and a polled point of the second, non-working state.

4. The method of claim 1, wherein computing the probability comprises computing the probability using at least in part a time weighting function which decreases exponentially with the distance between the event time and the service change time window.

5. The method of claim 1, comprising determining whether one or more other events of a type identical to the detected event occurred, and wherein computing the probability comprises computing the probability using at least in part a false occurrence weighting function which decreases the probability of the detected event as the cause of the service change for instances in which the detected event occurred outside the service change time window.

6. The method of claim 1, comprising storing historical data associating occurrences of prior events with prior service changes, and wherein computing the probability that the detected event caused the service change comprises computing the probability based at least in part on the historical data.

7. The method of claim 6, wherein storing historical data comprises storing data representing instances in which prior events occurred within prior service change time windows, and wherein computing the probability that the detected event caused the service change comprises using at least in part a positive occurrence weighting function which increases the probability of the detected event as the cause of the service change based on instances in the historical data in which a prior event of a type identical to the detected event occurred within a prior service change time window.

8. The method of claim 6, wherein storing historical data comprises storing data representing instances in which prior events were identified as having caused prior service changes, and wherein computing the probability that the detected event caused the service change comprises using at least in part a historical weighting function which increases the probability of the detected event as the cause of the service change based on instances in the historical data in which a prior event of a type identical to the detected event was identified as having caused a prior service change.

9. The method of claim 1, comprising retrieving data representing a plurality of detected events and corresponding event times, and wherein computing the probability comprises computing probabilities for each of the plurality of detected events.

10. The method of claim 9, wherein computing probabilities comprises computing the probabilities such that the total of all computed probabilities is 1.

11. The method of claim 1, wherein the service comprises service over a communication network and wherein the detected event comprises a network event.

12. The method of claim 1, wherein the service comprises service provided by an application program and wherein the detected event comprises an application program event.

13. The method of claim 1, wherein the service change is a service outage, comprising determining the service change time window as a change in service quality from the first working state to the second, non-working state.

14. The method of claim 1, wherein the service change is a service recovery, comprising determining the service change time window as a change in service quality from the second, non-working state to the first, working state.

15. The method of claim 1, wherein determining the service change time window comprises detecting a change in service quality by detecting a step change in measured usage.

16. A method for analyzing potential causes of a service change, the method comprising:

determining a service change time window encompassing a change of service between a first working state and a service outage, the service change being determined at least in part based on measured service usage levels;

detecting occurrences of a set of events within a given time prior to and during the service change time window, each occurrence of an event being associated with a time at which the event occurred; and

computing a probability distribution for the set of events, which probability distribution determines for each event in the set the probability that the detected event caused the service change, the probability distribution being based at least in part on relations between the time of each event occurrence and the service change time window.

17. The method of claim 16, wherein computing the probability distribution for the set of events comprises computing the probability distribution using a first weighting function which is the product of two or more second weighting functions.

18. The method of claim 16, wherein the two or more second functions are selected from the group consisting of:

a time weighting function which decreases exponentially the probability of a given event as the cause of the service change with the distance between the given event time and the service change time window;

a false occurrence weighting function which decreases the probability of a given event as the cause of the service change for instances in which events of the same type as the given event occurred outside the service change time window;

a positive occurrence weighting function which increases the probability of a given event as the cause of the service change based on instances stored in a historical

database in which events of the same type as the given event occurred within a prior service change time window; and

a historical weighting function which increases the probability of a given event as the cause of the service change based on instances in the historical database in which events of the same type as the given event were identified as having caused a prior service outage.

19. The method of claim 18, wherein the step of computing the probability distribution comprises using a first weighting function which is the product of the time weighting function, false occurrence weighting function, positive occurrence weighting function, and user weighting function.

20. The method of claim 16, comprising monitoring service quality, and wherein determining the service change time window comprises determining a service failure time window based upon a change in monitored service quality and narrowing the service failure time window to the service change time window based upon the service usage amount measured during that service failure time window.

21. The method of claim 20, wherein the service quality is monitored through periodic polling of the service quality, and comprising determining the service failure time window as bounded by a polled point of the first working state and a polled point of the second, non-working state.

22. The method of claim 16, comprising computing the probability distribution such that the total of all probabilities in the distribution is 1.

23. The method of claim 16, wherein the service comprises service over a communication network and wherein the detected events comprise network events.

24. The method of claim 16, wherein the service comprises service provided by an application program and wherein the detected events comprise application program events.

25. The method of claim 16, wherein the service change is a service outage, comprising determining the service change time window as a change in service from the first working state to the second, non-working state.

26. The method of claim 16, wherein the service change is a service recovery, comprising determining the service change time window as a change in service from the second, non-working state to the first, working state.

27. The method of claim 1, wherein determining the service change time window comprises detecting a step change in measured usage.

28. A network monitoring system comprising:

a service monitor for monitoring quality of service on the network;

a usage meter for measuring usage of the network;

an event detector for detecting network events and times at which the network events occur; and

a probable cause engine, coupled to receive data from the service monitor, usage meter, and the event detector, for:

setting a service change time window based upon data received from the service monitor or usage meter, the service change time window encompassing at least part of an occurrence of a service outage in the network; and

determining which of the network events detected by the event detector is the most likely cause of a service change based at least in part of the relations of the detected network event times to the service change time window.

29. A computer readable medium storing program code for, when executed, causing a computer to perform a method for analyzing a potential cause of an change in a service, wherein service quality of the service is monitored, usage amount of the service is measured, and service events are detected, the method comprising:

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state, and upon a change in service usage amount, the service change time window encompassing at least part of a service outage;

retrieving data representing a detected event and a time in which the event occurred; and

computing a probability that the detected event caused the service change based at least in part on a correlation between the event time and the service change time window.

30. A method for quantifying the effect of an outage in a service over a first period of time, the method comprising:

measuring usage of the service over time;

defining a cost of outage time window comprising the first time period and a second time period following the first time period; and

computing a cost of outage as the difference between the measured service usage during the cost of outage time window with service usage measured during a comparison window, the comparison window being substantially equal in time to that of the cost of outage time window and reflecting a similar period of service activity as that of the cost of outage time window without having a service outage.

31. The method of claim 30, comprising determining the second period of time to be a time in which the measured service usage returns to within a given percentage of a normal service usage.

32. The method of claim 30, comprising determining the second period of time to be the shorter of (1) a time in which the measured service usage returns to within a given percentage of a normal service usage and (2) a maximum time period.

33. The method of claim 30, wherein computing the cost of outage comprises computing the difference in units of service usage.

34. The method of claim 33, wherein the service is a communication service conveying a plurality of messages, the method comprising computing the cost of outage in numbers of messages conveyed.

35. The method of claim 33, wherein the service is a network server providing data items in response to requests therefor, the method comprising computing the cost of outage in numbers of requests received or data items provided by a server on the network.

36. The method of claim 33, comprising converting the computed units of cost of service outage to a monetary value.

37. The method of claim 36, wherein converting the computed units of cost of service outage comprises multiplying the units of cost of service outage by a first monetary value per unit of usage.

38. The method of claim 30, comprising comparing the cost of outage to a second cost of outage value for a different service and prioritizing the outages based on the compared costs.

39. The method of claim 30, comprising computing the difference between the monitored service usage following the cost of outage time window and a normal service usage level to thereby measure a long term effect of the service outage.

40. A method for quantifying the effect of an outage in a service, the method comprising:

measuring usage amounts of the service during a period of the service outage and a second period following the service outage;

comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs; and

determining a level of loss of service due to the service outage based on the comparison.

41. The method of claim 40, comprising defining the second period as the shorter of a time period in which measured service usage amounts return to within a given range of normal usage amounts and a predefined maximum time period.

42. The method of claim 40, wherein measuring service usage amounts comprises measuring service usage amounts in terms of units of service usage.

43. The method of claim 42, wherein the service is a communication service conveying a plurality of messages, comprising measuring service usage amounts in terms of number of messages conveyed by the system.

44. The method of claim 42, wherein the service is a network server providing data items in response to requests therefor, comprising measuring service usage amounts in terms of numbers of requests received or data items provided by a server on the network.

45. The method of claim 40, wherein determining the level of service loss comprises determining that substantially no loss of service occurred due to the outage based on the measured service usage amounts and normal service usage amounts being substantially equal.

46. The method of claim 40, comprising:

measuring service usage amounts during a third period following the second period;

comparing the measured third period service usage amounts to normal usage amounts measured under similar service conditions for a similar period of time; and

determining a long term effect on the service due to the service outage based on the comparison.

47. A computer readable medium storing program code which, when executed, causes a computer to perform a method for quantifying the effect of an outage in a service over a first period of time, the method comprising:

measuring service usage over time;

defining a cost of outage time window comprising the first time period and a second time period; and

computing a cost of outage as the difference between the measured level of service usage during the cost of outage time window with a level of usage in a comparison window, the comparison window being substantially equal in time to the cost of outage time window and reflecting a similar period of service activity as the cost of outage time window without having a service outage.

48. A method for predicting a cost of an outage of a service, the method comprising:

measuring time duration for and service usage during the outage;

comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs, to thereby determine a usage loss amount; and

computing a predicted cost of the outage based at least upon a cost component, the cost component comprising a function of the measured time of the outage and measured usage loss amount.

49. The method of claim 48, comprising measuring service usage on an ongoing basis and detecting the onset of the service outage using the measured service usage.

50. The method of claim 49, wherein detecting the onset of the service outage comprises detecting a step change in service usage.

51. The method of claim 48, comprising monitoring quality of the service and detecting the onset of a service outage based upon the service quality.

52. The method of claim 51, wherein monitoring service quality comprises monitoring service quality through periodic polling of the service quality, and wherein detecting the onset of a service outage comprises detecting the outage onset as bounded by a polled point of a first, working state and a polled point of a second, non-working state.

53. The method of claim 48, wherein computing the predicted cost of the outage comprises using a service demand cost component representing an affect on service usage based upon the duration of an outage.

54. The method of claim 53, wherein using the service demand cost component comprises multiplying the measured usage loss by a usage loss curve which is a function of time duration of an outage and represents a predicted percentage usage due to an outage based on time duration of the outage.

55. The method of claim 54, comprising generating the usage loss curve using historical data derived from prior service outages.

56. The method of claim 48, wherein computing the predicted cost of the outage comprises using a customer retention cost component representing a number or percentage of customers lost due to the outage.

57. The method of claim 48, wherein computing the predicted cost of the outage comprises using an agreement penalty component representing penalties arising under one or more service agreements due to a service outage.

58. The method of claim 48, wherein computing the predicted cost of the outage comprises computing the cost in units of service usage.

59. The method of claim 58, comprising converting the computed units of predicted cost to a monetary value by multiplying the units of predicted cost by a first monetary value per unit of usage.

60. The method of claim 48, comprising comparing the predicted cost of service outage to a second predicted cost of outage value for a different service and prioritizing the outages based on the compared costs.

61. A network monitoring system comprising:

a usage meter for measuring usage of a service on the network;

an event detector for detecting network events and times at which the network events occur;

a probable cause engine, coupled to receive data from the usage meter and the event detector, for determining which of the network events detected by the event detector is the most likely cause of a service outage based at least in part of the relations of the detected network event times to a service change time window, the service change time window encompassing at least part of an occurrence of the service outage in the network; and

a costing engine, coupled to receive data from the usage meter, for predicting the cost of the service outage.

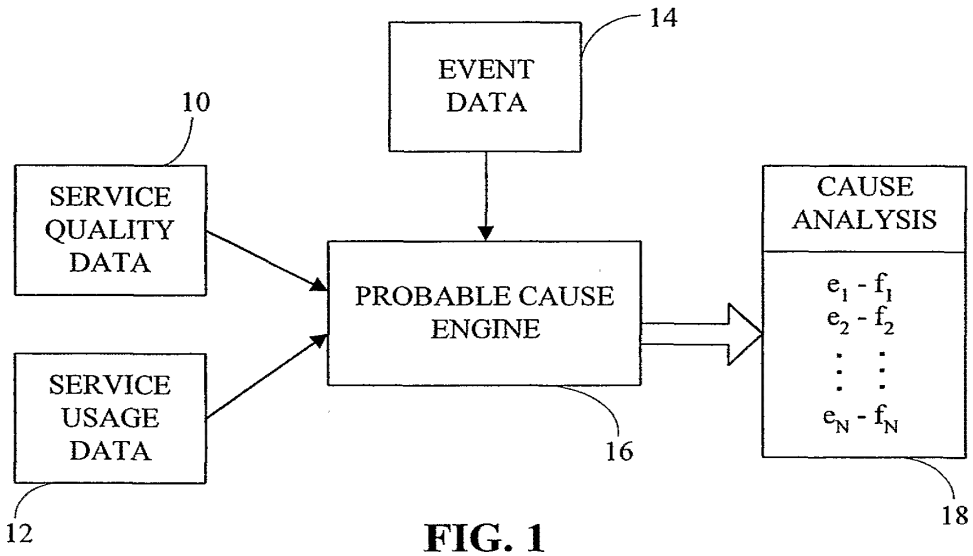

14
EVENT DATA
10
SERVICE QUALITY DATA
SERVICE USAGE DATA
12
PROBABLE CAUSE ENGINE
16
CAUSE ANALYSIS
e_1 - f_1
e_2 - f_2
e_N - f_N
18

FIG. 1

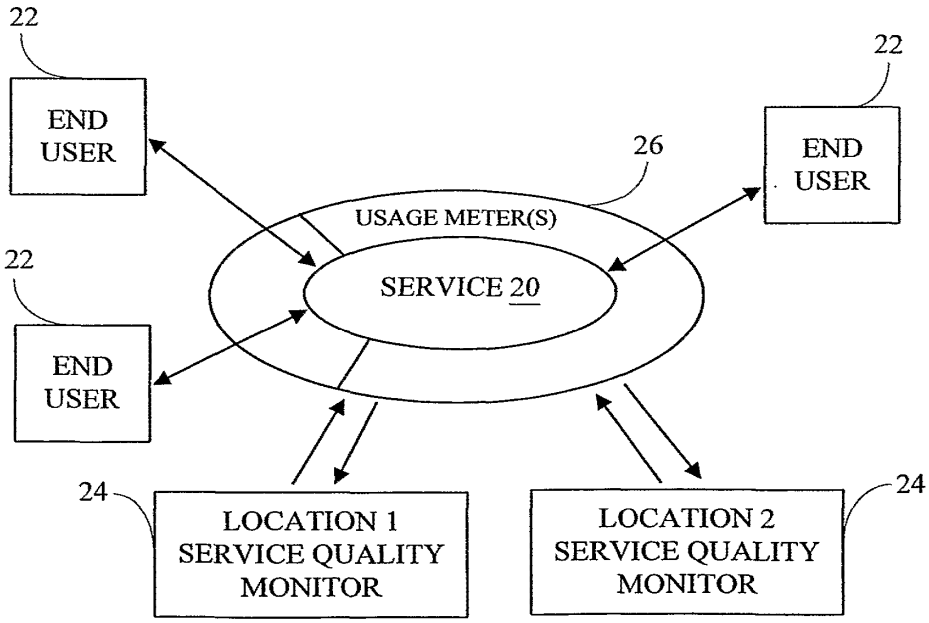
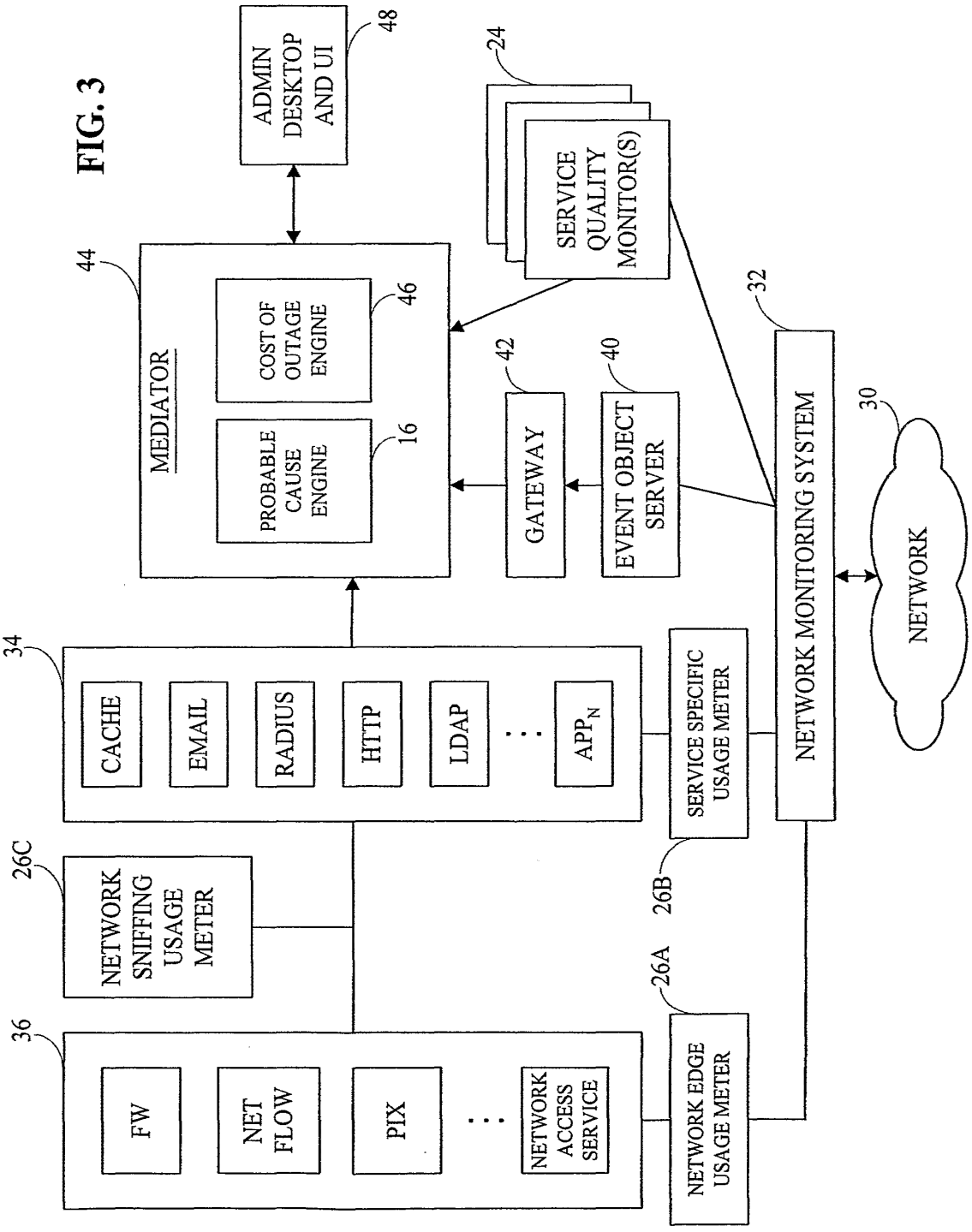

22
END USER
22
END USER
26
USAGE METER(S)
SERVICE 20
22
END USER
24
LOCATION 1 SERVICE QUALITY MONITOR
LOCATION 2 SERVICE QUALITY MONITOR
24

FIG. 2

FIG. 3


ADMIN DESKTOP AND UI
48
24
SERVICE QUALITY MONITOR(S)
44
MEDIATOR
COST OF OUTAGE ENGINE
46
PROBABLE CAUSE ENGINE
16
42
GATEWAY
40
EVENT OBJECT SERVER
32
30
NETWORK
NETWORK MONITORING SYSTEM
34
CACHE
EMAIL
RADIUS
HTTP
LDAP
APP$_N$
SERVICE SPECIFIC USAGE METER
26C
NETWORK SNIFFING USAGE METER
26B
36
FW
NET FLOW
PIX
NETWORK ACCESS SERVICE
26A
NETWORK EDGE USAGE METER

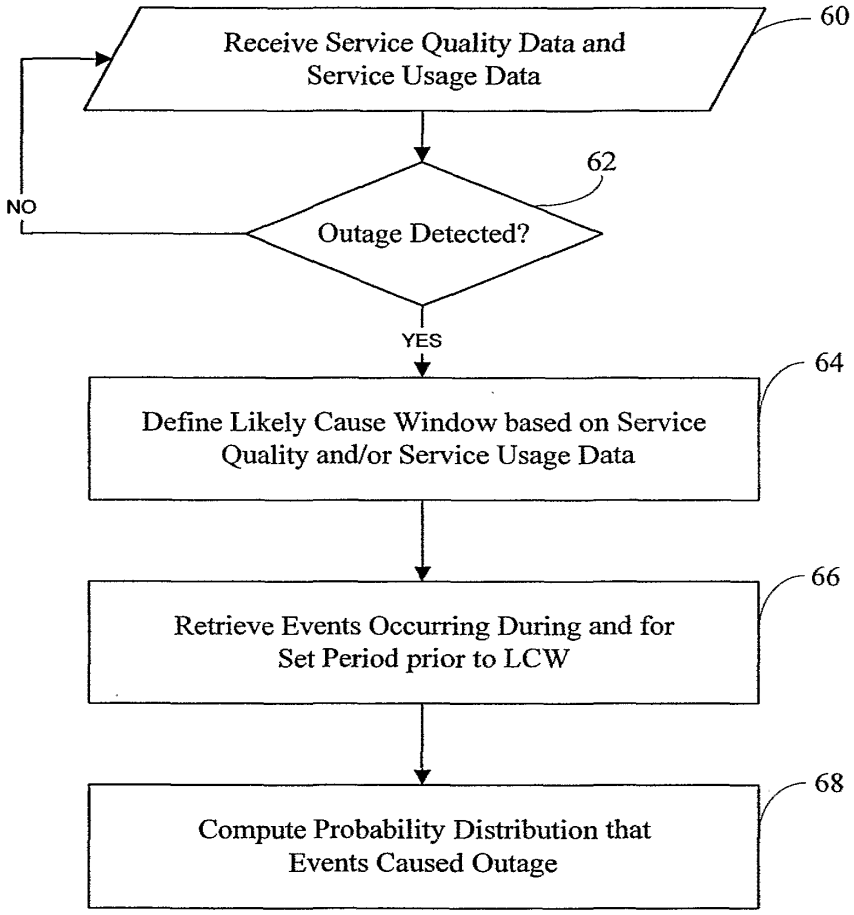

Receive Service Quality Data and Service Usage Data
60
62
Outage Detected?
NO
YES
64
Define Likely Cause Window based on Service Quality and/or Service Usage Data
66
Retrieve Events Occurring During and for Set Period prior to LCW
68
Compute Probability Distribution that Events Caused Outage

FIG. 4

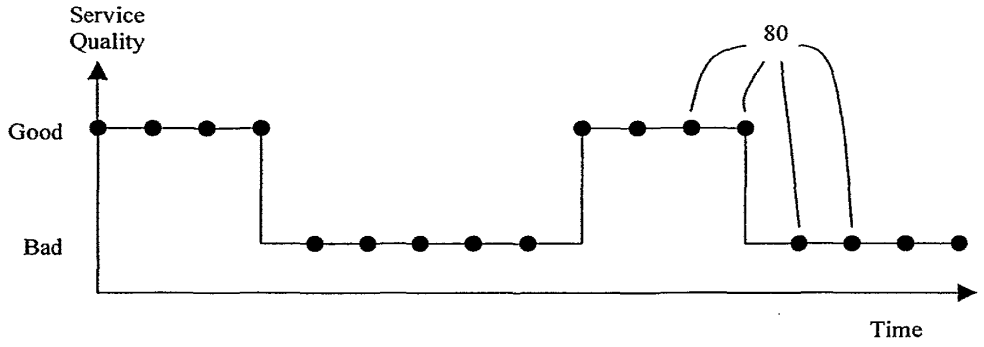


Fig. 5

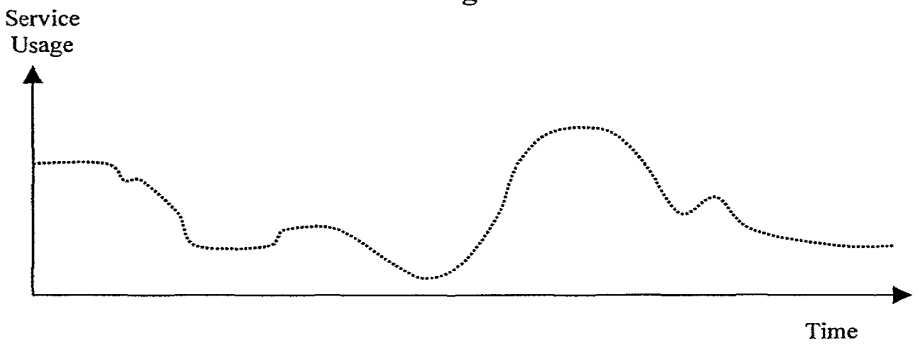


Fig. 6

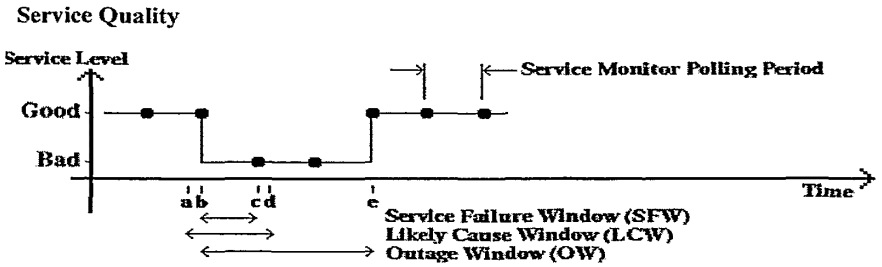


FIG. 7

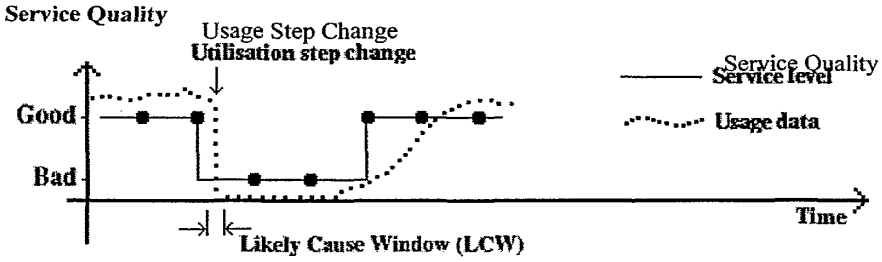


FIG. 8

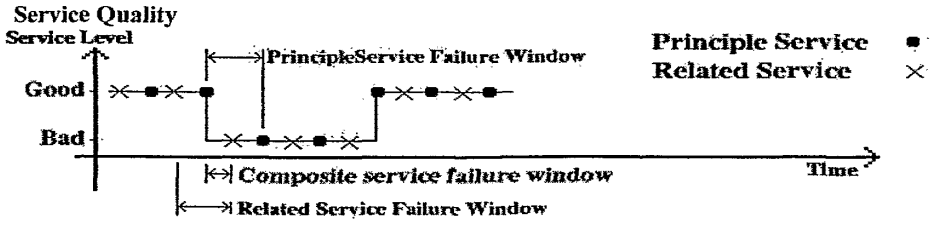


FIG. 9

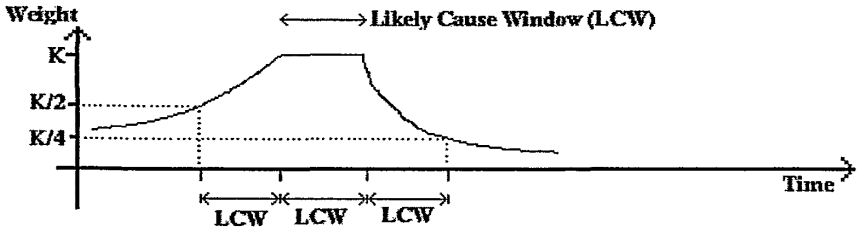


FIG. 10

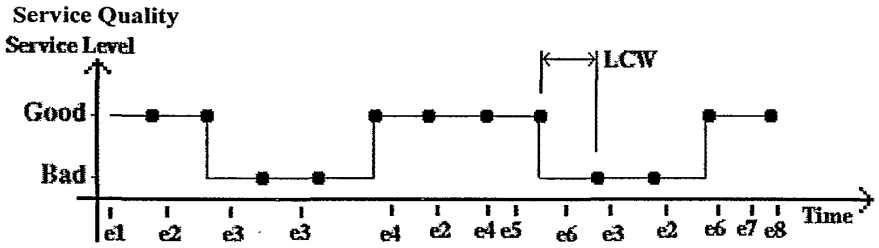


FIG. 11

Event	T(e)	FO(e)	PO(e)	U(e)	F(e)	P(e)
e3	2.11	1.00	4	1	8.44	0.5072
e6	4.00	0.50	2	1	4.00	0.2404
e2	1.24	0.25	2	4	2.48	0.1488
e5	2.61	0.50	1	1	1.31	0.0785
e4	1.38	0.25	1	1	0.34	0.0207
e7	0.07	0.50	1	1	0.03	0.0021
e1	0.06	0.50	1	1	0.03	0.0019
e8	0.02	0.50	1	1	0.01	0.0005
				Total:	16.64	1.0000

FIG. 12

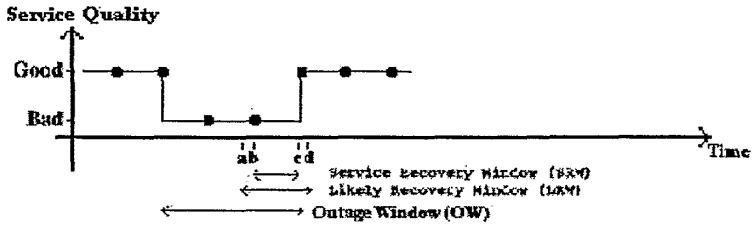

Service Quality
Good
Bad
ab
cd
Time
Service Recovery Window (SRW)
Likely Recovery Window (LRW)
Outage Window (OW)

Fig 13

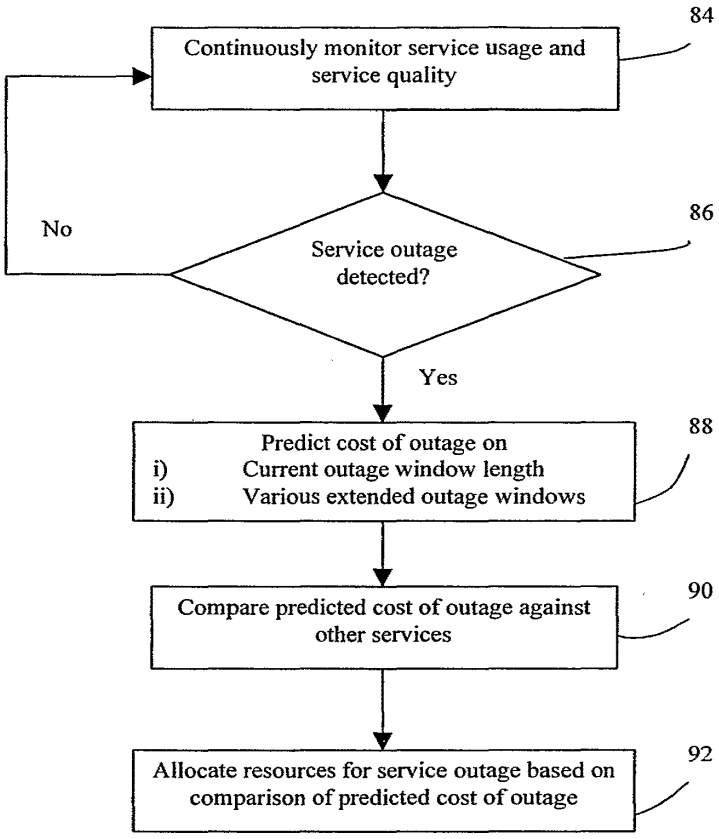

84
Continuously monitor service usage and service quality
86
No
Service outage detected?
Yes
88
Predict cost of outage on
i) Current outage window length
ii) Various extended outage windows
90
Compare predicted cost of outage against other services
92
Allocate resources for service outage based on comparison of predicted cost of outage

FIG. 14

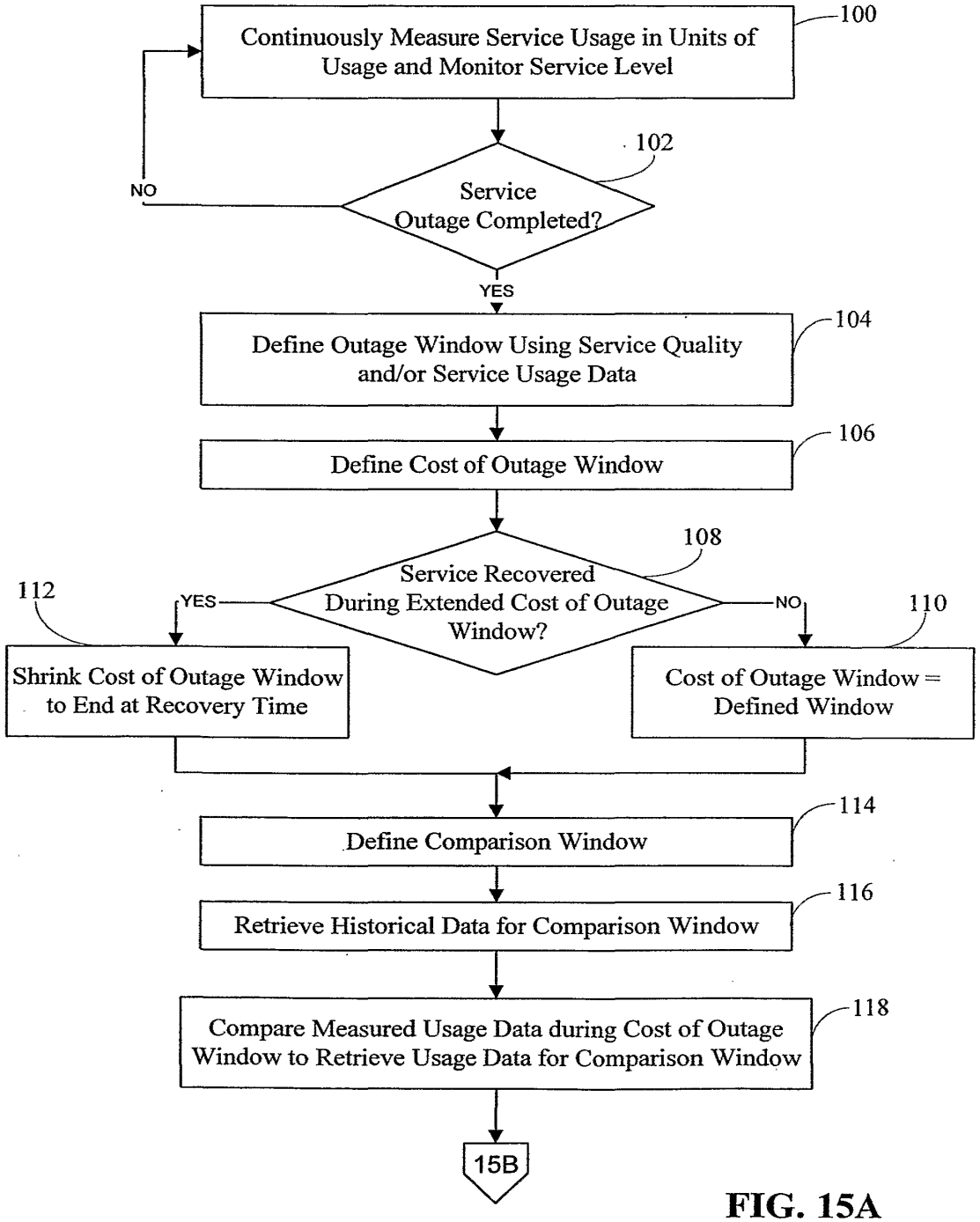

Continuously Measure Service Usage in Units of Usage and Monitor Service Level
100
102
Service Outage Completed?
NO
YES
Define Outage Window Using Service Quality and/or Service Usage Data
104
Define Cost of Outage Window
106
108
Service Recovered During Extended Cost of Outage Window?
YES
NO
112
110
Shrink Cost of Outage Window to End at Recovery Time
Cost of Outage Window = Defined Window
Define Comparison Window
114
Retrieve Historical Data for Comparison Window
116
Compare Measured Usage Data during Cost of Outage Window to Retrieve Usage Data for Comparison Window
118
15B

FIG. 15A

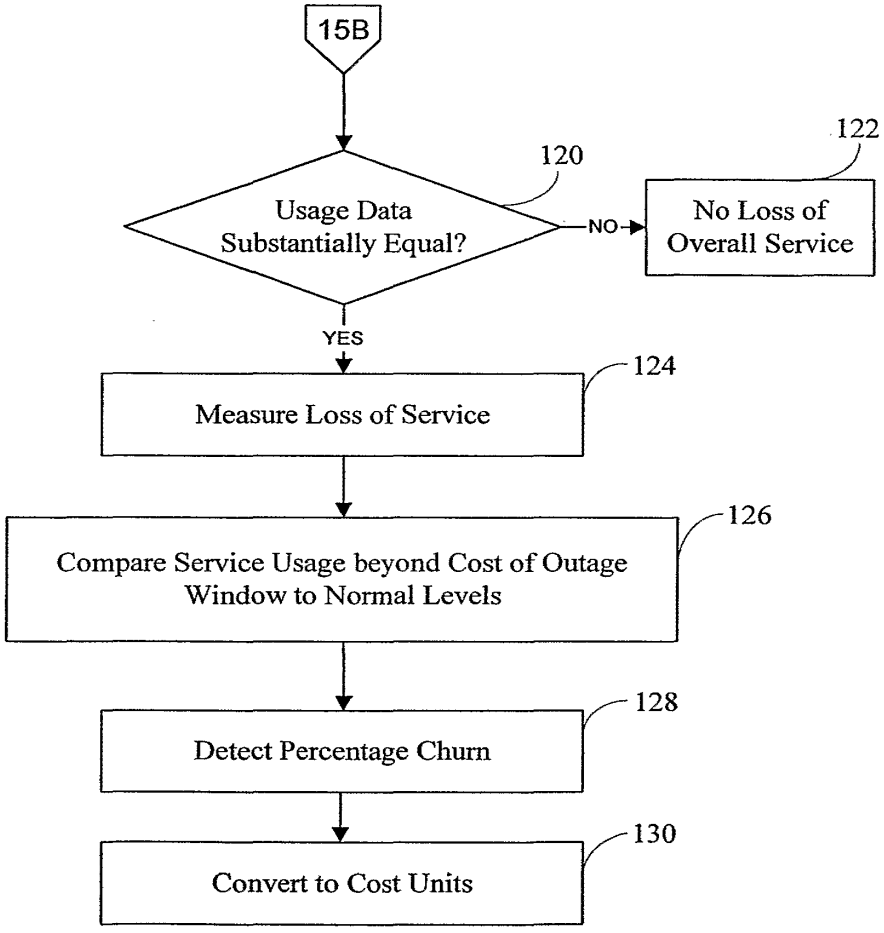

15B
120
Usage Data Substantially Equal?
NO
122
No Loss of Overall Service
YES
124
Measure Loss of Service
126
Compare Service Usage beyond Cost of Outage Window to Normal Levels
128
Detect Percentage Churn
130
Convert to Cost Units

FIG. 15B

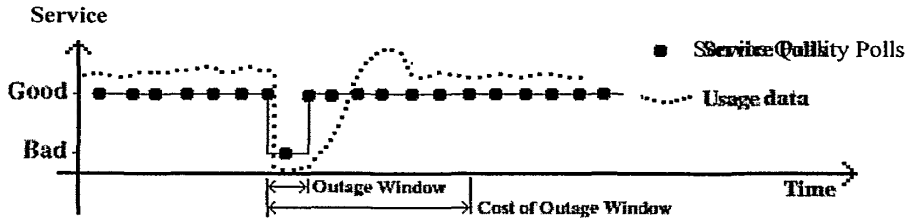


FIG. 16

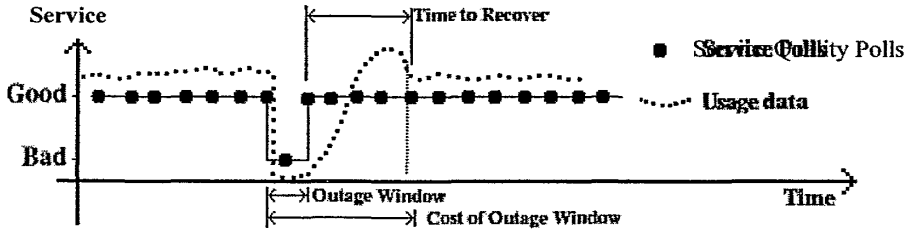


FIG. 18

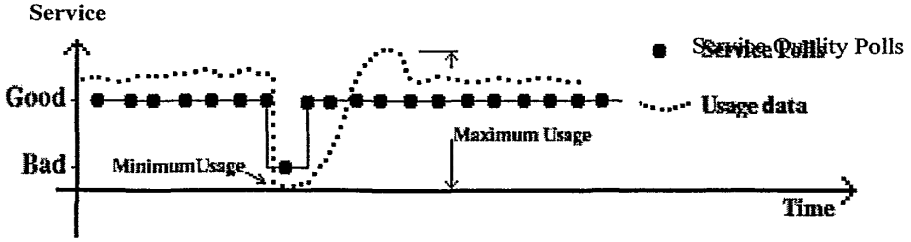


FIG. 19

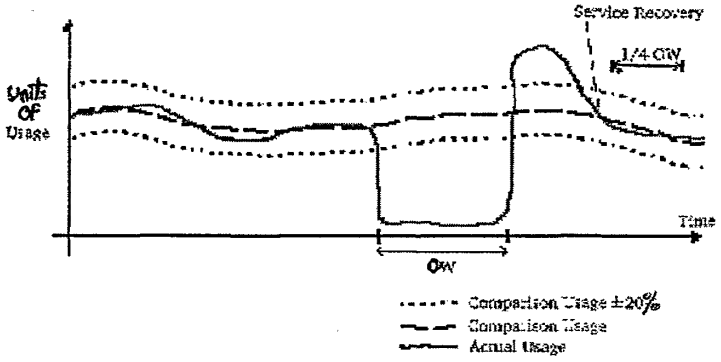

Service Recovery
1/4 CW
Units of Usage
Time
CW
Comparison Usage ±20%
Comparison Usage
Actual Usage

FIG. 17

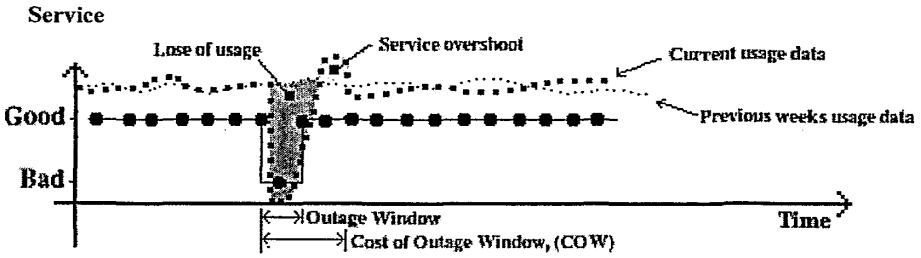


FIG. 20

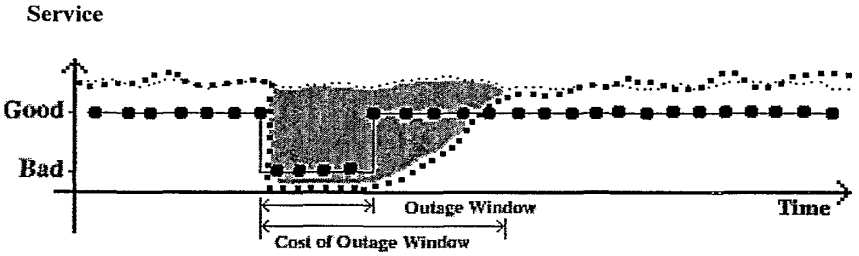


FIG. 21

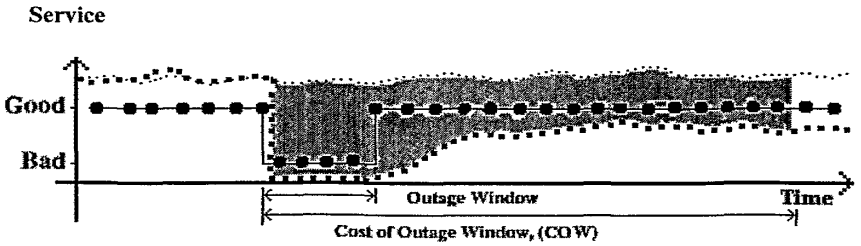


FIG. 22

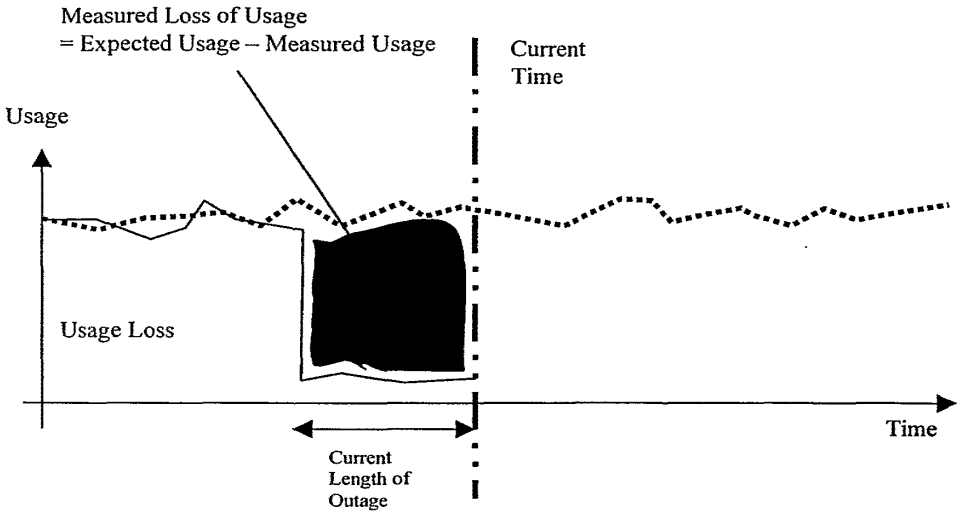

Measured Loss of Usage
= Expected Usage – Measured Usage
Current
Time
Usage
Usage Loss
Time
Current
Length of
Outage

FIG. 23

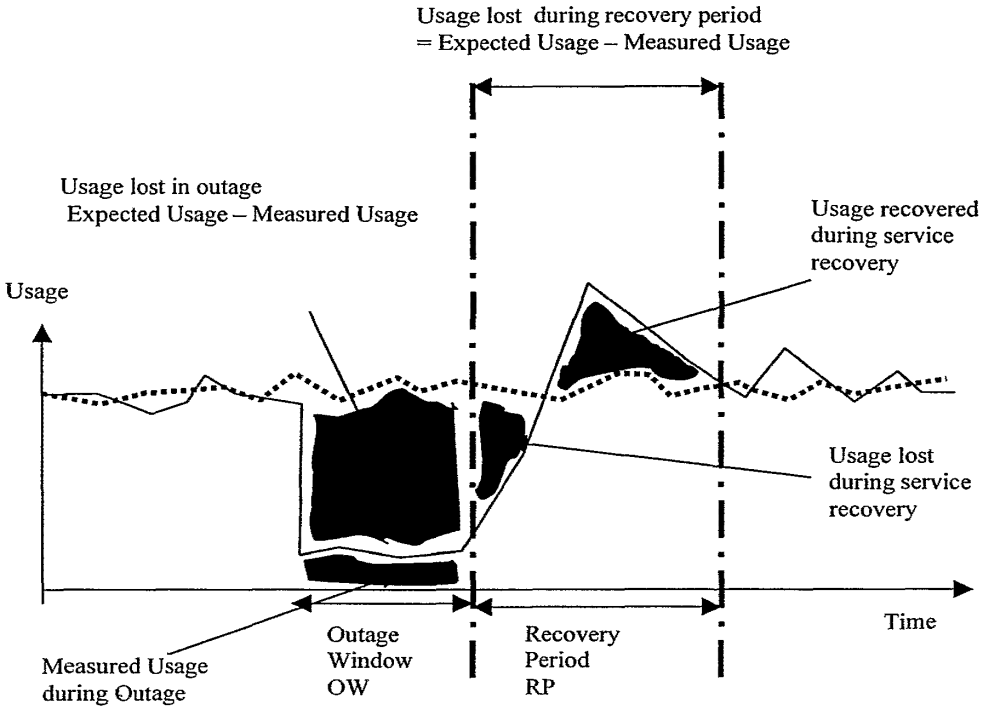

Usage lost during recovery period
= Expected Usage – Measured Usage
Usage lost in outage
Expected Usage – Measured Usage
Usage recovered
during service
recovery
Usage
Usage lost
during service
recovery
Time
Measured Usage
during Outage
Outage
Window
OW
Recovery
Period
RP

FIG. 24

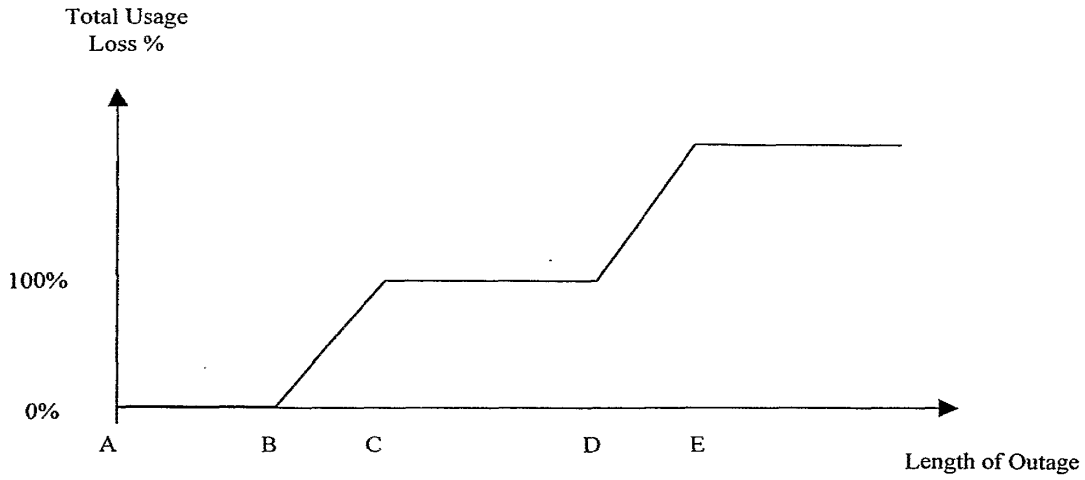


FIG. 25

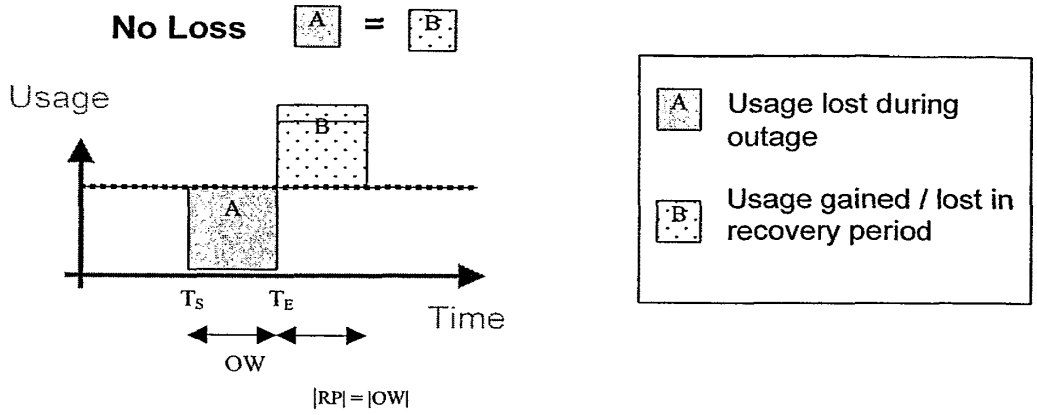

No Loss A = B
Usage
B
A
T_S
T_E
Time
OW
|RP| = |OW|
A Usage lost during outage
B Usage gained / lost in recovery period

FIG. 26

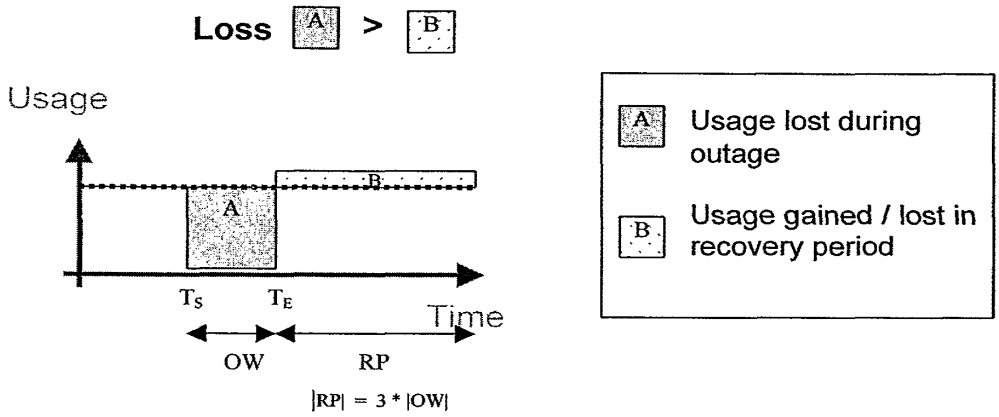

Loss A > B
Usage
B
A
T_S
T_E
Time
OW
RP
|RP| = 3 * |OW|
A Usage lost during outage
B Usage gained / lost in recovery period

FIG. 27

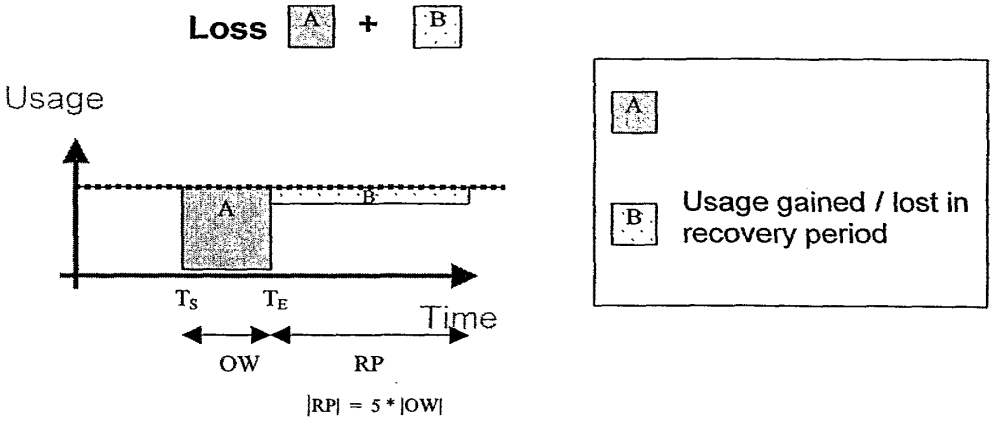

Loss A + B
Usage
A
B
T_S
T_E
Time
OW
RP
|RP| = 5 * |OW|
A
B
Usage gained / lost in recovery period

FIG. 28

Electronic Acknowledgement Receipt

EFS ID:	25158154
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
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:	RALEP032C1
Receipt Date:	10-MAR-2016
Filing Date:	15-NOV-2013
Time Stamp:	12:49:09
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)	P032C1.pdf	613129 2b84995b8166b4d4179e792e8cef57fdb623e667	no	8

Warnings:	
Information:	

2	Foreign Reference	2072.pdf	819567 9bd3134bd27e9dd9d134e7565086a86315c0ab30	no	33
Warnings:					
Information:					
3	Foreign Reference	2073.pdf	1463202 ba90a6bf82143d32fc7a1fbab25c6e727606a4c3	no	59
Warnings:					
Information:					
			Total Files Size (in bytes):	2895898	

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/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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	5974439	A	1999-10-26	Bollella, Gregory	
	2	6038540	A	2000-03-14	Krist et al.	
	3	6058434	A	2000-05-02	Wilt et al.	
	4	6125391	A	2000-09-26	Meltzer et al.	
	5	6393014	B1	2002-05-21	Daly et al.	
	6	6397259	B1	2002-05-28	Lincke et al.	
	7	6735206	B1	2004-05-11	Oki et al.	
	8	6748437	B1	2004-06-08	Mankude et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	7017189	B1	2006-03-21	DeMello et al.	
	11	7024460	B2	2006-04-04	Koopmas et al.	
	12	7047276	B2	2006-05-16	Liu et al.	
	13	7058022	B1	2006-06-06	Carolan et al.	
	14	7149521	B2	2006-12-12	Sundar et al.	
	15	7162237	B1	2007-01-09	Silver et al.	
	16	7200112	B2	2007-04-03	Sundar et al.	
	17	7248570	B2	2007-07-24	Bahl et al.	
	18	7266371	B1	2007-09-04	Amin et al.	
	19	7366654	B2	2008-04-29	Moore, Robert C.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7391724	B2	2008-06-24	Alakoski et al.	
	21	7395244	B1	2008-07-01	Kingsford, Bryan	
	22	7411930	B2	2008-08-12	Montojo et al.	
	23	7454191	B2	2008-11-18	Dawson et al.	
	24	7508799	B2	2009-03-24	Sumner et al.	
	25	7512128	B2	2009-03-31	DiMambro et al.	
	26	7554983	B1	2009-06-30	Muppala, Suresh	
	27	7564799	B2	2009-07-21	Holland et al.	
	28	7627767	B2	2009-12-01	Sherman et al.	
	29	7676673	B2	2010-03-09	Weller et al.	
	30	7817615	B1	2010-10-19	Breau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7844034	B1	2010-11-30	Oh et al.	
	32	7849161	B2	2010-12-07	Koch et al.	
	33	7849477	B2	2010-12-07	Cristofalo et al.	
	34	7860088	B2	2010-12-28	Lioy, Marcello	
	35	7889384	B2	2011-02-15	Armentrout et al.	
	36	7894431	B2	2011-02-22	Goring et al.	
	37	7899039	B2	2011-03-01	Andreasen et al.	
	38	7966405	B2	2011-06-21	Sundaresan et al.	
	39	7978686	B2	2011-07-12	Goyal et al.	
	40	7987496	B2	2011-07-26	Bryce et al.	
	41	8032168	B2	2011-10-04	Ikaheimo, Jorma	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8073427	B2	2011-12-06	Koch et al.	
	43	8104080	B2	2012-01-24	Burns et al.	
	44	8131840	B1	2012-03-06	Denker, Richard E.	
	45	8150394	B2	2012-04-03	Bianconi et al.	
	46	8190122	B1	2012-05-29	Alexander et al.	
	47	8385964	B2	2013-02-26	Haney, Richard D.	
	48	8407763	B2	2013-03-26	Weller et al.	
	49	8484568	B2	2013-07-09	Rados et al.	
	50	8503455	B2	2013-08-06	Heikens, Heico	
	51	8504032	B2	2013-08-06	Lott et al.	
	52	8504687	B2	2013-08-06	Maffione et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8504690	B2	2013-08-06	Shah et al.	
	54	8522337	B2	2013-08-27	Adusumilli et al.	
	55	8527662	B2	2013-09-03	Biswas et al.	
	56	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	57	8644813	B1	2014-02-04	Gailloux et al.	
	58	8667542	B1	2014-03-04	Bertz et al.	
	59	8793304	B2	2014-07-29	Lu et al.	
	60	8812525	B1	2014-08-19	Taylor III, Buford Leonard	
	61	8863111	B2	2014-10-14	Selitser et al.	
	62	8948726	B2	2015-02-03	Smith et al.	
	63	8966018	B2	2015-02-24	Bugwadia et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	9002342	B2	2015-04-07	Tenhunen et al.	
	65	RE44412		2013-08-06	Naqvi 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	20030134650	A1	2003-07-17	Sundar et al.	
	2	20030159030	A1	2003-08-21	Evans, Junius A.	
	3	20040127208	A1	2004-07-01	Nair et al.	
	4	20040260766	A1	2004-12-23	Barros et al.	
	5	20050041617	A1	2005-02-24	Huotari et al.	
	6	20050096024	A1	2005-05-05	Bicker et al.	
	7	20060075506	A1	2006-04-06	Sanda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	8	20060095517	A1	2006-05-04	O'Connor et al.	
	9	20060126562	A1	2006-06-15	Liu, Huitao	
	10	20060277590	A1	2006-12-07	Limont et al.	
	11	20060291419	A1	2006-12-28	McConnell et al.	
	12	20070257767	A1	2007-11-08	Beeson, Curt	
	13	20080018494	A1	2008-01-24	Waite et al.	
	14	20080034063	A1	2008-02-07	Yee, Robert	
	15	20090036111	A1	2009-02-05	Danford et al.	
	16	20120108225	A1	2012-05-03	Luna 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]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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)	2015-12-15
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 Acknowledgement Receipt	
EFS ID:	24373900
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
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:	RALEP032C1
Receipt Date:	15-DEC-2015
Filing Date:	15-NOV-2013
Time Stamp:	22:06:41
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)	P032C1_IDS.pdf	613890 918db8067eebbe45a4e25a5bdb153ed226d277fd	no	11

Warnings:
Information:

Total Files Size (in bytes):	613890

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.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 11/27/2015

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
11/27/2015	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.
14/082,040	15 November, 2013	RALEIGH ET AL.	RALEP032C1

		EXAMINER	
Headwater Partners I LLC 555 Twin Dolphin Drive, Suite 310 Redwood Shores, CA 94065		ANDREW JOSEPH RUDY	
		ART UNIT	PAPER
		3687	20151118

DATE MAILED:

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

Commissioner for Patents

The Restriction Requirement mailed November 17, 2015 is hereby vacated. Another office action will be forthcoming.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

PTO-90C (Rev.04-03)

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.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 11/17/2015

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
11/17/2015	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. 14/082,040	Applicant(s) RALEIGH ET AL.	
	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 2 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 *15 November 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) *1-23* 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) _____ is/are rejected.

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

9)☒ Claim(s) *1-23* 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: _____.

Notice of Pre-AIA or AIA Status

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

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-21, drawn to a system, classified in 709/224.

II. Claims 22-23 drawn to a method/medium, classified in 705/30.

3. The inventions are distinct, each from the other because of the following reasons:

Inventions Group II and Group I are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another and materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP § 806.05(e)). In this case the process may be practiced by hand or by non-statutory electronic signals.

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because one or more of the following reasons apply:

The inventions are distinct from each other.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of an invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103 or pre-AIA 35 U.S.C. 103(a) of the other invention.

4. A telephone call was made to Mr. Jonathan Darrow (Reg. No. 51,595) on November 10, 2015 to request an oral election to the above restriction requirement, but did not result in an election being made.

5. The examiner has required restriction between product or apparatus claims and process claims. Where applicant elects claims directed to the product/apparatus, and all product/apparatus claims are subsequently found allowable, withdrawn process claims that include all the limitations of the allowable product/apparatus claims should be considered for rejoinder. All claims directed to a nonelected process invention must include all the limitations of an allowable product/apparatus claim for that process invention to be rejoined.

In the event of rejoinder, the requirement for restriction between the product/apparatus claims and the rejoined process claims will be withdrawn, and the rejoined process claims will be fully examined for patentability in accordance with 37 CFR 1.104. Thus, to be allowable, the rejoined claims must meet all criteria for patentability including the requirements of 35 U.S.C. 101, 102, 103 and 112. Until all claims to the elected product/apparatus are found allowable, an otherwise proper restriction requirement between product/apparatus claims and process claims may be maintained. Withdrawn process claims that are not commensurate in scope with an allowable product/apparatus claim will not be rejoined. See MPEP § 821.04. Additionally, in order for rejoinder to occur, applicant is advised that the process claims should be amended during prosecution to require the limitations of the product/apparatus claims. **Failure to do so may result in no rejoinder.** Further, note that the prohibition against double patenting rejections of 35 U.S.C. 121 does not apply

where the restriction requirement is withdrawn by the examiner before the patent issues. See MPEP § 804.01.

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
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Inventor name search conducted.	11/10/2015	AJR
Continuity data reviewed.	11/10/2015	AJR
Bibliographic data updated.	11/10/2015	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. 1015

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/082,040	11/15/2013 RULE	709	3687	RALEP032C1

APPLICANTS
Headwater Partners I LLC, Redwood Shores, CA;

INVENTORS
Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

**** CONTINUING DATA ***************************

This application is a DIV of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009 ABN
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009 PAT 9137739
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009 PAT 8839387
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009 ABN
and is a CIP of 12/380,757 03/02/2009 PAT 8326958
and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009 PAT 8799451
and is a CIP of 12/380,769 03/02/2009 PAT 8675507
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010

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	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

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	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8339991		2012-12-25	Biswas et al.	
	54	8630314		2014-01-14	York, Frederick John	
	55	8868725		2014-10-21	Samba, Augustine S.	

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	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	
	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20120166604	A1	2012-06-28	Fortier et al.	
	12	20020191573		2002-12-19	Whitehill et al.	
	13	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	14	20090070379		2009-03-12	Rappaport, Theodore R.	
	15	20100318652		2010-12-16	Samba, Augustine S.	

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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

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)	2015-09-17
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.

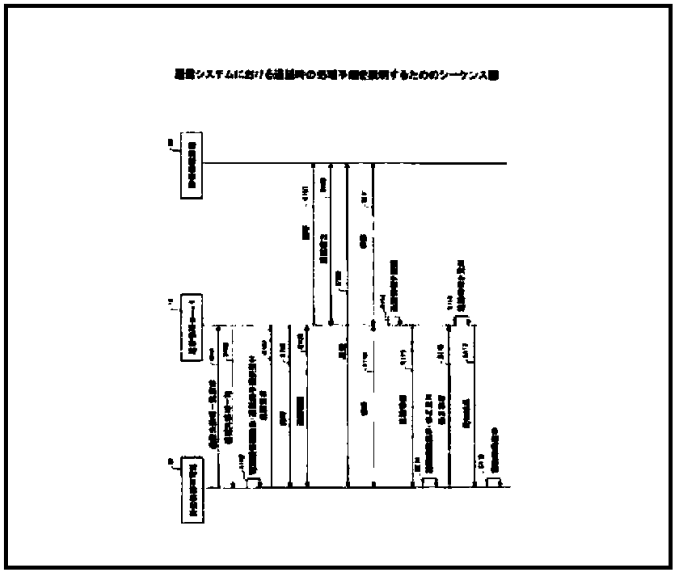
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

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)

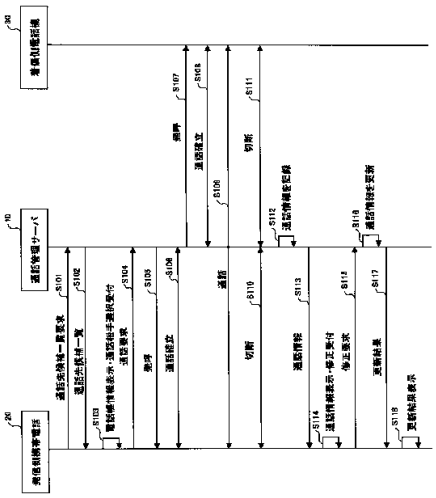
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　辻内　秀敏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K025 AA01　CC01　CC07　GG10　GG12

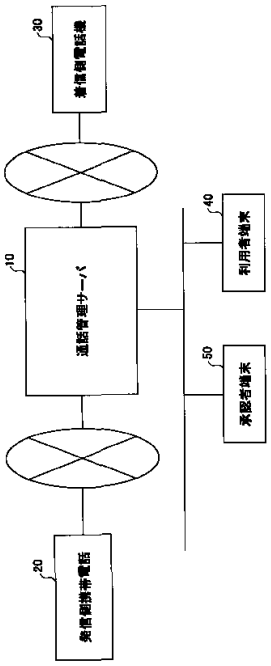
(54)【発明の名称】通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法

(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

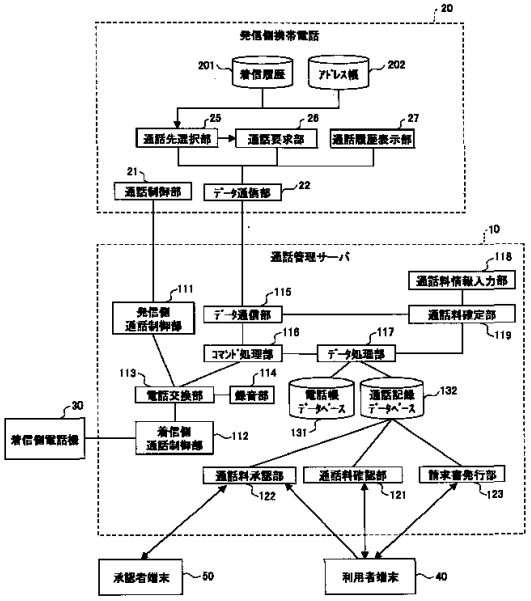
通信システムにおける通話時の処理手順を説明するためのシーケンス図



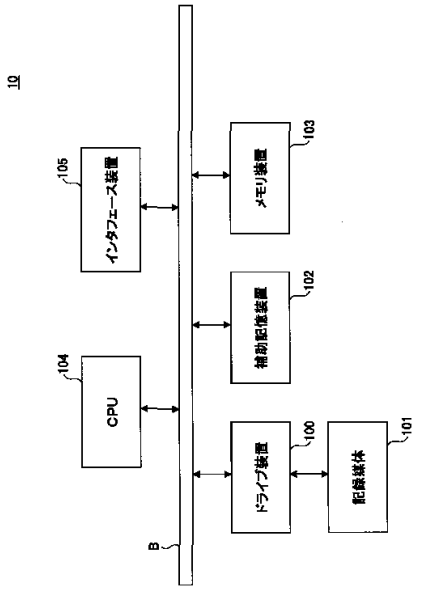
本発明の実施の形態における通信システム構成例を示す図



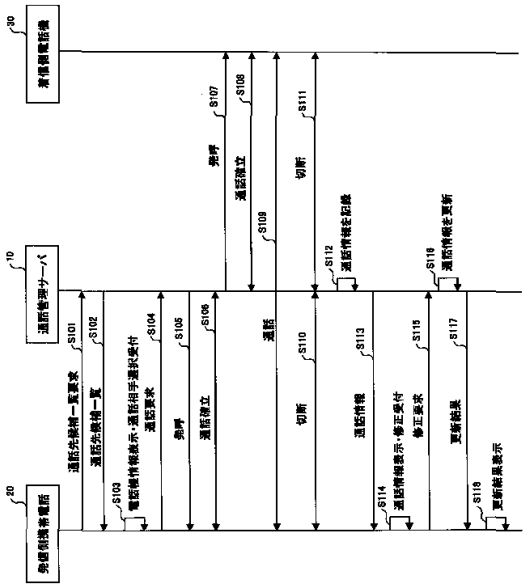
本発明の実施の形態における通信システムの機能構成例を示す図



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

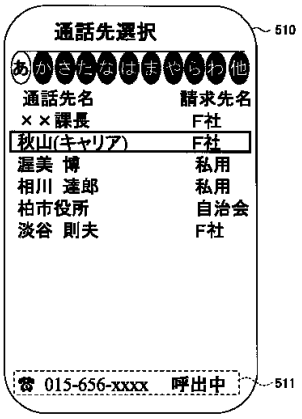


電話帳データベースの構成例を示す図

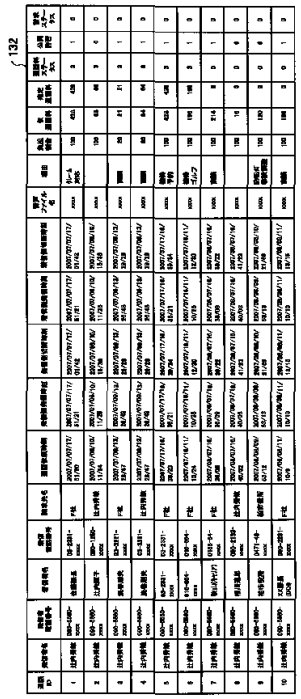
131

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	090-5580-xxxx	辻内匡子	090-1250-xxxx	妻	辻内秀敏	xxx@xxxxxxx
辻内秀敏	090-5580-xxxx	淡谷則夫	03-3221-xxxx	地上電器	F社	xxx@xxxxxxx
辻内秀敏	090-5580-xxxx	柏市役所	0471-46-xxxx	自治会	柏市役所	xxx@xxxxxxx
辻内秀敏	090-5580-xxxx	佐藤課長	03-2331-xxxx	OO商事	F社	xxx@xxxxxxx
辻内秀敏	090-5580-xxxx	秋山(キャリア)	0156-64-xxxx	F社	F社	xxx@xxxxxxx
辻内秀敏	090-5580-xxxx	相川達郎	050-2133-xxxx	親戚	辻内秀敏	
辻内秀敏	090-5580-xxxx	××課長	090-2231-xxxx	顧客	F社	xxx@xxxxxxx

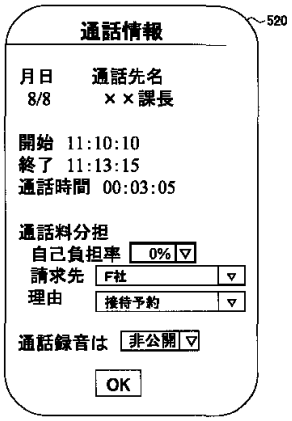
通話先選択画面の表示例を示す図



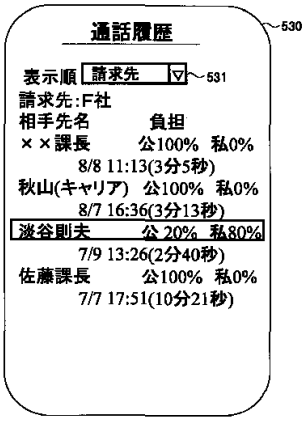
通話記録データベースの構成例を示す図



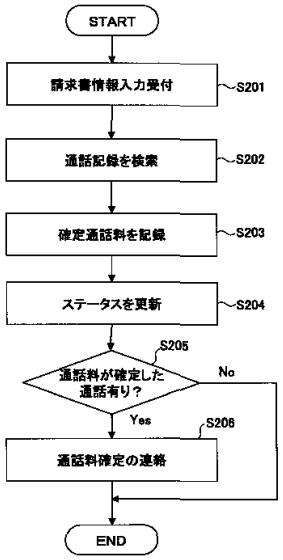
通話情報画面の表示例を示す図



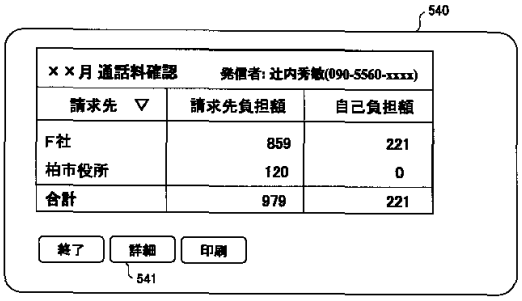
通話履歴画面の表示例を示す図



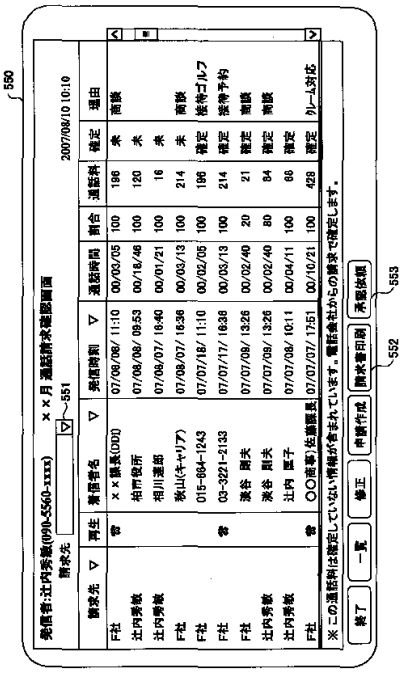
通話料の請求に応じて通話管理サーバによって実行される通話料の確定処理の処理手順を説明するためのフローチャート



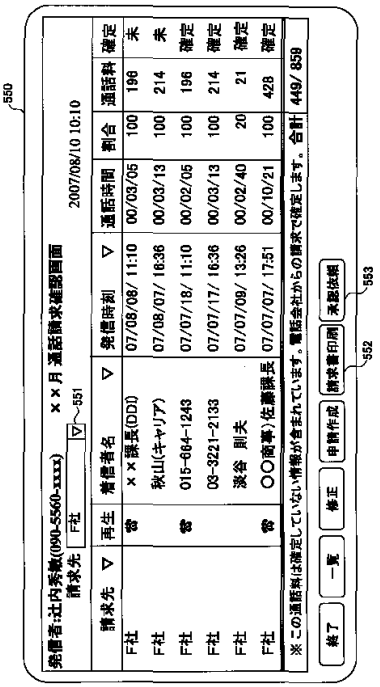
通話料確認画面の表示例を示す図



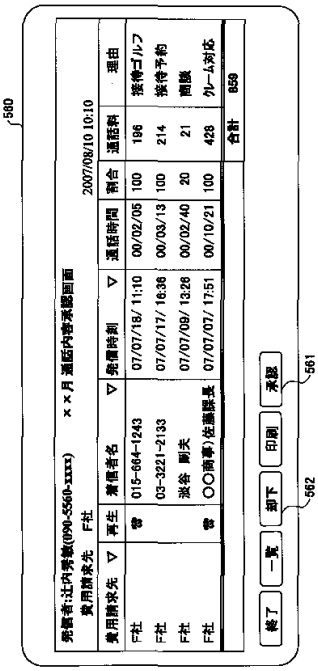
通話料確認詳細画面の表示例を示す図



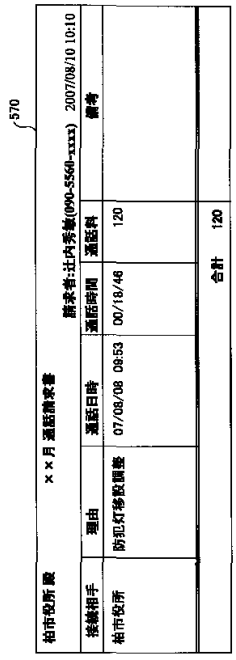
請求先が所属企業に絞り込まれた場合の通話料詳細画面の表示例を示す図



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

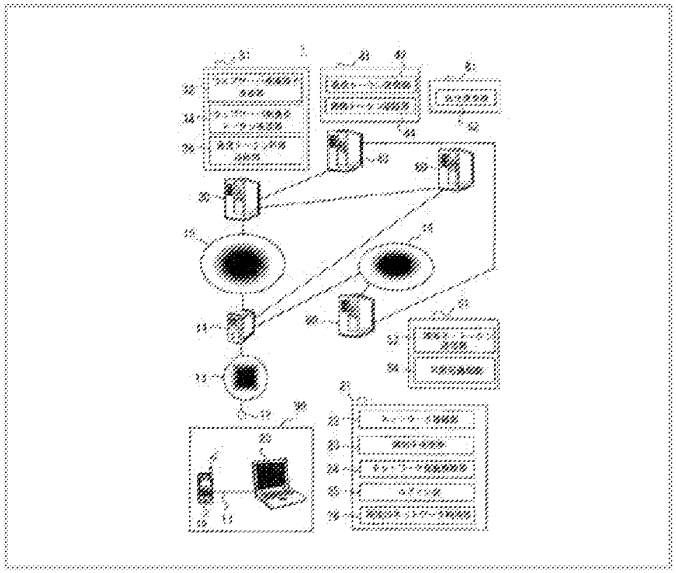
(51)Int.Cl. *H04L 12/56 (2006.01)*
H04M 15/00 (2006.01)
H04M 11/00 (2006.01)

(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)

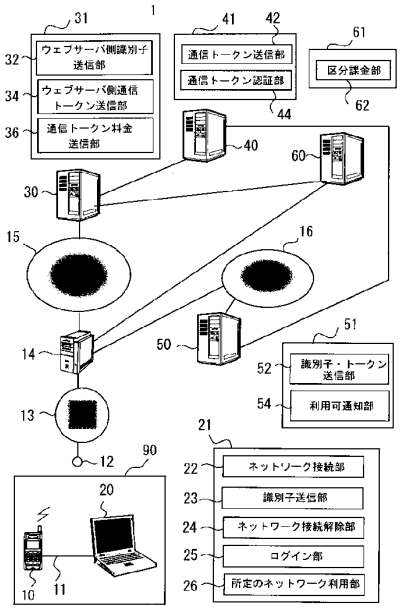
(71)出願人　596100812
京セラコミュニケーションシステム株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100108372
弁理士　谷田　拓男
(72)発明者　増田　景一
京都府京都市伏見区竹田鳥羽殿町６番地
京セラコミュニケーションシステム株式会社内

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。

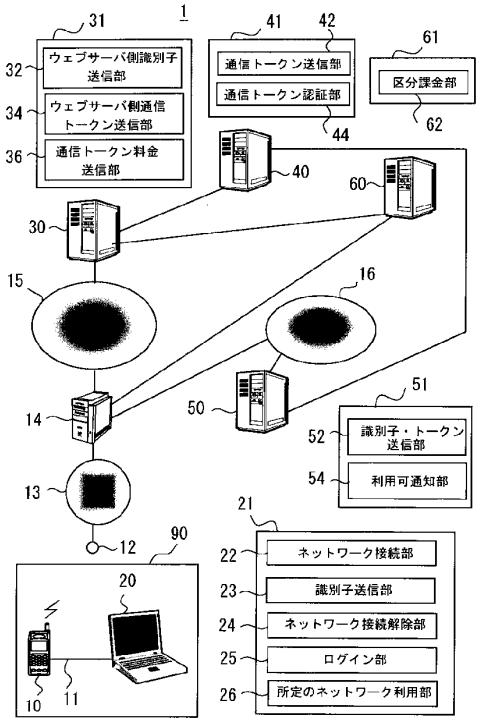
【産業上の利用可能性】

【００６８】

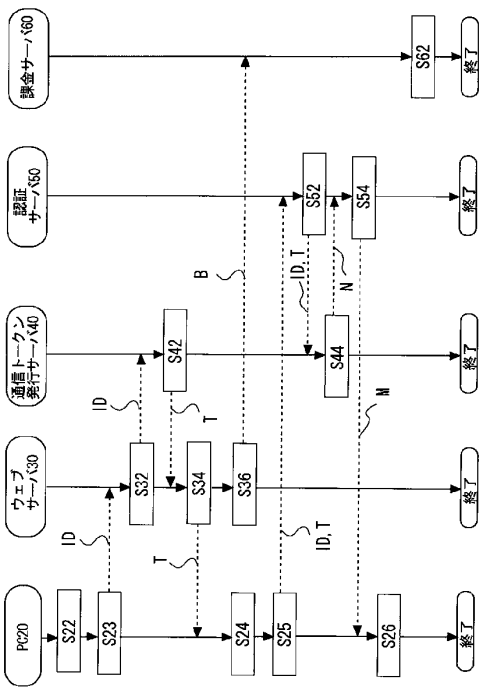
本発明の活用例として、上述のように公私分計を即時に行うことができるため、会社所有のＰＣおよび携帯電話器を用いた所定のネットワーク１６の利用に対する従来の会社側との割引契約に、個人所有のＰＣおよび携帯電話器を用いた場合における所定のネットワーク１６の利用に対しても即時に割引を適用するシステムへの応用が挙げられる。

【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。

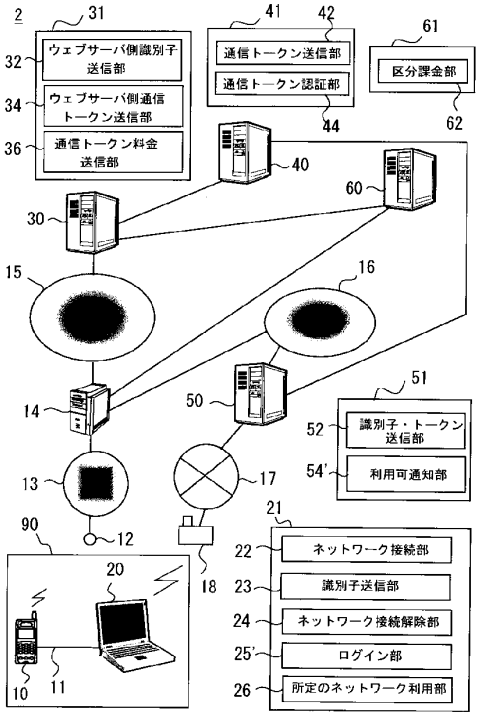
【図１】


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
52
識別子・トークン送信部
54
利用可通知部
13
12
90
21
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
ログイン部
26
所定のネットワーク利用部
20
10
11

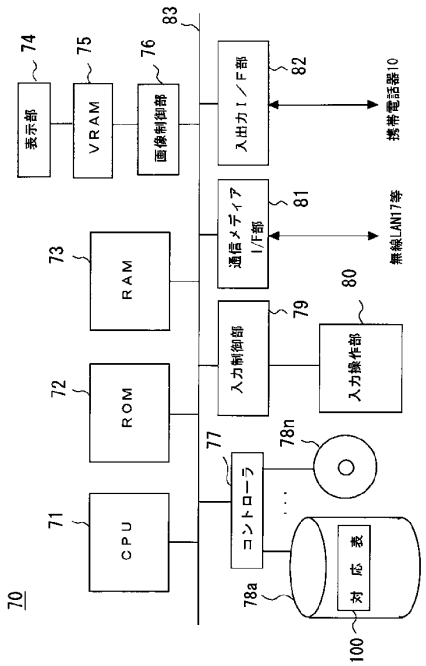
【図２】


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
M
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
52
識別子・トークン送信部
54'
利用可通知部
13
17
18
12
90
21
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'
ログイン部
26
所定のネットワーク利用部
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
78a
対応表
100
78n
83
携帯電話器10
無線LAN17等

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.

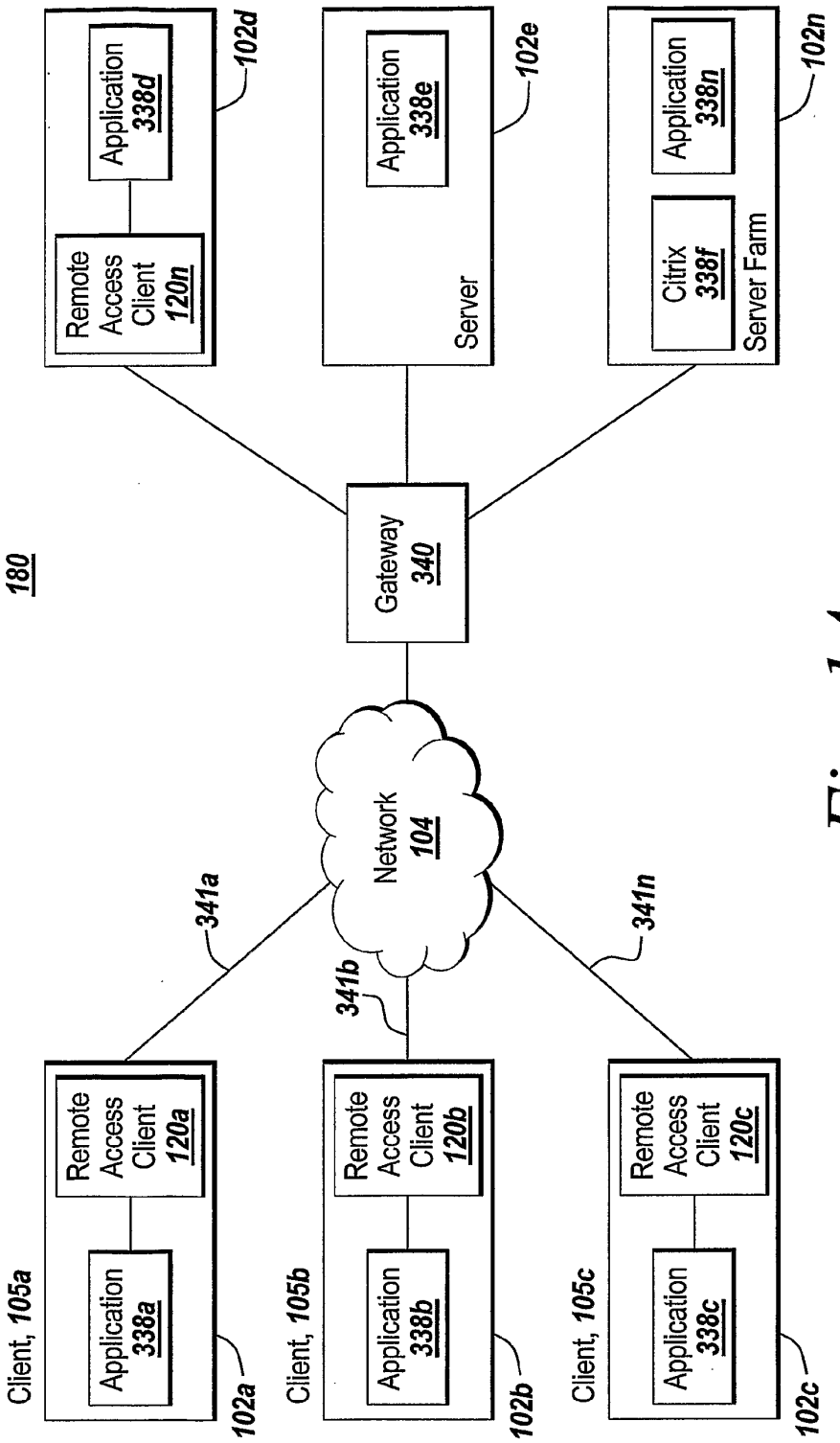

180
Gateway 340
Network 104
Remote Access Client 120n
Application 338d
102d
Application 338e
Server
102e
Citrix 338f
Application 338n
Server Farm
102n
341a
341b
341n
Client, 105a
Remote Access Client 120a
Application 338a
102a
Client, 105b
Remote Access Client 120b
Application 338b
102b
Client, 105c
Remote Access Client 120c
Application 338c
102c

Fig. 1A

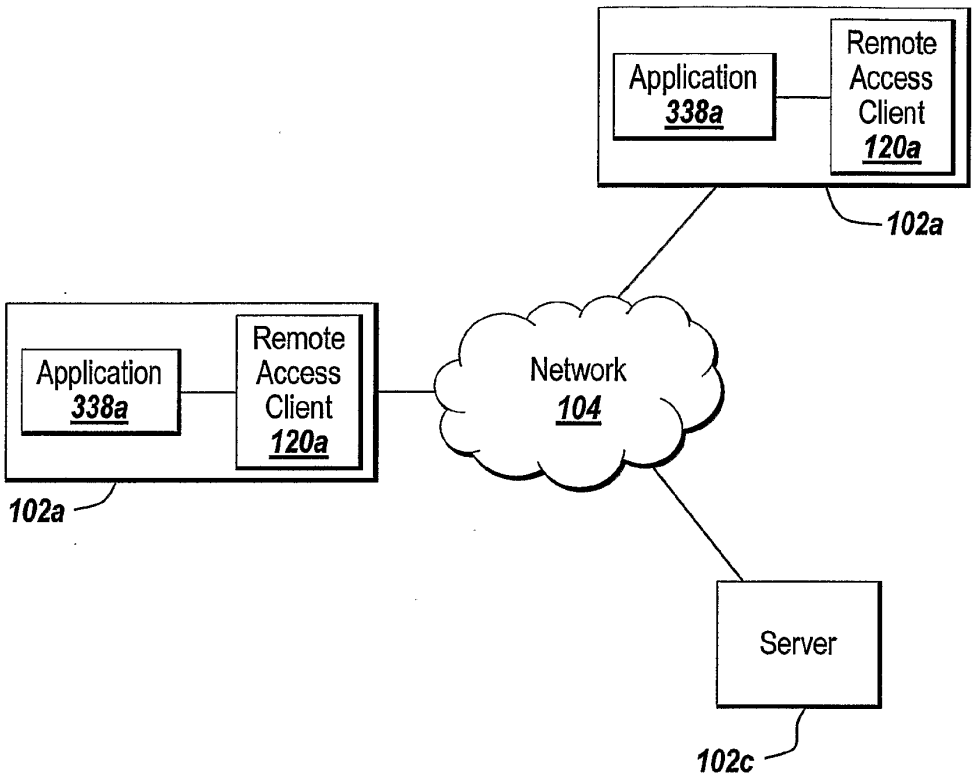

Application
338a
Remote
Access
Client
120a
102a
Application
338a
Remote
Access
Client
120a
102a
Network
104
Server
102c

Fig. 1B

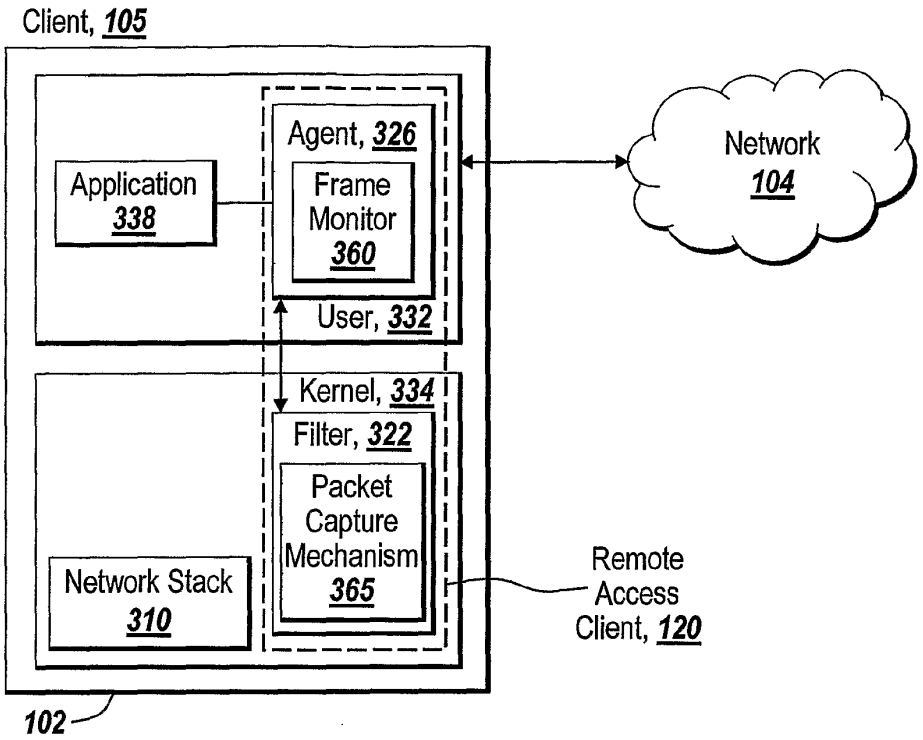

Client, 105
Agent, 326
Application 338
Frame Monitor 360
User, 332
Kernel, 334
Filter, 322
Packet Capture Mechanism 365
Network Stack 310
Network 104
Remote Access Client, 120
102

Fig. 1C

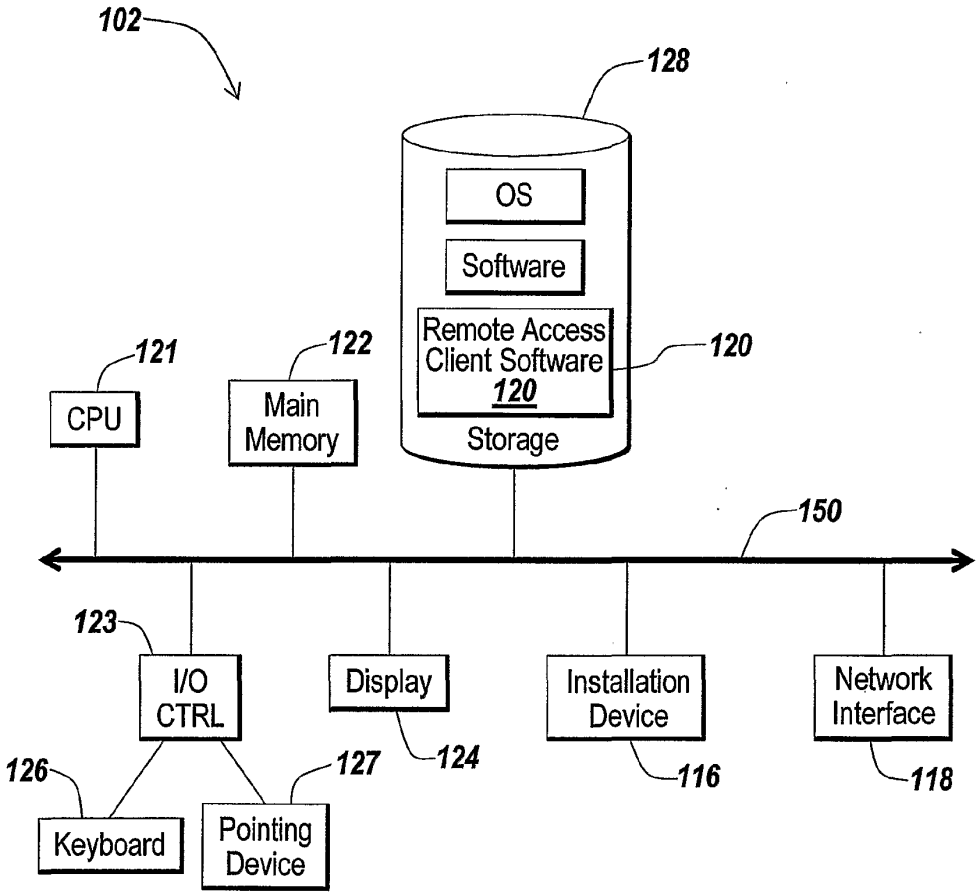

102
128
OS
Software
Remote Access Client Software
120
120
Storage
121
CPU
122
Main Memory
150
123
I/O CTRL
Display
124
Installation Device
116
Network Interface
118
126
Keyboard
127
Pointing Device

Fig. 1D

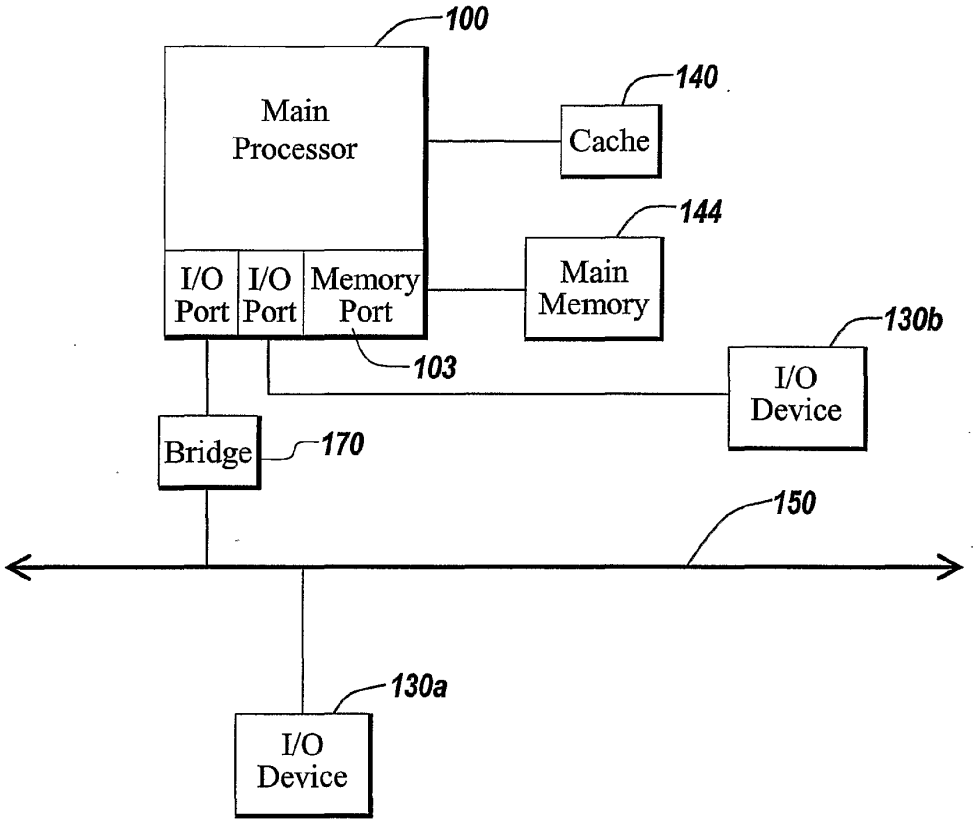

100
Main Processor
140
Cache
144
Main Memory
I/O Port
I/O Port
Memory Port
103
130b
I/O Device
Bridge
170
150
130a
I/O Device

Fig. 1E

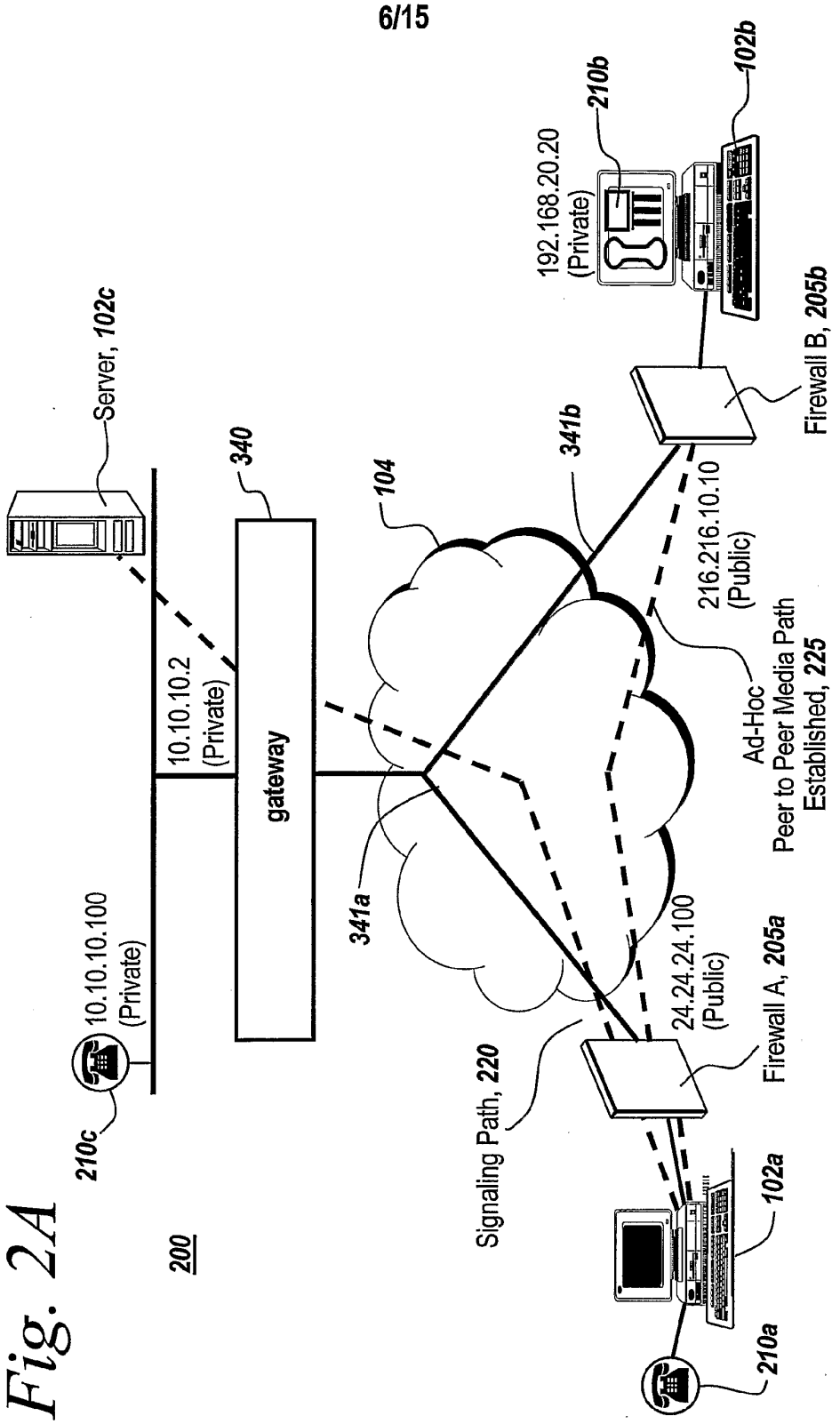

Server, 102c
340
104
341b
192.168.20.20
(Private)
210b
102b
10.10.10.2
(Private)
gateway
216.216.10.10
(Public)
Ad-Hoc
Peer to Peer Media Path
Established, 225
Firewall B, 205b
10.10.10.100
(Private)
341a
24.24.24.100
(Public)
Signaling Path, 220
Firewall A, 205a
210c
200
102a
210a

Fig. 2A

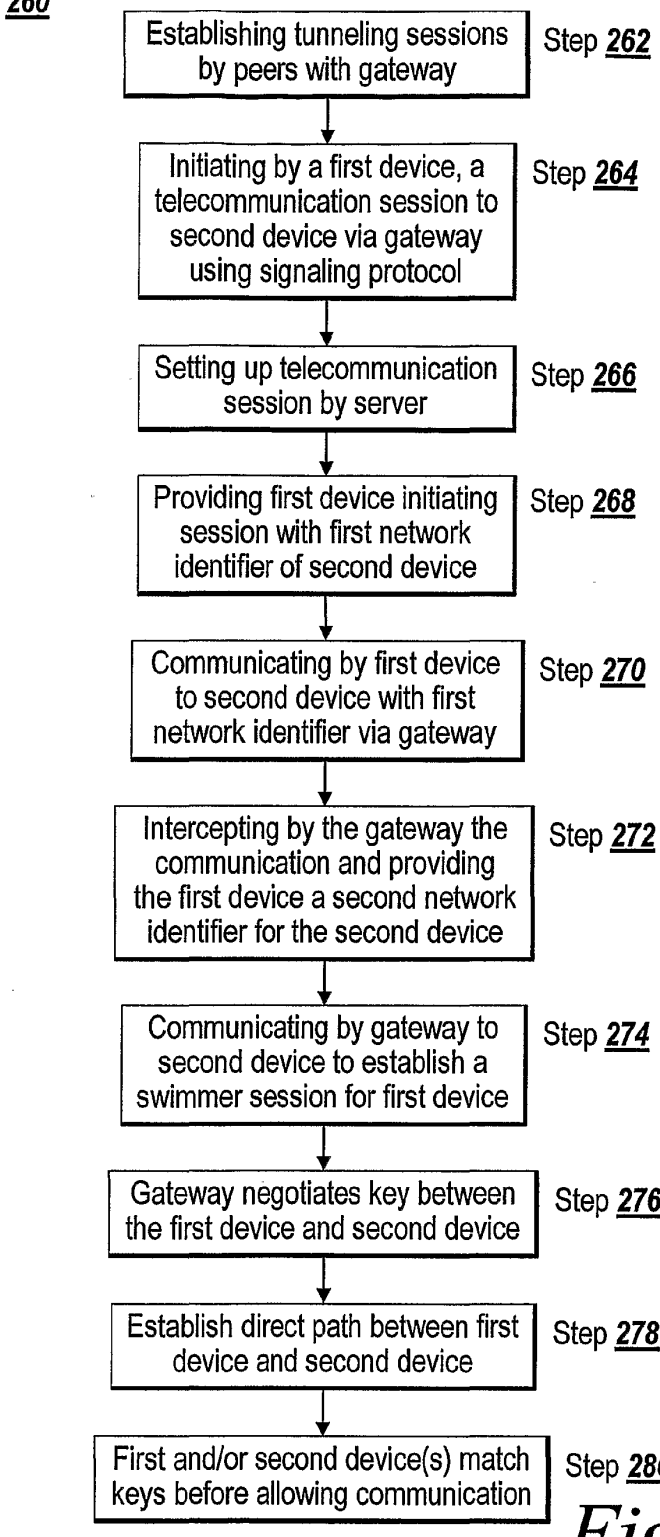

260
Establishing tunneling sessions by peers with gateway
Step 262
Initiating by a first device, a telecommunication session to second device via gateway using signaling protocol
Step 264
Setting up telecommunication session by server
Step 266
Providing first device initiating session with first network 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

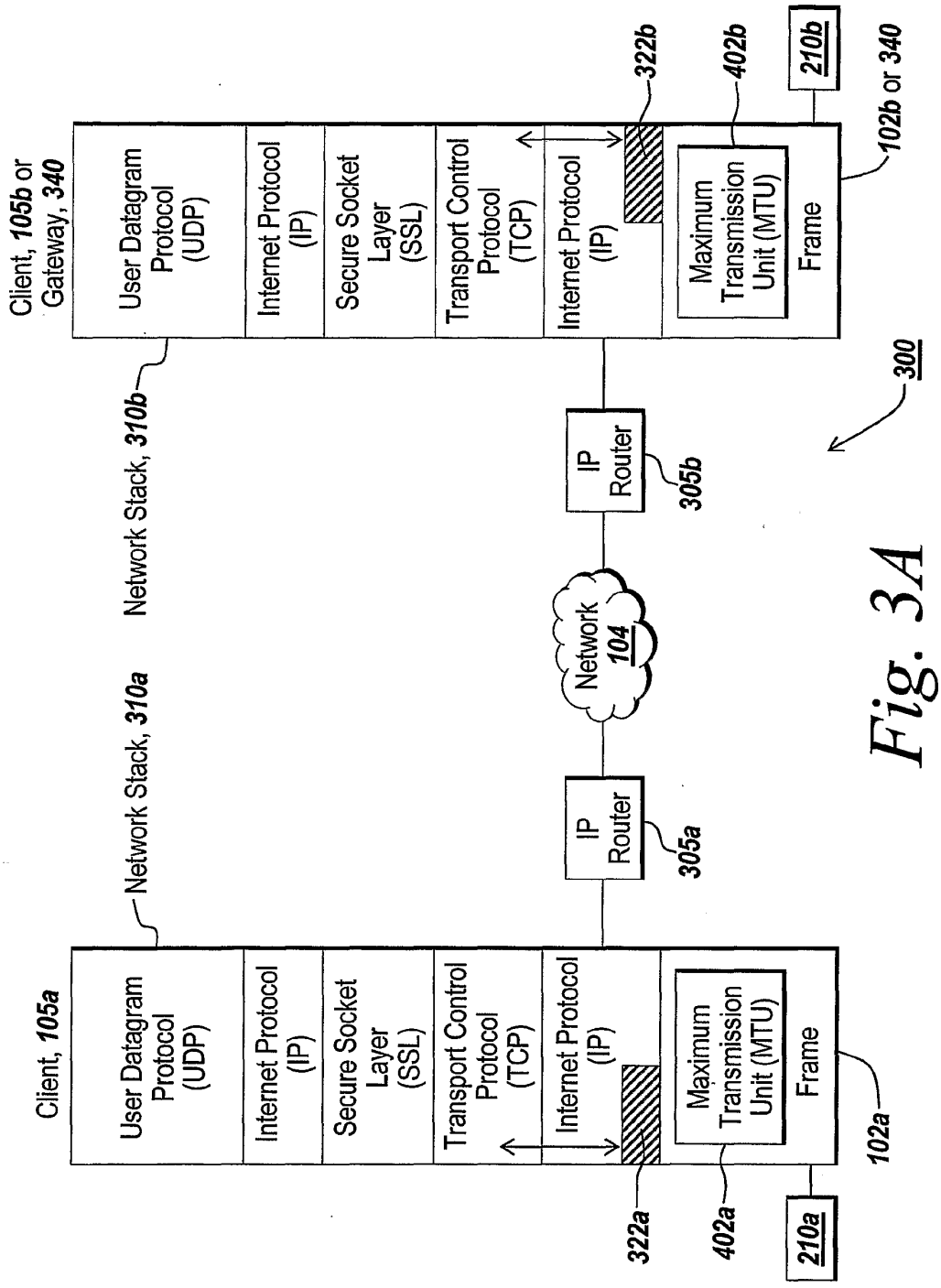

Client, 105a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
Network Stack, 310a
IP Router
305a
Network 104
IP Router
305b
Network Stack, 310b
Client, 105b or Gateway, 340
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
322a
402a
210a
102a
322b
402b
210b
102b or 340
300

Fig. 3A

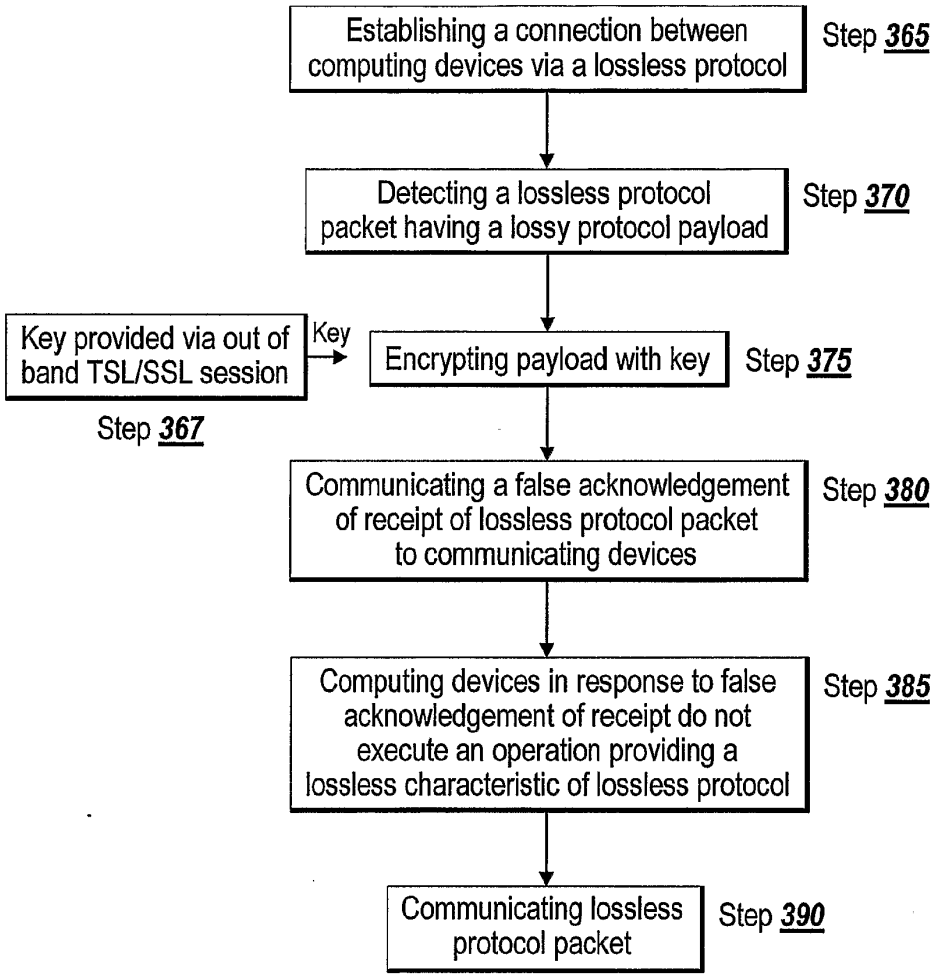

Establishing a connection between computing devices via a lossless protocol
Step 365
Detecting a lossless protocol packet having a lossy protocol payload
Step 370
Key provided via out of band TSL/SSL session
Key
Encrypting payload with key
Step 375
Step 367
Communicating a false acknowledgement of receipt 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

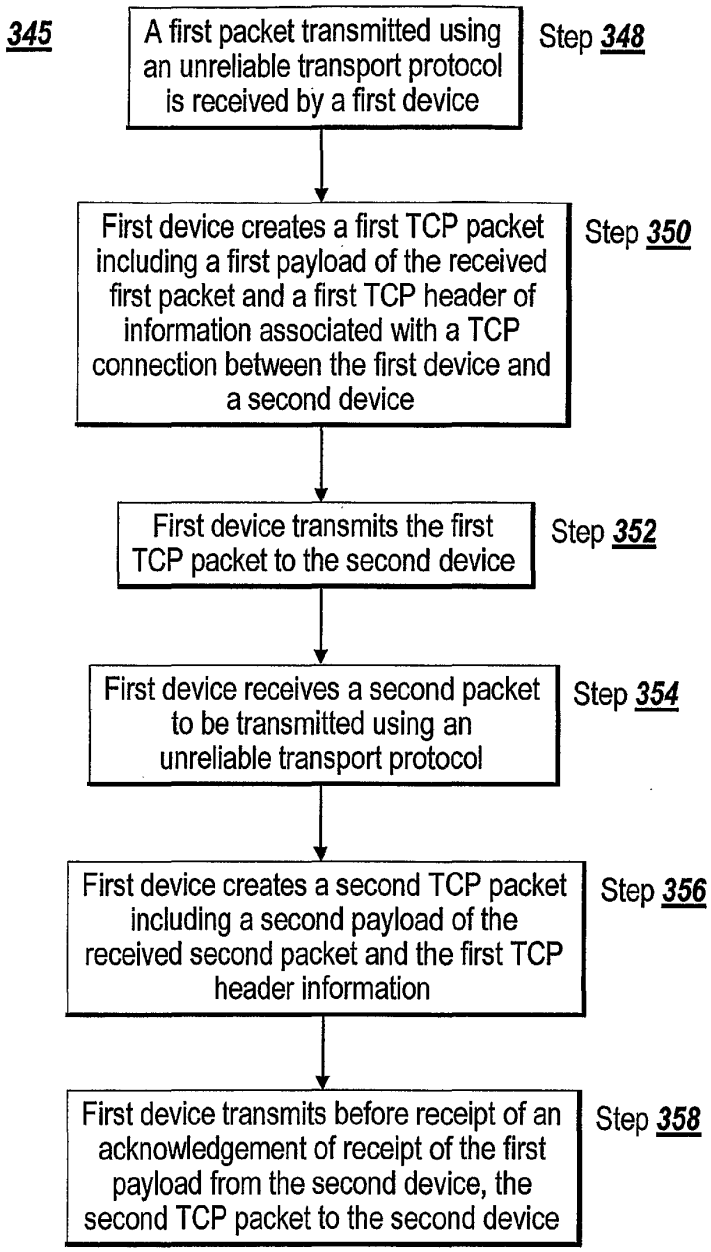

345
A first packet transmitted using an unreliable transport protocol is received by a first device
Step 348
First device creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection between the first device and 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

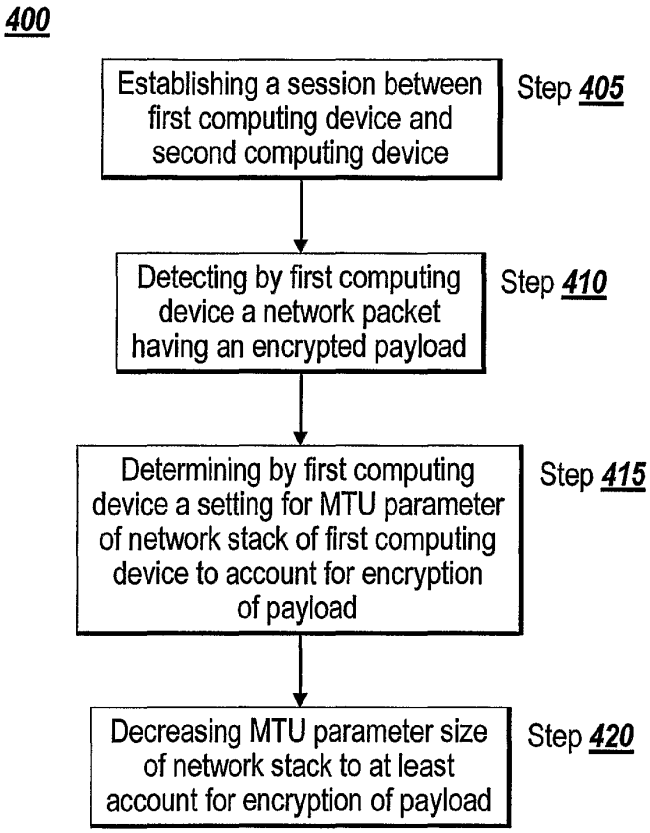

400
Establishing a session between first computing device and second computing device
Step 405
Detecting by first computing device a network packet having an encrypted payload
Step 410
Determining by first computing device a setting for MTU parameter of network stack of first computing device to account 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

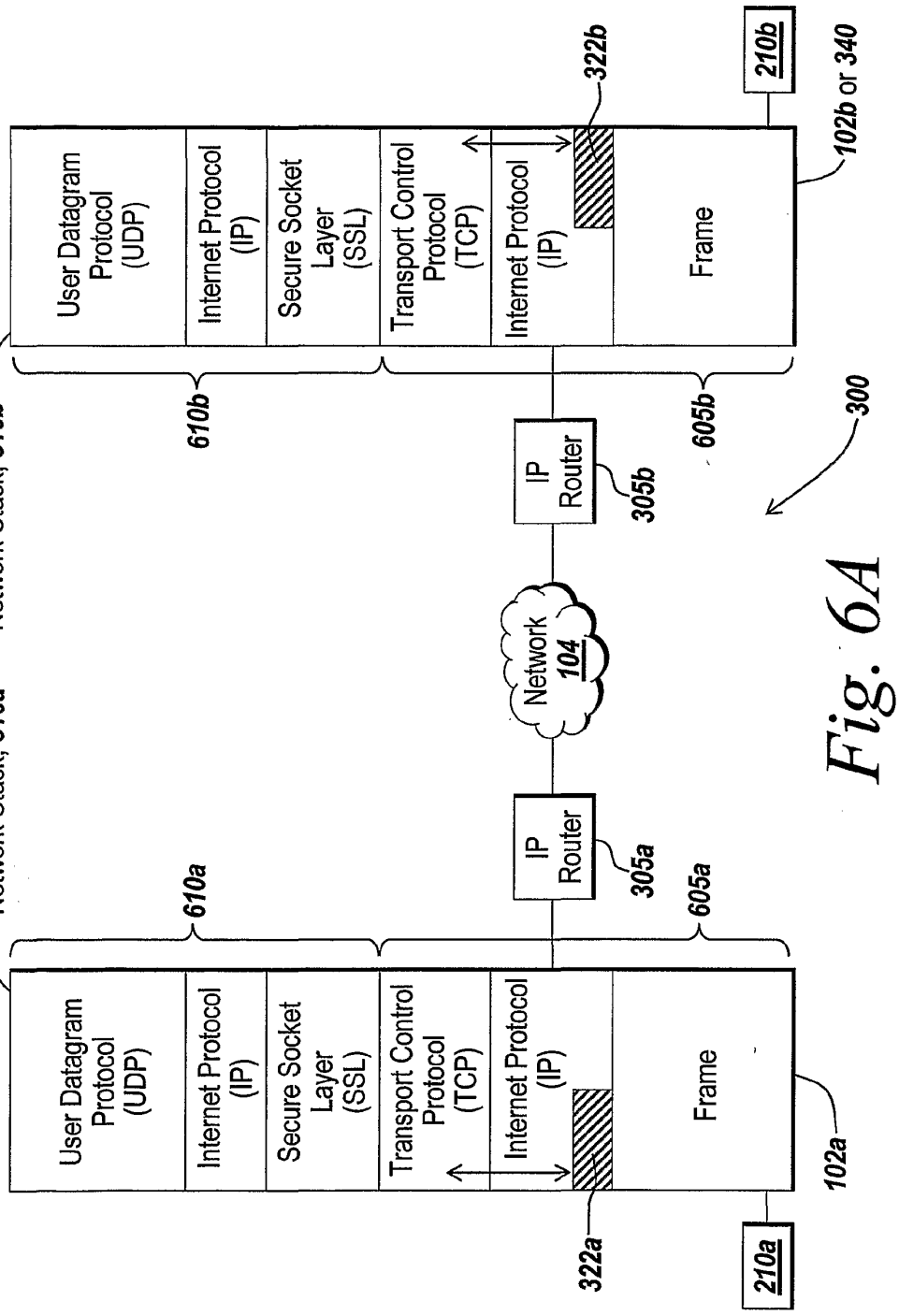

Network Stack, 310b
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Frame
322b
210b
102b or 340
610b
605b
300
IP Router
305b
Network 104
IP Router
305a
Network Stack, 310a
610a
605a
322a
210a
102a

Fig. 6A

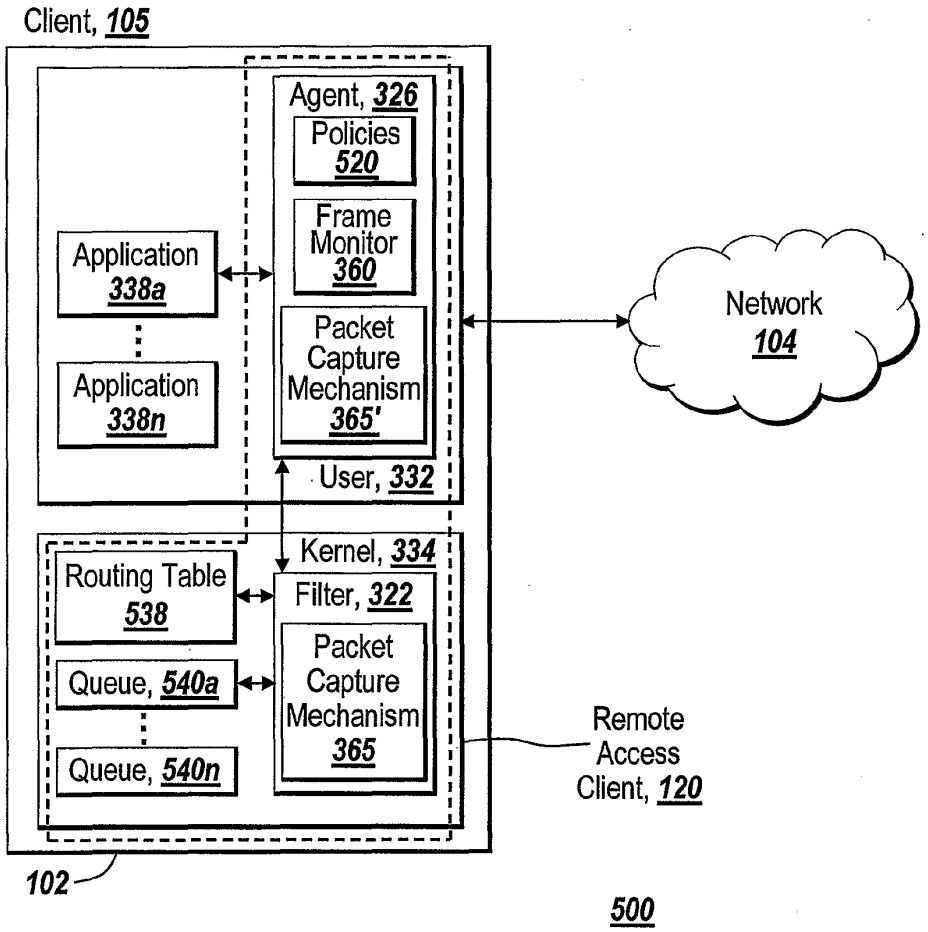

Client, 105
Agent, 326
Policies 520
Frame Monitor 360
Application 338a
Application 338n
Packet Capture Mechanism 365'
Network 104
User, 332
Kernel, 334
Routing Table 538
Filter, 322
Queue, 540a
Queue, 540n
Packet Capture Mechanism 365
Remote Access Client, 120
102
500

Fig. 5A

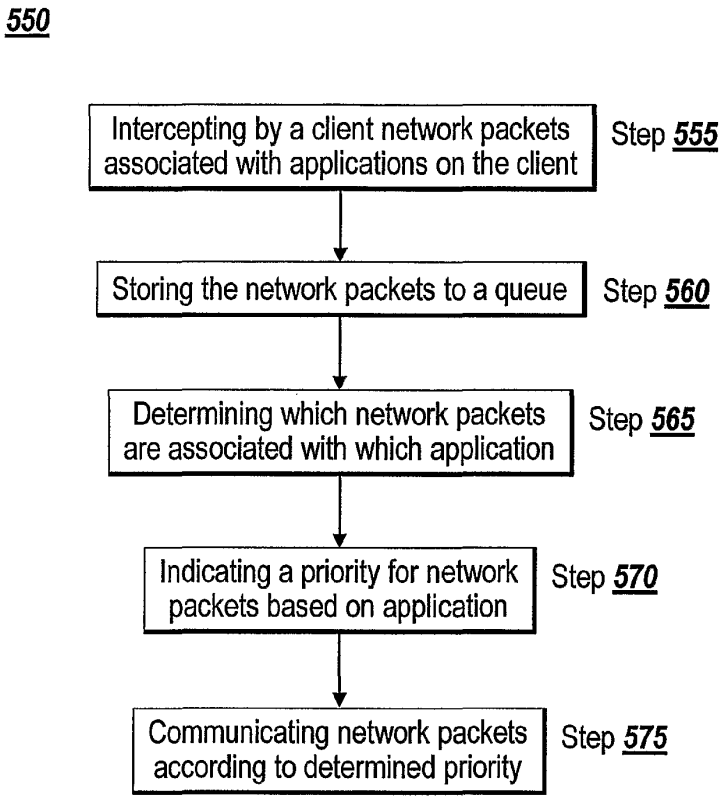

550
Intercepting by a client network packets associated with applications on the client
Step 555
Storing the network packets to a queue
Step 560
Determining which network packets are associated with which application
Step 565
Indicating a priority for network packets based on application
Step 570
Communicating network packets according to determined priority
Step 575

Fig. 5B

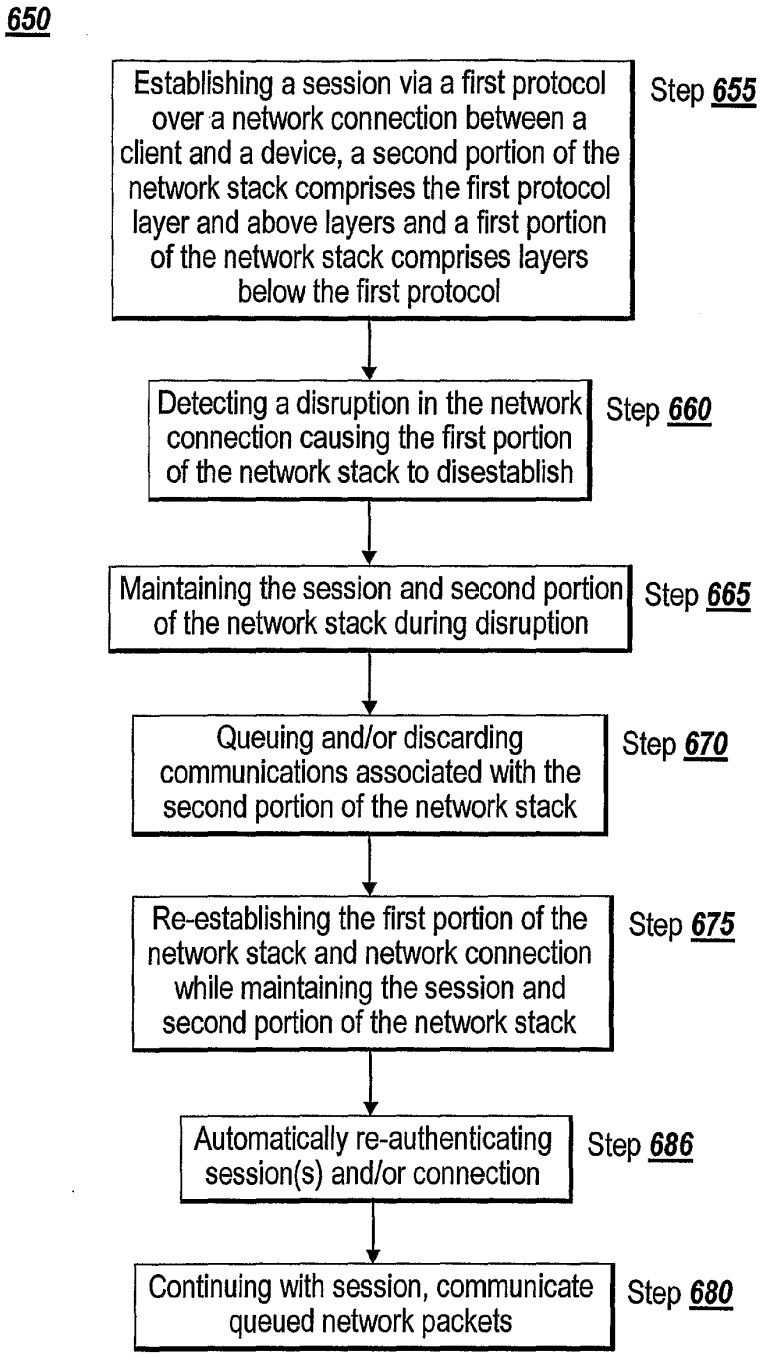

650
Establishing a session via a first protocol over a network connection between a client and a device, a second portion of the network stack comprises the first protocol layer and above layers and a first portion of the network stack comprises layers below the first protocol
Step 655
Detecting a disruption 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

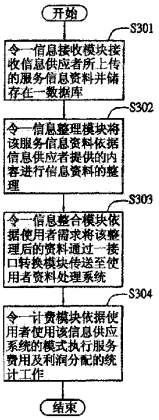
[74] 专利代理机构 北京三幸商标专利事务所
代理人 刘激扬

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

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

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

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

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

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。

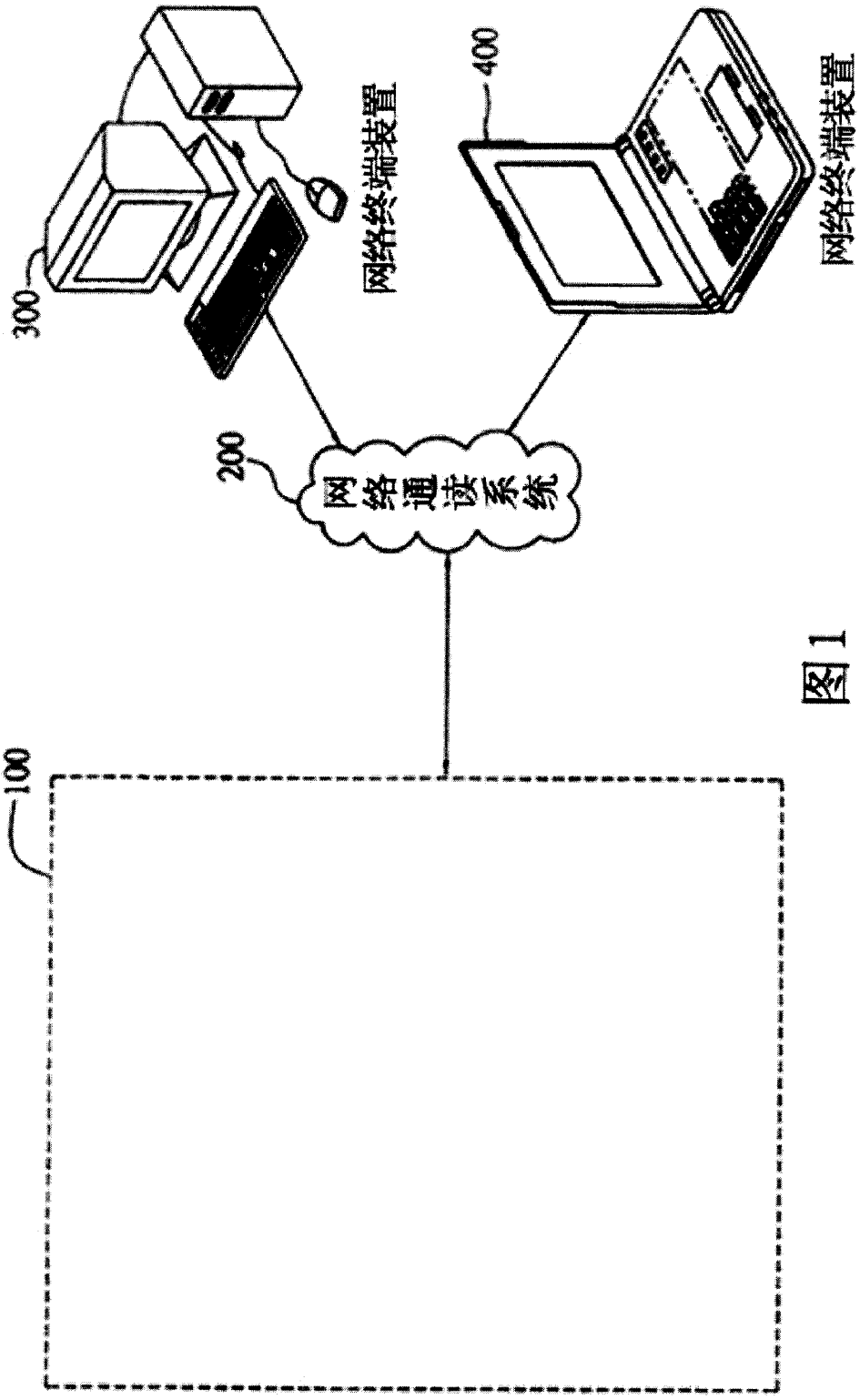


图 1

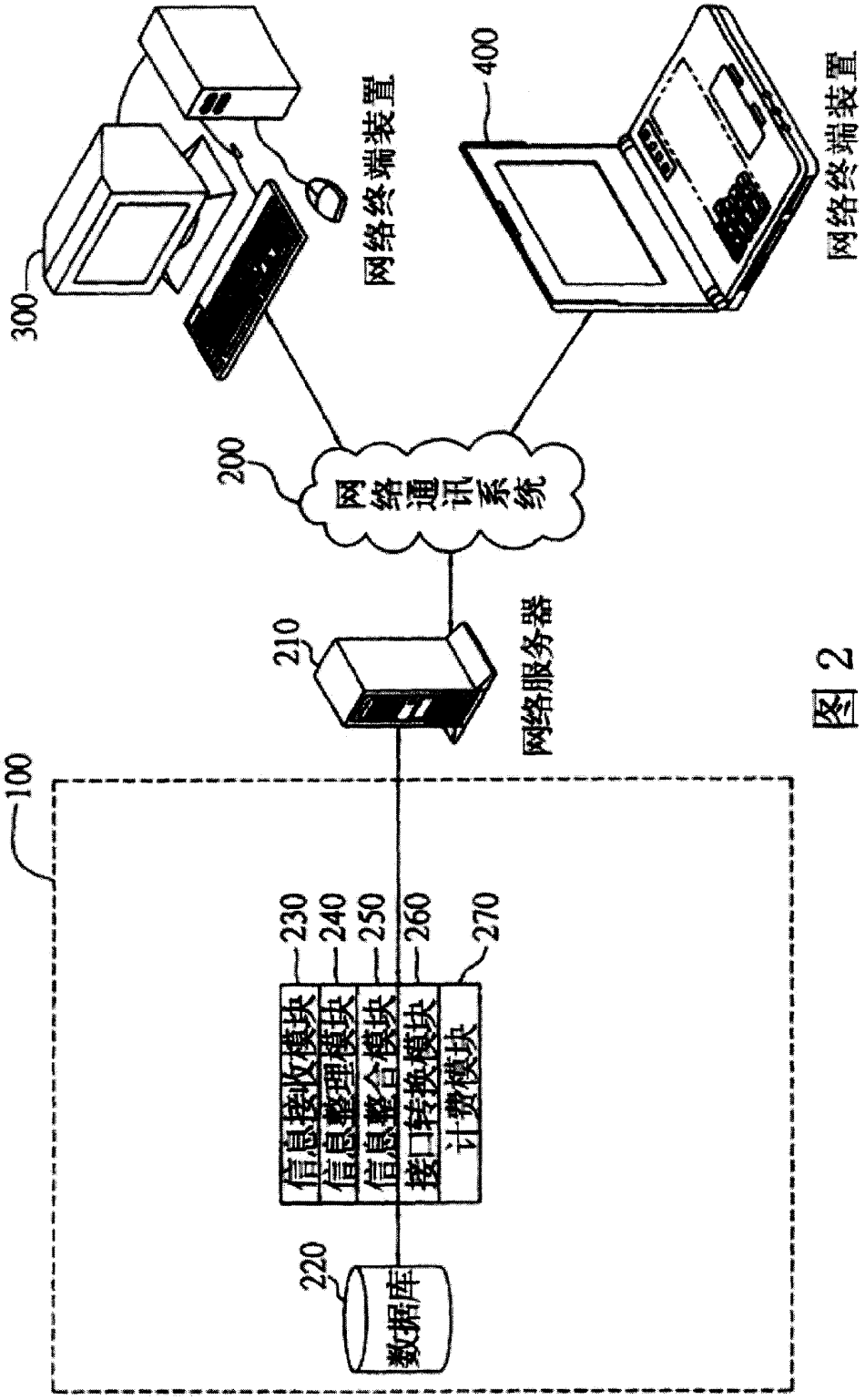

300
网络终端装置
400
网络终端装置
200
网络通讯系统
210
网络服务器
100
230
240
250
260
270
信息接收模块
信息整理模块
信息整合模块
接口转换模块
计费模块
220
数据库

图 2

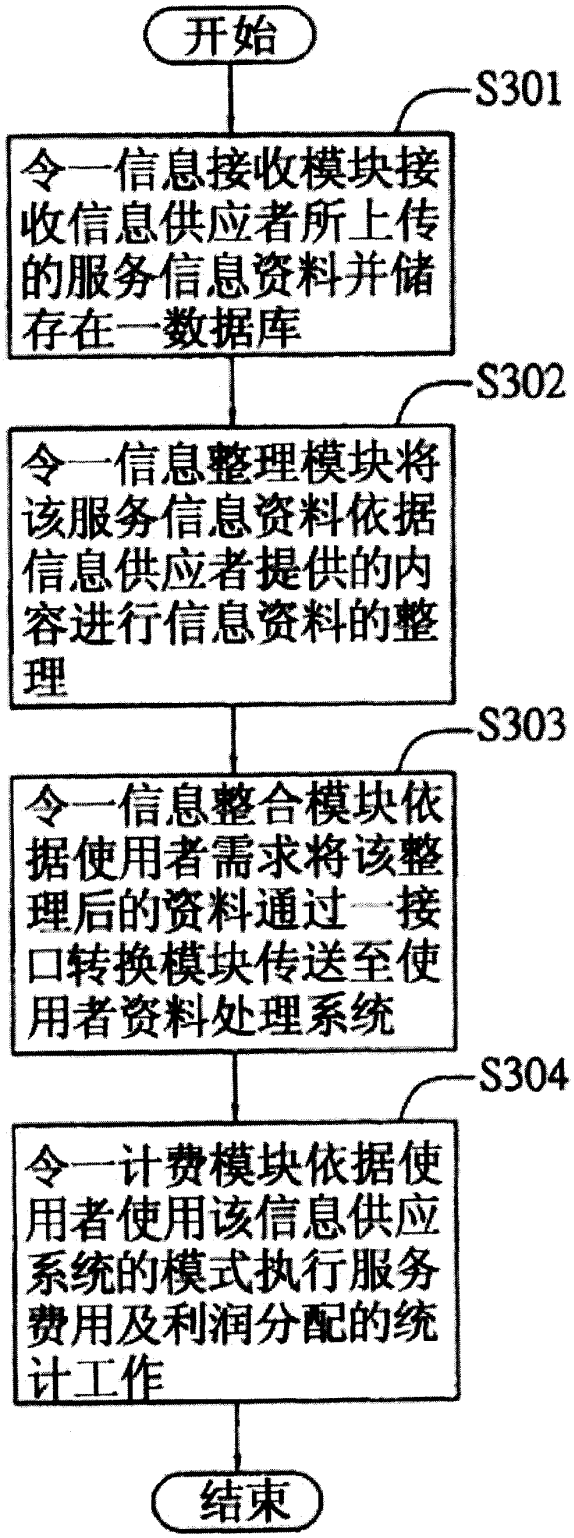

开始
S301
令一信息接收模块接收信息供应者所上传的服务信息资料并储存在一数据库
S302
令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行信息资料的整理
S303
令一信息整合模块依据使用者需求将该整理后的资料通过一接口转换模块传送至使用者资料处理系统
S304
令一计费模块依据使用者使用该信息供应系统的模式执行服务费用及利润分配的统计工作
结束

图 3

Annie

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, 吴鸿祺
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

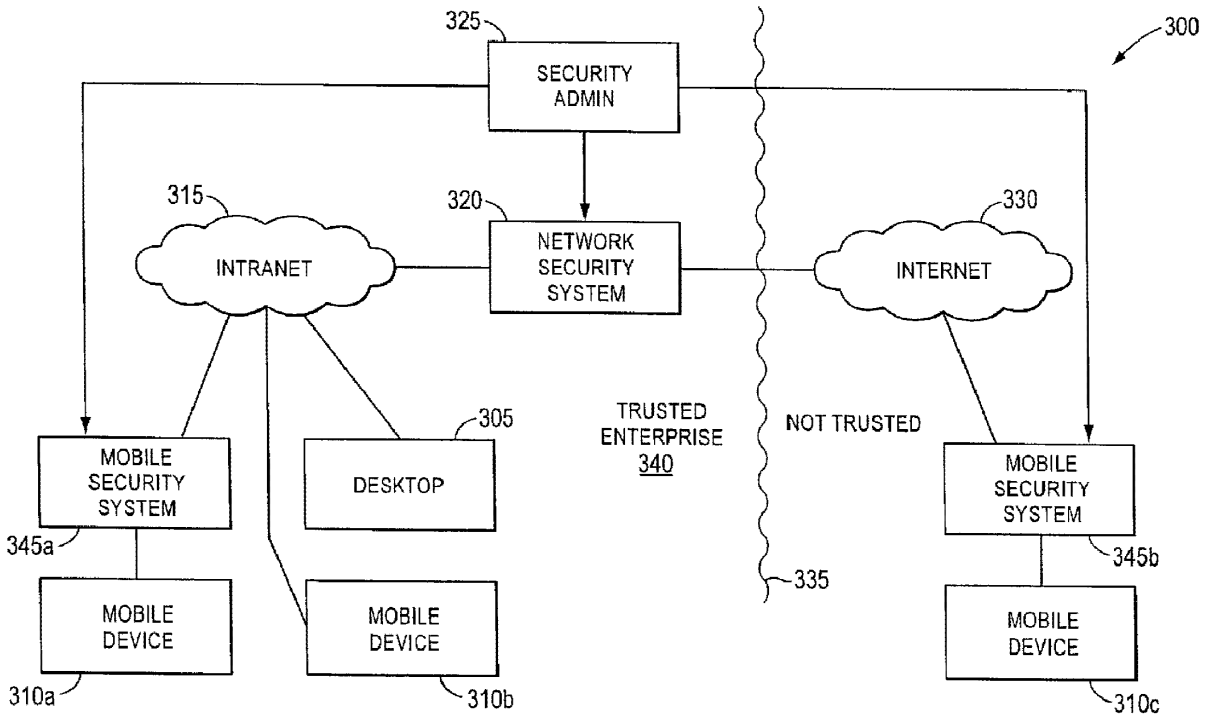


FIG. 3

(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

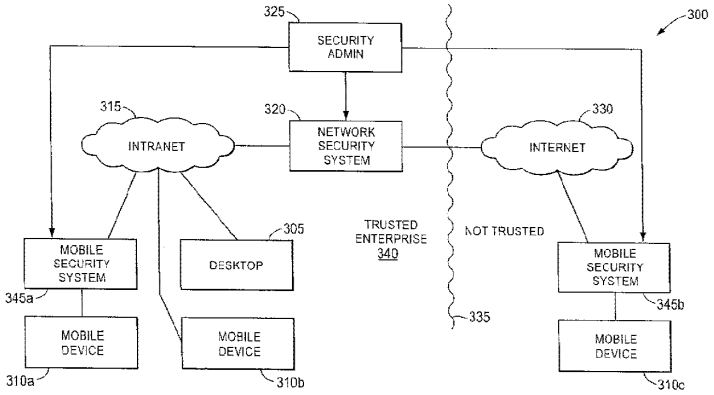


FIG. 3

(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.

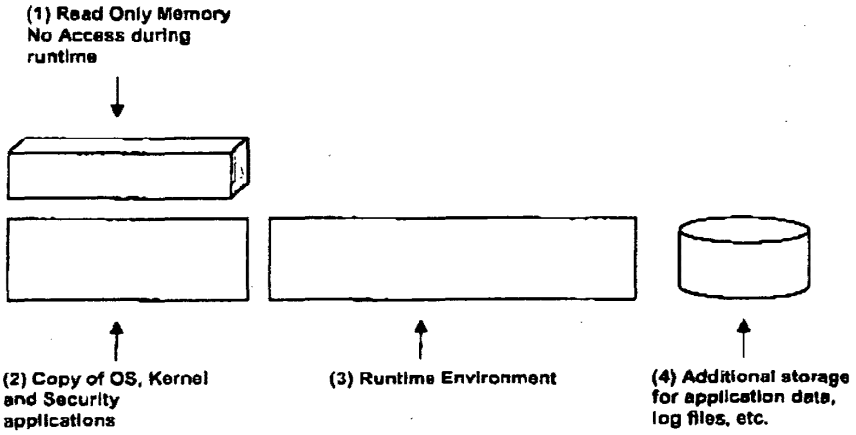
One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled 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.