

Clarke, Modet & Co.

COLOMBIA
E-MAIL: clarkemo@colomsat.net.co
SANTAFÉ DE BOGOTÁ, A.A. 92397

SUPERINDUSTRIA Y COMERCIO

Radicación : 00032800 00000002 Folios: 96
Fecha (AMD): 2000-07-11 15:40:59
Trámite : 002 PATENTES D 1 REGISTRO/ 441 RESPUESTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

SEÑOR JEFE
DIVISION DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
E. S. D.

COD 08

REF.: SOLICITUD DE PATENTE
EXPEDIENTE No 00032800
SOLICITANTE: SHARINGA NETWORKS INC.
PATENTE: UN MÉTODO Y SISTEMA DE ACCESO A UNA RED DE
COMUNICACIONES
FECHA DE SOLICITUD: MAYO 8 DE 2.000

ASUNTO: CONTESTACIÓN AUTO

DILIA RODRIGUEZ D'ALEMAN, en mi condición de apoderada de la sociedad solicitante, por el presente escrito doy respuesta a su auto notificado por estado de Mayo 25 de 2.000, sometiendo a su consideración los siguientes documentos y aclaraciones:

1. DOCUMENTOS:

1. El documento de PODER otorgado a mi favor, junto con la prueba de existencia y representación legal del solicitante, debidamente legalizados.

Su traducción oficial al Español debidamente avalada por el Ministerio de Relaciones Exteriores.

2. Copia certificada de la prioridad Australiana PQ 3682 de Mayo 6 de 1999 y su traducción.
3. Nuevo juego de dibujos formales y con letreros en idioma español.
4. Arte final de la figura N°. 1, por ser la más representativa de la invención.

ACLARACIONES:

1. Su Despacho objeta la reivindicación 26 y propone su retiro.

El solicitante acoge el criterio del Señor Examinador y en tal virtud retira la reivindicación 26.

En consecuencia se presenta la página 29 del capítulo reivindicatorio, eliminando dicha reivindicación.



Clarke, Modet & Co.

COLOMBIA

E-MAIL: clarkemo@colomsat.net.co
SANTAFÉ DE BOGOTÁ, A.A. 92397

En el evento que resultara alguna discrepancia de carácter técnico, manifiesto expresamente que el solicitante mantiene interés en la solicitud por lo que quedo a disposición de atender a las observaciones formales y técnicas que su Despacho requiera antes o durante el examen de fondo, evitando el archivo de la solicitud.

Señor Jefe,

DILIA RODRIGUEZ D'ALEMAN

CCR/srr

P- 330

Clarke, Modet & Co. Colombia Ltda.

PROPIEDAD INDUSTRIAL y DERECHOS DE AUTOR

Apartado Aéreo 92397
Santafe de Bogotá, Colombia

PODER

Yo (nosotros), abajo firmante(s)

Sydney Gordon Low

en mi (nuestro) carácter de representante(s) legales de

Sharinga Networks Inc.

una sociedad organizada y existente de acuerdo con las leyes de

Estados Unidos de América

y en actual cumplimiento de su objeto social, con domicilio en

1310 King Street, Wilmington, New Castle
County Delaware USA 19801

por el presente instrumento confiero (conferimos) poder especial a favor de DILIA MARIA RODRIGUEZ D'ALEMAN, con Cédula de Ciudadanía No. 41.654.882 de Bogotá y tp. 20824 y CLAUDIA LUCIA CARO RAMIREZ, con Cédula de Ciudadanía No. 40.017.374 de Tunja, y tp. 36448, con domicilio en Santa Fé de Bogotá, Colombia, para que actuando en su orden en nombre del (de la) otorgante le (la) representen ante cualquier entidad, autoridad y/o persona, especialmente ante las del orden Administrativo, Contencioso Administrativo, Judicial, Tribunales de Arbitramento y/o cualquier otro en lo referente a los siguientes asuntos:

- 1) Solicitar, tramitar, obtener y/o registrar cualquiera de las modalidades de Propiedad Industrial, tales como: patentes de invención, modelos de utilidad; diseños industriales, variedades vegetales; marcas, lemas, nombres y enseñanzas comerciales y denominaciones de origen; así como sus renovaciones, prórrogas, transferencias, cambios de nombre y/o domicilio, contratos y licencias.
- 2) Solicitar, tramitar, obtener y/o registrar derechos de autor, en cualquiera de sus presentaciones así como la protección de secretos industriales y know-how.
- 3) Solicitar, tramitar, obtener y/o registrar registros sanitarios, permisos y/o licencias de funcionamiento; así como sus renovaciones o prórrogas, transferencias, cambios de nombre y/o domicilio, contratos y licencias.
- 4) Ejercer acciones de oposición, observación, reclamos, reconsideración, reposición, apelación, cancelación administrativa o judicial, nulidad, protección al consumidor, concesión de licencias, protección de secretos industriales y demás acciones y recursos relacionados con derechos derivados de los asuntos arriba indicados y en contra de la competencia desleal, acciones derivadas de la obtención o explotación de licencias, acciones de indemnización de perjuicios. También podrá(n) intervenir en juicios civiles, comerciales, penales, contencioso-administrativos, tutelas y de policía; en acciones o juicios promovidos por el (la) mandante o en contra el (ella).
- 5) Registrar nombres de dominio ante la entidad competente.
- 6) En el ejercicio de este mandato los mandatarios arriba mencionados quedan facultados para: conciliar, cancelar, transigir, comprometer en árbitros, desistir, recibir y tomar posesión de la cosa objeto de litigio y renunciar o desistir a derechos concedidos o en curso de concesión, admitir los hechos del proceso.
- 7) Ratificar o no la agencia oficiosa.
- 8) Así mismo faculto (facultamos) a los mencionados apoderados para recibir notificaciones y designar apoderados judiciales o extrajudiciales, sustituir el presente poder y revocar las sustituciones que hicieren.

Dado y firmado en Melburne Victoria

a los 25 días de Mayo/2000 de
SHARINGA NETWORKS INC

X

Firma / signature

POWER OF ATTORNEY

I (we), the undersigned

X SYDNEY GORDON LOW

legal representative(s) of

SHARINGA NETWORKS INC

an organization existing under the laws of

United States

and in present execution of its business activity, domiciled at

1310 King Street, Wilmington, New Castle County

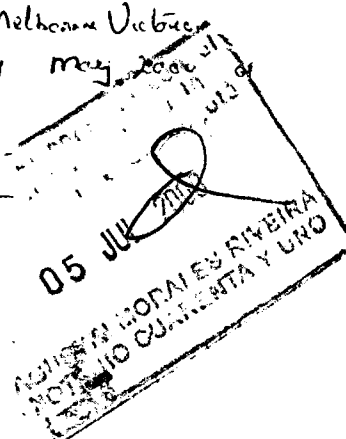
Delaware, United States of America 19801

do hereby grant POWER OF ATTORNEY to DILIA MARIA RODRIGUEZ D'ALEMAN, identification card No. 41.654.882 of Bogotá, and tp. 20824 and CLAUDIA LUCIA CARO RAMIREZ, tp. 36448, identification card No. 40.017.374 of Tunja, residing in Santa Fé de Bogotá, Colombia, to act in the order of their appointment in behalf of grantor before any entity, authority and/or natural or juridical person, specially before those Administrative, Administrative-Contentious, Judicial, arbitration courts, and/or any other, in all matters concerning the following:

- 1) To apply, process, obtain and/or register any of the modalities of Industrial Property, such as: Patents of Invention, Utility Models, Designs, vegetal varieties; Marks, Slogans, Trade Names and emblems and appellations of Origin; as well as their renewals, extensions, assignments, changes of name and/or domicile, agreements and licenses.
- 2) To apply, process, obtain and/or register copyrights of any kind as well as protection of industrial secrets or know-how.
- 3) To apply, process, obtain and/or register sanitary registrations, operating authorizations and/or licenses; as well as their renewals or extensions, assignments, changes of name and/or domicile, agreements and licenses.
- 4) To bring actions of opposition, observations, claims, reconsideration, appeal or legal remedies, cancellations, nullity, protection to the consumer, granting of licenses, protection of trade secrets and other actions related with rights derived from the above-mentioned matters and against the unfair competition, actions resulting from the obtention or exploitation of licenses, recovering damages actions. They can also intervene or participate in Civil, Commercial, Criminal or Contentious-Administrative Trials; the actions for writ mandamus, police actions; in actions, lawsuits or litigations instituted by the grantor or against him.
- 5) To register domain names before the competent entity.
- 6) To the effect of this mandate the above-named proxy are empowered to: conciliate, cancel, settle, submit to arbitration, withdraw and to receive and take possession of the litigation related object and waive or renounce the rights granted or in process of granting, admit the facts of the case.
- 7) To ratify or not the officious agency.
- 8) I (we) hereby appoint the afore mentioned attorneys with powers to receive notifications and to designate judicial and extrajudicial attorneys substitute this Power of Attorney and to revoke such substitutions.

X Granted and signed at Melburne Victoria

X on this 25 day of May 2000



65-604

CERTIFICADO NOTARIAL (Cuando el solicitante es SOCIEDAD)

(Poderes otorgados en: El Salvador, Estados Unidos, México y Venezuela)

A los _____ días del mes de _____
de _____, el Notario que suscribe DA FE de
que:

1. _____
(nombre de la persona que firma el poder)

mayor de edad y domiciliado _____
firmó de su puño
y letra el documento que antecede.

2. Conoce al (a) otorgante y que este (a) está
legalmente capacitado para el otorgamiento.

3. El otorgante ha firmado el referido documento en
su carácter de _____
de la persona jurídica _____

4. La citada persona jurídica con sede en _____
está
legalmente constituida, que tiene actualmente
existencia legal y que el acto para el cual se ha
otorgado este poder está comprendido entre los que
constituyen su objeto social.

5. El otorgante tiene efectivamente la representación
que ostenta, que esta es legítima y que está
facultado para otorgar este poder.

6. Las anteriores certificaciones de los puntos 3, 4 y 5, me
constan porque he tenido a la vista los
documentos auténticos.

CHARLES BERNARD CORE BRETT
NOTARY PUBLIC

111-112 COLLEEN STREET

Notario Público MELBOURNE VIC
AUSTRALIA

NOTA: A continuación de lo anterior, el Consul de
Colombia debe autenticar la firma del Notario Público.

CERTIFICADO NOTARIAL (Cuando el solicitante es INDIVIDUO)

A los _____ días del mes de _____
de _____, el Notario que suscribe DA FE de
que:

1. _____
(nombre de la persona que firma el poder)

mayor de edad y domiciliado en _____
firmó en su presencia
el documento que antecede, conoce al otorgante
y que este está legalmente capacitado para el
otorgamiento.

Notario Público

NOTA: A continuación de lo anterior, el Consul de
Colombia debe autenticar la firma del Notario Público.

Para todos los demás países el Señor Consul de
Colombia o ante quien se otorgue, debe expedir una
certificación dejando constancia 1) de la existencia
legal de la sociedad, 2) de que esta ejerce actualmente
su objeto social, y 3) de que la persona o personas que
otorgan el poder están facultadas para hacerlo, dejando
constancia así mismo de que tuvo a la vista las pruebas
que acreditan tales circunstancias.

X NOTARIAL CERTIFICATE (When the applicant is a CORPORATION)

(Powers of attorney granted in: El Salvador, Mexico, U.S.A and Venezuela)

This 25th day of May 2000
the undersigned Notary CERTIFIES that

1. SYDNEY GORDON LOW
(name of the person who signs the power of attorney)

of legal age and domiciled
in MELBOURNE VICTORIA
set his hand on the foregoing document.

2. The grantor is to him personally known and that
he/she has legal capacity to execute the document.

3. The grantor has executed the foregoing document
in his capacity of DIRECTOR
of the juridical person SHARINGA
NETWORK INC

4. The mentioned juridical person with place of
business in DELAWARE USA
is duly organized, has actual legal existence and that
the purposes for which the power of attorney is granted
are within the scope of its corporate purposes.

5. The grantor has in fact the referred quality and
that his/her representation is legal and that he/she
is empowered to grant this power of attorney.

6. I have based the above certifications 3, 4 and 5, on
the authentic documents which for such purpose were
exhibited to me.

NOTA: Then the Colombian Consul
signature of the Notary Public.

NOTARIAL CERTIFICATE (When the applicant is an INDIVIDUAL)

On this _____ day of _____
the undersigned Notary CERTIFIES that

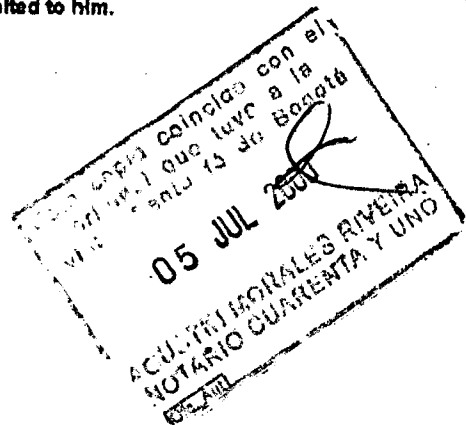
1. _____
(name of the person who signs the Power of Attorney)

of legal age and domiciled at _____
signed in his presence
the foregoing document. the grantor is to him
personally known and that he/she has legal capacity to
execute the document.

Notary Public

NOTA: Then the Colombian Consul must legalize the
signature of the Notary Public.

For all other countries the Colombian Consul or before
who it is granted must issue a certification stating 1) the
legal existence of the corporation, 2) that the corporate
purposes are actually being accomplished, 3) that the
person or persons who grant this Power of Attorney are
empowered to do it. The Consul will certify also that the
documents evidencing those circumstances were
exhibited to him.



REGISTRATION OFFICIAL No. 2000/132
M. C. DE PIPOPIBITA
CALLE 13 DE
BOGOTÁ
D.F.S. No. 423 DEL M. C. DE JUSTICIA

66 613

RANU VATANA an official of the Department of Foreign Affairs and Trade, Australia DO HEREBY CERTIFY that the following is a true and correct copy of the documents above mentioned and that the signature of CHARLES BERNARD CORE BRETT appearing in the City of MELBOURNE in the State of VICTORIA Australia, and that the seal impressed is the Official Seal of the said CHARLES BERNARD CORE BRETT in so doing I certify that the Department endorses, in accordance with the provisions of the Statute in that behalf made, the accuracy of the contents of the document.

Given under my hand and the seal of the Department of Foreign Affairs and Trade this 29th day of MAY Two Thousand (2000)



EL CONSULADO DE COLOMBIA EN
SYDNEY 13/00 1/6/00

Previa la confrontacion correspondiente DA FE de que la firma que aparece en este documento es similar a la REGISTRADA aqui por RANU VATANA, OFICIAL DEL DEPARTAMENTO DE RELACIONES EXTERIORES Y COMERCIO DE MELBOURNE, AUSTRALIA



J. Alzamor
JOAQUIN ALFREDO ALZAMORA CAMPO
CONSUL GENERAL

PAGADOS: IMPUESTO DE TIMBRE: US\$7.00
DERECHOS CONSULARES: US\$15.00

MINISTERIO DE RELACIONES EXTERIORES
28/1/4
CUBA FIRMADA ADECE EN EL DOCUMENTO DE SEMPERA LAS FIRMAS INDICADAS
NO SE ASUME RESPONSABILIDAD DEL TEXTO
2000 JUN 19 A 10:29
RELACIONES EXTERIORES
SECRETARIA DE BOGOTÁ-B.C.
PRODUCCION OFICIAL NO. 2000/132
HIDRAULICA DE PIEDRANTA
RES. No. 313 DEL MIN. DE JUSTICIA
05 JUL 2000
JOSÉ MANUEL RIVERA
CÓDIGO CUARENTA Y UNO

67⁶62

TRADUCCIÓN OFICIAL No.2000/132 de un documento escrito en inglés, el cual para su identificación se sella con el sello del traductor al tiempo con la presente. Esta traducción ha sido preparada por Hilda Aguilera de Piedrahita traductora e intérprete oficial debidamente reconocida por el Ministerio de Relaciones Exteriores y autorizada por el Ministerio de Justicia y del Derecho, por resolución número 323 de 1980.

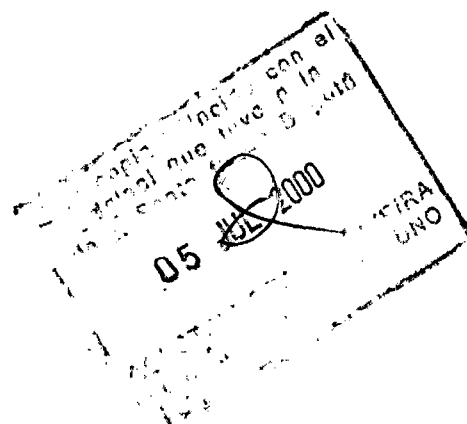
(Se traduce un Certificado Notarial y sus legalizaciones otorgados por la compañía Sharinga Networks Inc., escritos en inglés, adjuntos a un poder escrito en inglés y español.)

CERTIFICADO NOTARIAL (SOCIEDADES)

(Poderes otorgados en El Salvador, México, Estados Unidos de América y Venezuela)

Expedido hoy 25 de Mayo del 2000, el suscrito Notario CERTIFICA que:

- 1) Sidney Gordon Low, mayor de edad y domiciliado en Melbourn, Victoria, suscribió el anterior documento.
- 2) El otorgante le es conocido personalmente y tiene capacidad para firmar el documento.
- 3) El otorgante ha suscrito el anterior documento en su calidad de Director de la persona jurídica Sharinga Network Inc.



6863*

- 4) La mencionada persona jurídica con domicilio comercial en Delaware, Estados Unidos de América, está debidamente constituida, tiene actualmente existencia legal y el fin para el cual se otorga este poder se encuentra dentro de su objeto social.
- 5) El otorgante tiene en efecto la capacidad referida y su representación es legal y está autorizado para otorgar este poder.
- 6) Fundamento las certificaciones 3), 4) y 5) en los documentos auténticos que para tal fin me fueron exhibidos.

(Firmado) Ilegible

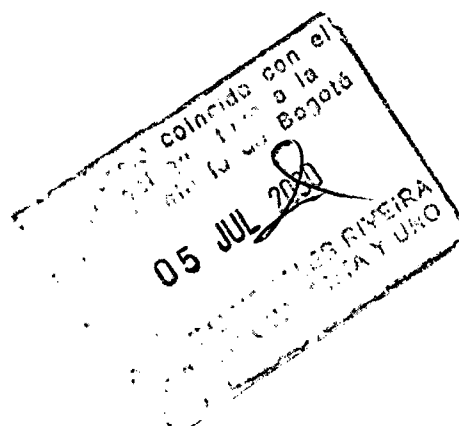
Notario Público

(Sello Notarial de Oblea)

(Sello Notarial a Tinta: CHARLES BERNARD GORE BRETT, NOTARIO PÚBLICO, Nivel 3, 12 Collins Street, Melbourne Vic, Australia)

Nota: El Consulado de Colombia debe autenticar la firma del Notario Público.

(Sello a tinta: Yo, Ranu Vatana, funcionario del Departamento de Relaciones Exteriores y Comercio, Australia, POR EL PRESENTE CERTIFICO que esta firma, de CHARLES BRETT, que aparece al respaldo de los documentos



PRODUCCION ORIGINAL No. 2000/32

69 64 8

adjuntos es la firma auténtica de CHARLES BERNARD GORE BRETT, Notario Público residente en la ciudad de Melbourne en el Estado de Victoria, Australia, que el sello impreso es el Sello Oficial del mencionado CHARLES BERNARD GORE BRETT. En la certificación, ni yo ni el departamento asumimos responsabilidad alguna en relación con el contenido del documento. Dado bajo mi firma y Sello del Departamento de Relaciones Exteriores y Comercio hoy 29 de Mayo del Dos Mil (2000)).

(Sello a Tinta del Departamento de Relaciones Exteriores y Comercio en Melbourne)

EN ESPAÑOL, autenticación 131/00 de la firma que antecede por el Consulado de Colombia en Sidney de Junio 1, 2000. Pagados el Impuesto de Timbre y los Derechos Consulares, por valor de veintidós dólares (US\$22).

Autenticación por el Ministerio de Relaciones Exteriores Número 283114, de Junio 19 del 2000, suscrita por el Jefe de Legalizaciones.

ES TRADUCCIÓN FIEL Y COMPLETA de la cual se deja copia en los archivos de esta oficina para su confrontación y a la cual me remito.

Santafé de Bogotá, Junio 26 del 2000.

Hilda Aguilera de Piedra

TRADUCCION OFICIAL No. 2000/132
HILDA AGUILERA DE PIEDRA
INTERPRETE OFICIAL
CPS No. 373 DEL MIN. DE JUST.

3

MINISTERIO DE RELACIONES
EXTERIORES
Hilda Aguilera
087461
CUYA FIRMA SE ENCUENTRA EN EL
DOCUMENTO LEGALIZADO
LAS FIRMAS CUYAS FIRMAS

NO SE ASUME
RESPONSABILIDAD
05 JUN 2000
A las 10:17
M. Jarama
OFICINA DE LEGALIZACIONES
2000 JUN 29

State of Delaware
Office of the Secretary of State

PAGE 1

65 9
70

I, EDWARD J. FREEL, SECRETARY OF STATE OF THE STATE OF DELAWARE, DO HEREBY CERTIFY THE ATTACHED IS A TRUE AND CORRECT COPY OF THE CERTIFICATE OF INCORPORATION OF "SHARINGA NETWORKS INC.", FILED IN THIS OFFICE ON THE TENTH DAY OF NOVEMBER, A.D. 1999, AT 9 O'CLOCK A.M.

A FILED COPY OF THIS CERTIFICATE HAS BEEN FORWARDED TO THE NEW CASTLE COUNTY RECORDER OF DEEDS.

*I certify that this document is a
true and complete copy of the original*

Charles Bernard Gore Brett

CHARLES BERNARD GORE BRETT
NOTARY PUBLIC
LEVEL 3, 12 COLLINS STREET
MELBOURNE VIC
AUSTRALIA



Edward J. Freel

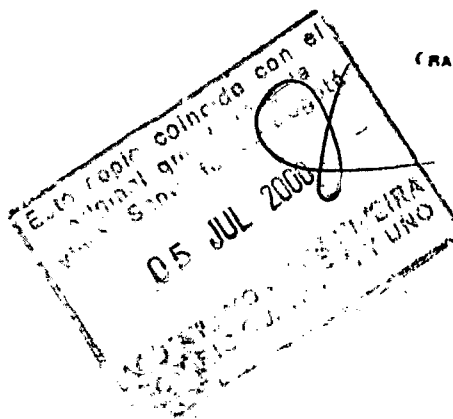
Edward J. Freel, Secretary of State

3122225 8100

991477990

AUTHENTICATION: 0075681

DATE: 11-10-99



TRADUCCION OFICIAL No. 2000/133
RECEIVED SECRETARIA DE ECONOMIA Y FINANZAS

66 10
74

I, RANU VATANA an officer
of the Department of Foreign Affairs and Trade, Australia
DO HEREBY CERTIFY that the signature
CHARLES BRETT
Appearing on the documents above/below/attached
herein is the true signature of
CHARLES BERNARD GORE BRETT
Minister Resident in the City of MELBOURNE
in the State of VICTORIA Australia, and
That this seal is the Official Seal of the said
CHARLES BERNARD GORE BRETT
in so far as it relates to the Department of Foreign Affairs
and Trade and as to the accuracy of the contents of
the documents.

Given under my hand and the seal of the Department of
Foreign Affairs and Trade this 29th day of MAY
(2000)



EL CONSULADO DE COLOMBIA EN
SYDNEY B2/00 1/6/00

Previa la confrontacion
correspondiente DA FE de que
la firma que aparece en este
documento es similar a la
REGISTRADA aqui por RANU VATANA,

OFICIAL DEL DEPARTAMENTO DE RELACIONES
EXTERIORES Y COMERCIO DE MELBOURNE, AUSTRALIA.

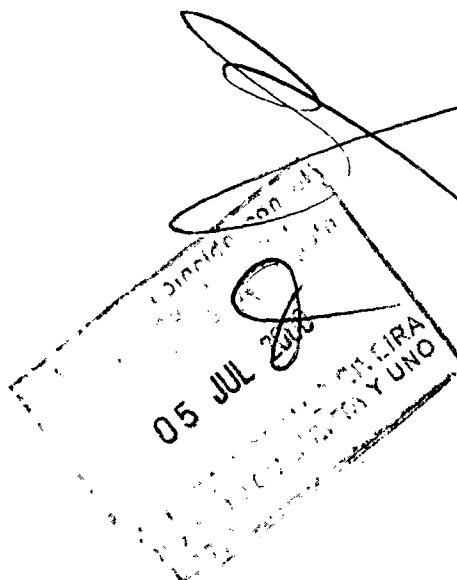


Alfonso Alzamora
ALFONSO ALZAMORA CAMPO
CONSUL GENERAL

PAGADOS: IMPUESTO DE TIMBRE: US\$7.00
DERECHOS CONSULARES: US\$15.00

MINISTERIO DE RELACIONES
EXTERIORES
283115
ALFREDO ALZAMORA
CUYA FIRMA APARECE EN EL
DOCUMENTO DESEMPENA
LAS FUNCIONES INDICADAS.
PRODUCCION ORIGINAL NO. 72201133
MILITARIA Y CIVIL DE PREPARACION
Y CONTROL DE DOCUMENTOS
RES. NO. 223 DEL MIN. DE JUSTICIA

NO SE ASUME
RESPONSABILIDAD DEL TEXTO
1991 JUN 19 A 10 29
RELACIONES
EXTERIORES
SANTO DOMINGO D.C.



CERTIFICATE OF INCORPORATION
OF
SHARINGA NETWORKS INC.

FIRST: The name of the corporation is Sharinga Networks Inc.

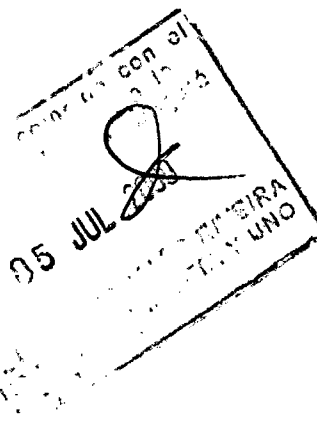
SECOND: The registered office of the corporation in the State of Delaware is located at 1310 King Street, Wilmington, New Castle County, Delaware 19801, and its registered agent is PJEKS Corporate Services, Inc.

THIRD: The purpose of the corporation and the nature and objects of the business to be transacted, promoted, and carried on are to engage in any lawful act or activity for which corporations may be organized under the General Corporation Law of Delaware.

FOURTH: The total number of shares of stock which the corporation shall have authority to issue is three thousand (3,000) shares of common stock, with no par value.

FIFTH: Whenever a compromise or arrangement is proposed between this corporation and its creditors or any class of them and/or between this corporation and its stockholders or any class of them, any court of equitable jurisdiction within the State of Delaware may, on the application in a summary way of this corporation or any creditor or stockholder thereof or on the application of any receiver or receivers appointed for this corporation under the provisions of section 291 of Title 8 of the Delaware Code or on the application of trustees in dissolution or of any receiver or receivers appointed for this corporation under the provision of section 279 of Title 8 of the Delaware Code, order a meeting of the creditors or class of creditors, and/or of the stockholders or class of stockholders of this corporation, as the case may be, to be summoned in such a manner as the said Court directs. If a majority in number representing three-fourths in value of the creditors or class of creditors, and/or of the stockholders or class of stockholders of this corporation, as the case may be, agree to any compromise or arrangement and to any reorganization of this corporation as a consequence of such compromise or arrangement, the said compromise or arrangement and the said reorganization shall, if sanctioned by the court to which the said application has been made, be binding on all the creditors or class of creditors, and/or on all the stockholders or class of stockholders, of this corporation, as the case may be, and also on this corporation.

SIXTH: To the fullest extent permitted by law, the corporation shall have the power to indemnify any person who was or is a party or is threatened to be made a party to any threatened, pending or completed action, suit or proceeding, whether civil, criminal, administrative or investigative by reason of the fact that he is or was a director, officer, employee or agent of the corporation, or is or was serving at the request of the corporation as a director, officer, employee or agent of another



fz

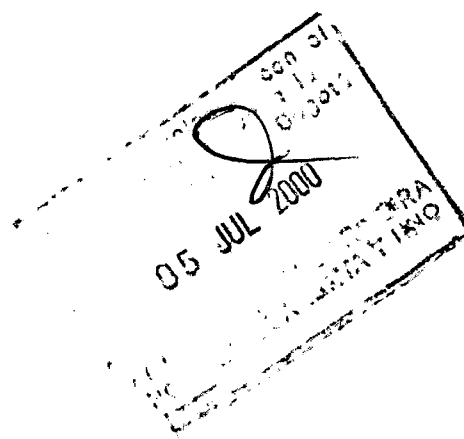
7368

corporation, partnership, joint venture, trust or other enterprise, against expenses (including attorneys' fees), liability, loss, judgment, fines and amounts paid in settlement actually and reasonably incurred by him in connection with such action, suit or proceeding if he acted in good faith and in a manner reasonably believed to be in or not opposed to the best interests of the corporation, and, with respect to any criminal action or proceedings, had no reasonable cause to believe his conduct was unlawful. The termination of any action, upon a plea of nolo contendere or equivalent, shall not, of itself, create a presumption that the person did not act in good faith and in a manner which he reasonably believed to be in or not opposed to the best interests of the corporation, and, with respect of any criminal action or proceeding, had reasonable cause to believe that his conduct was unlawful.

Such indemnity shall inure to the benefit of the heirs, executors and administrators of any such person so indemnified pursuant to this Article. The right to indemnification under this Article shall be a contract right and shall include, with respect to directors and officers, the right to be paid by the corporation the expenses incurred in defending any such proceeding in advance of its disposition; provided however, that, if the Delaware General Corporation Law requires, the payment of such expenses incurred by a director or officer in advance of the final disposition of a proceeding shall be made only upon delivery to the corporation of an undertaking, by or on behalf of such director or officer, to repay all amounts so advanced if it shall ultimately be determined that such director or officer is not entitled to be indemnified under this Article or otherwise. The corporation may, by action of its board of directors, pay such expenses incurred by employees and agents of the corporation upon such terms as the board of directors deems appropriate. Indemnification of, and advancement of expenses to, such person shall be mandatory to the extent that applicable law provides that the corporation may authorize such indemnification and advancement of expenses. Such indemnification and advancement of expenses shall be in addition to any other rights to which those seeking indemnification and advancement of expenses may be entitled under any law, Bylaw, agreement, vote of stockholders, or otherwise.

The corporation may, to the fullest extent permitted by applicable law, at any time without further stockholder approval, purchase and maintain insurance on behalf of any person who is or was a director, officer, employee or agent of the corporation or is or was serving at the request of the corporation as a director, officer, employee or agent of another corporation, partnership, joint venture, trust or other enterprise against any liability asserted against such person and incurred by such person in any such capacity, or arising out of such person's status as such, whether or not the corporation would have the power to indemnify such person against such liability under applicable law.

Any repeal or amendment of this Article by the stockholders of the corporation or by changes in applicable law shall, to the extent permitted by applicable law, be prospective only, and shall not adversely affect any right to indemnification or



74

advancement of expenses of a director or officer of the corporation existing at the time of such repeal or amendment. In addition to the foregoing, the right to indemnification and advancement of expenses shall be to the fullest extent permitted by the General Corporation Law of the State of Delaware or any other applicable law and all amendments to such laws as hereafter enacted from time to time.

SEVENTH: No director of the corporation shall have any personal liability to the corporation or to any of its stockholders for monetary damages for breach of fiduciary duty as a director; provided, however, that this provision eliminating such personal liability of a director shall not eliminate or limit the liability of a director (i) for any breach of the director's duty of loyalty to the corporation or its stockholders, (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, (iii) under §174 of the General Corporation Law of Delaware, or (iv) for any transaction from which the director derived an improper personal benefit. If the Delaware General Corporation Law is amended to authorize corporate action further eliminating or limiting the personal liability of directors, then the liability of a director of the corporation shall be eliminated or limited to the fullest extent permitted by the Delaware General Corporation Law as so amended.

EIGHTH: The name and address of the incorporator are Deborah A. Trala, 1310 King Street, P.O. Box 1328, Wilmington, Delaware 19899.

NINTH: The Board of Directors shall have the power to make, add to, delete from, alter, and repeal the By-Laws.

TENTH: The corporation reserves the right to amend, alter, change, or repeal any provision contained in this certificate of incorporation in the manner now or hereafter prescribed by law and all rights conferred on officers, directors, and stockholders herein are granted subject to this reservation.

ELEVENTH: The election of directors need not be by written ballot.

TWELFTH: No holder of shares of the corporation of any class or series shall have any preemptive right to subscribe for, purchase, or receive any shares of the corporation of any class or series now or hereafter authorized, or any options or warrants for such shares, or any securities convertible into or exchangeable for such shares, which may at any time be issued, sold, or offered for sale by the corporation. Cumulative voting by the stockholders of the corporation at any election of directors of the corporation is hereby prohibited.

THIRTEENTH: The corporation elects not to be governed by 8 Del. C. §203 (the Delaware Takeover Statute).

THE UNDERSIGNED INCORPORATOR, for the purposes of forming a corporation, in pursuance of an act of the legislature of the State of Delaware entitled

2000/1/33
05 JUL 2000
The undersigned incorporator
has signed this certificate of incorporation
on this 5th day of July, 2000.

75 70 74

"An Act Providing a General Corporation Law" (approved March 10, 1899) and any acts amendatory thereof and supplemental thereto, does make and file this Certificate of Incorporation, hereby declaring and certifying that the facts herein stated are true and accordingly has hereunto set her hand and seal this 10th of November, 1999.

Sharon A. Prickett
INCORPORATOR

2001/133

05 JUN 1999

76 71 AS

TRADUCCIÓN OFICIAL No.2000/133 de un documento escrito en inglés, el cual para su identificación se sella con el sello del traductor al tiempo con la presente. Esta traducción ha sido preparada por Hilda Aguilera de Piedrahita traductora e intérprete oficial debidamente reconocida por el Ministerio de Relaciones Exteriores y autorizada por el Ministerio de Justicia y del Derecho, por resolución número 323 de 1980.

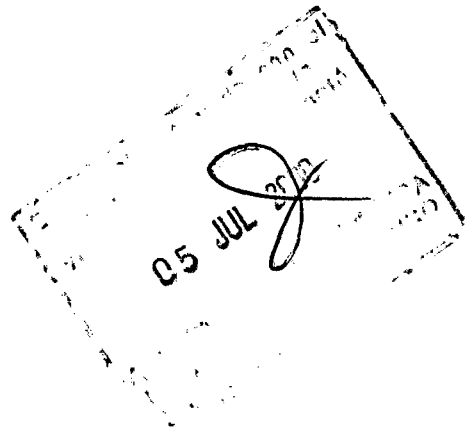
(Se traduce el Certificado de Constitución de la compañía Sharinga Networks Inc., escrito en inglés.)

ESTADO DE DELAWARE
SECRETARIO DE ESTADO
DIVISIÓN DE SOCIEDADES
PRESENTADO 9:00 AM 11/10/1999
9914477990 - 3122225

**CERTIFICADO DE CONSTITUCION
DE
SHARINGA NETWORKS INC.**

PRIMERO: El nombre de la sociedad es Sharinga Networks Inc.

SEGUNDO: La oficina registrada de la sociedad en el Estado de Delaware está situada en 1310 King Street , Wilmington, Condado de New Castle, Delaware



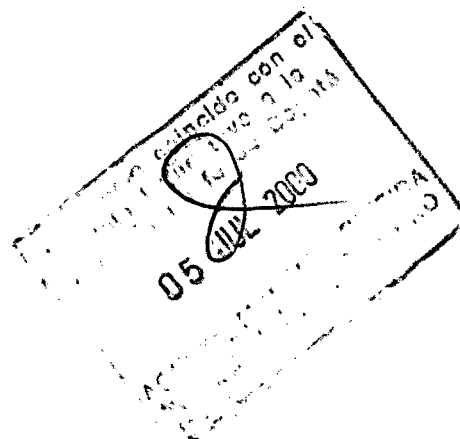
77 72 78

19801, y su agente registrado es PJEKS Corporate Services, Inc.

TERCERO: El objeto de la sociedad y la naturaleza y propósitos de los negocios que realizará, promoverá y llevará a cabo son ocuparse de cualquier acto legal o actividad para la cual pueden constituirse las sociedades bajo la Ley General de Sociedades de Delaware.

CUARTO: El número total de acciones de capital que la sociedad está autorizada a expedir es tres mil (3,000) acciones ordinarias, sin valor nominal.

QUINTO: Cuando se proponga entrar en una transacción o arreglo entre esta sociedad y sus acreedores, de cualquier clase de ellos y/o entre esta sociedad y sus accionistas, o cualquier clase de ellos, cualquier corte con jurisdicción competente dentro del Estado de Delaware puede, a solicitud presentada en forma sumaria por esta sociedad o por cualquier acreedor o accionista de ella o a solicitud de cualquier administrador o administradores judiciales nombrados para esta sociedad bajo las normas de la Sección 291 del Título 8 del Código de Delaware o a solicitud de fiduciarios en una disolución o de cualquier administrador o administradores judiciales nombrados para esta sociedad bajo la norma de la Sección 279 del Título 8 del Código de Delaware, ordenar una reunión de acreedores o clase de ellos, y/o de los accionistas o clase de ellos de esta sociedad, según sea el caso, convocarlos en la forma en que tal Corte ordene. Si una mayoría numérica que represente las tres cuartas partes en valor

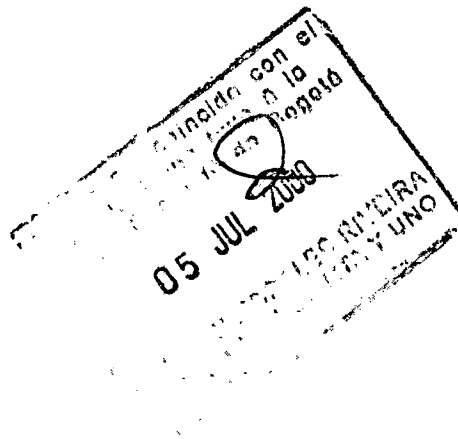


2000/133
JUL 10 2003
JUL 10 2003
JUL 10 2003

737
78

de los acreedores o clase de ellos, y/o de los accionistas o clase de ellos, de esta sociedad, según sea el caso, se compromete a transar o a arreglar cualquier reorganización de esta sociedad como consecuencia de tal transacción o arreglo, dicha transacción o arreglo y tal reorganización deberá, si fuese sancionada por la Corte ante la cual se haya hecho la solicitud, será obligatoria para todos los acreedores o clase de acreedores y/o para todos los accionistas o clase de accionistas de esta sociedad, según sea el caso y también para esta sociedad.

SEXTO: Hasta el máximo permitido por la ley, la sociedad estará facultada para indemnizar a cualquier persona que haya sido o sea parte o exista la posibilidad de que sea parte de cualquier acción potencial llevada a cabo o pendiente de llevarse a cabo, de cualquier pleito o proceso, ya sea civil, penal, administrativo o investigativo en razón del hecho de ser o haber sido, director, funcionario, empleado o agente de la sociedad, o sea, o haya estado al servicio, por solicitud de la sociedad, en calidad de director, funcionario o empleado, o agente de otra sociedad, compañía, empresa de riesgo compartido, fiducia u otra empresa, por cuenta de gastos (incluyendo honorarios de abogados), pasivos, pérdidas fallos, multas y sumas pagadas como transacción en que haya incurrido realmente y razonablemente en relación con dicha acción, pleito o proceso si hubiere obrado de buena fe y si en forma razonable hubiese creído que haya sido en beneficio del mejor interés de la sociedad, o no

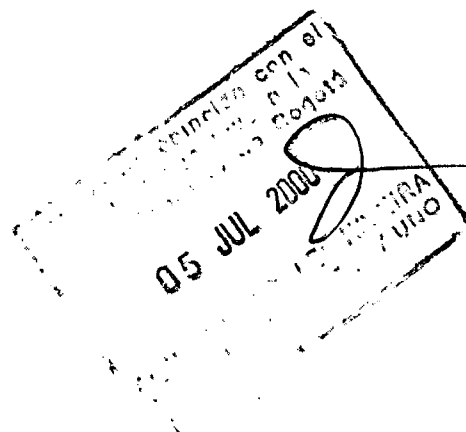


0022/133

29 74-18

opuesto a él, y, con respecto a cualquier acción penal o proceso no haya tenido causa razonable para creer que su conducta haya sido ilegal. La terminación de cualquier acción, por petición de no responder con venia de la Corte o un equivalente, no deberá en sí misma, crear la presunción de que la persona no actuó en buena fe y en forma en la cual haya creído razonablemente estar a favor o no opuesta a los mejores intereses de la compañía, y con respecto a cualquier acción penal o proceso, o haya tenido razón suficiente para creer que su conducta haya sido ilegal.

Tal indemnización tendrá efecto en beneficio de los herederos, albaceas y administradores de cualquiera de tales personas de dicha forma indemnizadas de conformidad con este Artículo. El derecho a indemnización bajo este Artículo representará un derecho contractual y deberá incluir, con respecto a los directores y funcionarios, el derecho de que la sociedad les pague los gastos en los cuales hayan incurrido en la defensa de tales procesos previamente a su disposición; siempre, sin embargo, que si la Ley General de Sociedades de Delaware lo requiera, el pago de dichos gastos incurridos por un director o funcionario previamente a la disposición definitiva de un proceso se hayan hecho a la entrega a la sociedad de un compromiso, suscrito por o en nombre de tal director o funcionario, en el sentido de pagar todas las sumas de tal forma anticipadas, si finalmente se determina que dicho director o funcionario no tiene derecho a indemnización bajo este Artículo, o de otra forma. La sociedad podrá



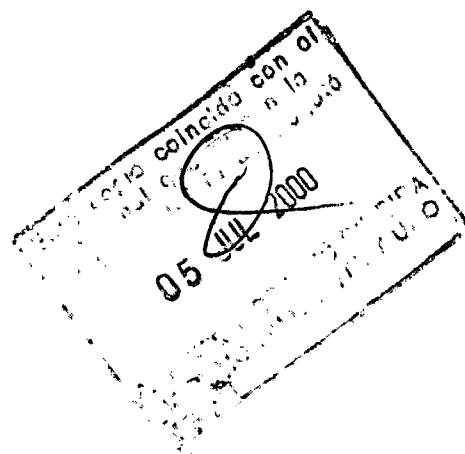
2000/35

75 19

por acción de su Junta Directiva pagar dichos gastos incurridos por empleados y agentes de la sociedad en los términos en que la junta directiva juzgue adecuado. La indemnización y avance para gastos, a dicha persona, será obligatoria en la medida en que la ley aplicable disponga que la sociedad puede autorizar la indemnización y anticipo para gastos. Tal indemnización y anticipo para gastos se hará en forma adicional a cualesquiera otros derechos que les correspondan bajo cualquier ley, Estatuto, convenio, voto de accionistas, u otros, quienes buscan indemnización y anticipo para gastos.

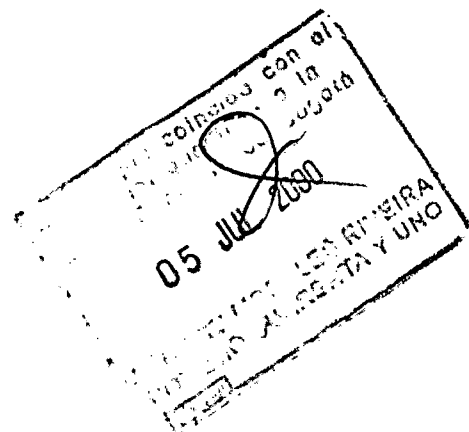
La sociedad podrá en la medida máxima permitida por la ley vigente, en cualquier tiempo sin aprobación adicional de accionistas, comprar y mantener seguros a nombre de cualquier persona que sea o haya sido director, funcionario, empleado o agente de la sociedad o sea o haya servido a solicitud de la sociedad como director, funcionario, empleado o agente de otra sociedad, compañía, empresa de riesgo compartido, fiducia u otra empresa contra cualquier pasivo que se haga valer contra tal persona y en el cual dicha persona haya incurrido en tal calidad o que surja de la condición como tal de dicha persona sea o no que la sociedad haya tenido facultad de indemnizar a esa persona contra dicho pasivo bajo la ley aplicable.

Cualquier revocación o enmienda de este artículo por los accionistas de la sociedad o por cualesquiera cambios en la ley vigente, en la medida que la ley lo permita , o que se encuentre en proyecto, no deberá afectar de manera



adversa el derecho a indemnización o anticipo de gastos de un director o funcionario de la sociedad existente en el momento de tal revocación o enmienda. Además de lo anterior, el derecho a indemnización y anticipo de gastos representará la máxima medida permitida por la Ley General de Sociedades del Estado de Delaware o por cualquier otra ley aplicable y por todas las enmiendas a tales leyes que puedan en adelante aprobarse de tiempo en tiempo.

SEPTIMO: Ningún director de la sociedad tendrá responsabilidad personal hacia la sociedad o hacia sus accionistas por perjuicios pecuniarios debidos a incumplimiento de deberes fiduciarios en calidad de director; siempre, sin embargo, que esta disposición que elimina la responsabilidad personal de director no elimine o limite la responsabilidad de cualquier director (i) por incumplimiento de los deberes de director en cuanto a lealtad a la sociedad o a sus accionistas, (ii) por actos u omisiones que no sean de buena fe o que involucren mala conducta intencional o una violación a sabiendas de la ley, (iii) bajo §174 de la Ley General de Sociedades de Delaware, o (iv) por cualquier transacción por la cual el director haya derivado beneficio personal incorrecto. Si la Ley general de Sociedades se reforma en forma que autorice a una acción de la sociedad de eliminar o limitar la responsabilidad personal de los directores, entonces las responsabilidades de los directores de la sociedad quedarán eliminadas o limitadas en la máxima medida permitida por la Ley General de



TRANSCRIPCION ORIGINAL No. 200/133
A ...
1972
Soy no 323 de la ...

24
8277

Sociedades de Delaware según se haya reformado.

OCTAVO: El nombre y dirección del constituyente de la sociedad es Deborah A. Trala 1310 King Street, P.O. Box 1328, Wilmington, Delaware 19899.

NOVENO: La Junta Directiva estará facultada para establecer, agregar, eliminar, modificar, y revocar los Estatutos.

DECIMO: La sociedad se reserva el derecho a modificar, alterar, cambiar, o revocar cualquier estipulación contenida en este Certificado de Constitución en la forma ahora o en adelante prescrita por la ley y todos los derechos conferidos a los funcionarios, directores, y accionistas de la presente, se otorgarán sujetos a esta reserva.

DECIMO PRIMERO: La elección de los directores no necesita ser por balota escrita.

DECIMO SEGUNDO: Ningún tenedor de acciones de la sociedad de clase o serie alguna tendrá ningún derecho de suscribir, comprar o recibir acciones de la sociedad de ninguna clase o serie que se autoricen ahora o en el futuro u opciones o derechos de suscripción por tales acciones, o títulos convertibles o cambiables por tales acciones que puedan en cualquier tiempo expedirse, venderse u ofrecerse en venta por la sociedad. La votación acumulativa por los accionistas de la sociedad en cualquier elección de directores de la corporación



2001/133

22
83 78
por el presente queda prohibida.

DECIMO TERCERO: La sociedad decide no regirse por 8 Del.C. §203 (Ley de Sustitución de Delaware)

EL SUSCRITO CONSTITUYENTE, para fines del establecimiento de una sociedad, en desarrollo de un acto de la legislatura del Estado de Delaware denominado "Un Acto que concede una Ley General de Sociedades" ("An Act Providing a General Corporation Law") (aprobada el 10 de Marzo de 1899) y cualesquiera actos enmendatorios y complementarios de la misma, firma y presenta este Certificado de Constitución, declarando por el presente y certificando que los hechos aquí manifestados son fieles y en consecuencia suscribe el presente y estampa su sello, hoy día 10 de Noviembre de 1999.

Firmado

DEBORAH A. TRALA

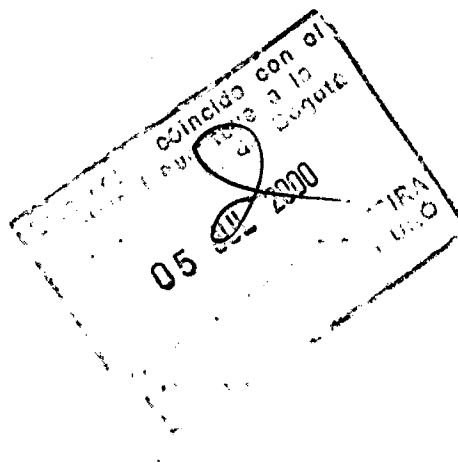
CONSTITUYENTE

(Sello en relieve)

ESTADO DE DELAWARE

OFICINA DEL SECRETARIO DE ESTADO PAG 1

YO, EDWARD J. FREEL, SECRETARIO DE ESTADO DEL ESTADO DE DELAWARE, POR EL PRESENTE CERTIFICO QUE, LA ADJUNTA ES COPIA



23
8479

FIEL Y CORRECTA DEL CERTIFICADO DE CONSTITUCIÓN DE LA
SOCIEDAD "SHARINGA NETWORKS INC." PRESENTADA EN ESTA
OFICINA EL DÍA 10 DE NOVIEMBRE DE 1999 A.D. A LAS 9 A.M.

UNA COPIA PRESENTADA DE ESTE CERTIFICADO SE HA REMITIDO
AL REGISTRADOR DE ESCRITURAS DEL CONDADO DE NEW CASTLE.

(FIRMADO)

Edward J. Freel, Secretario de Estado

(Sello de Oblea de la Secretaría de Estado)

(Sello Pre-impreso de la Oficina del Secretario de Estado de Delaware)

(Sello a Tinta: CHARLES BERNARD GORE BRETT, NOTARIO PÚBLICO,
NIVEL 3, 12 COLLINS STREET, MELBOURNE VIC, AUSTRALIA)

(Escrito a mano: Certifico que este documento es una copia fiel del documento
original, [firmado] Charles Bernard Gore Brett)

3122225 8100

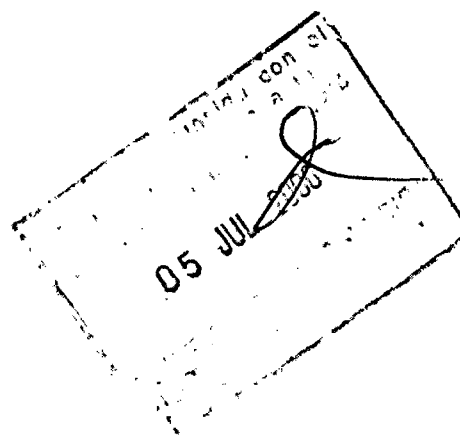
AUTENTICACIÓN: 0075681

991477990

FECHA:

11-10-99

(Sello a tinta: Yo, Ranu Vatana, funcionario del Departamento de Relaciones
Exteriores y Comercio, Australia, POR EL PRESENTE CERTIFICO que esta
firma, de CHARLES BRETT, que aparece al respaldo de los documentos



85 80 21

adjuntos es la firma auténtica de CHARLES BERNARD GORE BRETT, Notario Público residente en la ciudad de Melbourne en el Estado de Victoria, Australia, que el sello impreso es el Sello Oficial del mencionado CHARLES BERNARD GORE BRETT. En la certificación, ni yo ni el departamento asumimos responsabilidad alguna en relación con el contenido del documento. Dado bajo mi firma y Sello del Departamento de Relaciones Exteriores y Comercio hoy 29 de Mayo del Dos Mil (2000)).

(Sello a Tinta del Departamento de Relaciones Exteriores y Comercio en Melbourne)

EN ESPAÑOL, autenticación 132/00 de la firma que antecede por el Consulado de Colombia en Sidney de Junio 1, 2000. Pagados el Impuesto de Timbre y los Derechos Consulares, por valor de veintidós dólares (US\$22).

Autenticación por el Ministerio de Relaciones Exteriores Número 283115, de Junio 19 del 2000, suscrita por el Jefe de Legalizaciones.

ES TRADUCCIÓN FIEL Y COMPLETA de la cual se deja copia en los archivos de esta oficina para su confrontación y a la cual me remito.

Santafé de Bogotá, Junio 26 del 2000.

[Firma manuscrita]
TRADUCCION OFICIAL No. 2000/1133
MINISTERIO DE RELACIONES EXTERIORES

10

MINISTERIO DE RELACIONES EXTERIORES

007459

COPIA FIEL Y COMPLETA EN EL DOCUMENTO QUE EXPONE LAS FIRMAS INDICADAS

NO SE ASUME RESPONSABILIDAD DEL TERCERO

2000 JUN 29 A 10:17

OFICINA DE LEGALIZACIONES

05 JUL 2000
CITA
FOLIO

p. 330
86 81 25

TRADUCCION OFICIAL No. 344/2000.-

EL TEXTO QUE SIGUE ES TRADUCCION FIEL Y COMPLETA DE UN DOCUMENTO ESCRITO EN INGLES, Y LLEVA EL SELLO Y LA FIRMA DE HELENA URIBE DE LEMOINE, TRADUCTORA E INTERPRETE OFICIAL, SEGÚN RESOLUCION No. 3618 EXPEDIDA POR EL MINISTERIO DE JUSTICIA EL 6 DE SEPT. DE 1972.

AUSTRALIA

Oficina de Patentes
Camberra

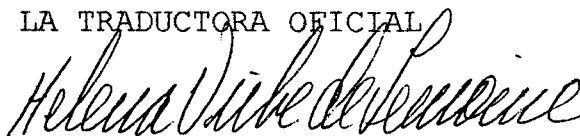
Yo, KAY WARD, LIDER DEL GRUPO DE RESPALDO DE EXAMEN Y VENTAS por el presente certifico que el documento adjunto es una copia verdadera de la especificación Provisional en relación con la Solicitud de patente No. PQ 3682 hecha por FREEONLINE COM.AU PTY. LIMITED radicada el 27 de octubre de 1999.

Certifico además que la anterior solicitud procede ahora a nombre de SHARINGA NETWORKS INC. de conformidad con las disposiciones de la Sección 113 de la Ley de Patentes de 1990. EN EVIDENCIA DE LO CUAL, he puesto mi firma hoy día veinticinco de Mayo de 2000.

FIRMADO POR: KAY WARD, LIDER DEL GRUPO DE RESPALDO DE EXAMENES Y VENTAS.

HAY SELLO EN RELIEVE DE LA OFICINA DE PATENTES DE AUSTRALIA.

LA TRADUCTORA OFICIAL



HELENA URIBE DE LEMOINE



26
8782

Patent Office
Canberra

I, KAY WARD, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PQ 3682 for a patent by FREEONLINE.COM.AU PTY. LIMITED filed on 27 October 1999.

I further certify that the above application is now proceeding in the name of SHARINGA NETWORKS INC pursuant to the provisions of Section 113 of the Patents Act 1990.

WITNESS my hand this
Twenty-fifth day of May 2000

K Ward

KAY WARD
TEAM LEADER EXAMINATION
SUPPORT AND SALES





Sharinga Networks Inc.
~~FREEONLINE.COM.AU PTY. LIMITED~~

A U S T R A L I A
Patents Act 1990

PROVISIONAL SPECIFICATION

for the invention entitled:

"A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM"

The invention is described in the following statement:

87 28
84

- 2 -

A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

5

The present invention relates to a method and system for accessing a communications network, such as the Internet.

Most Internet users currently connect to the Internet via the equipment of an Internet
10 service provider (ISP). The ISP provides remote access servers (RASs) which are able to communicate with remote computers of the users using modems and standard telephone lines. The remote computers and the RASs use standard software that executes a protocol, such as the point to point protocol (PPP), to allow the users to dial into the RASs and connect to the Internet. To achieve this, the connection or PPP software on the user's computer requires the
15 user to enter unique authentication data, such as the user's login name and password, and this is transmitted to the ISP when the software dials and connects to the ISP equipment. If the ISP equipment determines that the authentication data is valid, the user's computer is connected and the user is allowed uninhibited access to the Internet. The user is accordingly free to view any desired web pages using a web browser on the user's computer.

20

The success of web sites on the Internet, particularly from a commercial perspective, is almost solely dependent on a site's ability to attract traffic to it. For this reason, a number of well known sites, such as Netscape's home page and the home pages of ISPs have been reconfigured to operate as communication "portals" to the Internet in the hope that users will
25 continually revert to the sites to determine where to direct their browsers next. A number of sites have proved to be extremely lucrative, in the same manner as television stations which are able to attract large numbers of viewers. The current market value of companies such as Yahoo and Excite, which maintain high traffic volume sites, indicates how lucrative. As ISPs constitute a first point of connection for most Internet users, any steps or method which an
30 ISP can implement to direct users to particular pages, rather than the user's own default home page, would be highly desirable. The present invention seeks to provide such method or at least provide a useful alternative.

24
9085

- 3 -

In accordance with the present invention there is provided an access system including:
means for connecting a computer device and establishing a connection session for
accessing a network;

switch means having a plurality of access states, one of said access states being
5 assigned to said session for at least part of said session, each access state determining network
traffic receivable by said computer device; and

means for managing said session and assigning at least one of said access states during
said session based on connection data for said session and access requests from said computer
device.

10

Advantageously, the access requests may be requests for data on the Internet, such as
web pages, streaming audio and video, interactive chat sessions, e-mail or FTP sites, and said
access states determine whether the computer device can receive the data. The session
managing means may dynamically assign and adjust the access states during the session. The
15 access system may control the data delivered to the computer device, and an access state may
direct the computer device to a predetermined network location.

The present invention also provides an access system for a communications network,
such as the Internet, including:

20 means for connecting a computer device and establishing a TCP/IP session for access
to the network;

switch means having a plurality of access states, the access states determining the sites
and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the
25 session.

The access states are allocated based on connection data for the session, such as the
IP address for the session and/or profile data held for a user of the computer device. The
session may be allocated a number of access states at respective times during the session based
30 on access requests from the computer device.

Advantageously, the access system may partition the Internet based on respective

30
9-1 86

- 4 -

access states, which may be allocated to different sessions dynamically. Preferably one of the access states is an affiliate state which restricts access to locations on the network affiliated to a provider of the access system. The access system advantageously may partition or subdivide data provided by third parties on a public network, such as the Internet.

5

The present invention also provides a communications network access method, including:

establishing a TCP/IP session with a computer device; and

assigning access states during said session, said access states determining TCP/IP data
10 received by said computer device.

The present invention also provides a communications network access method, including:

connecting a computer device to a communications network;

15 accessing data from affiliate locations on said network without an access charge; and
accessing data from other locations on said network with an access charge.

The present invention also provides a communications network access method, including:

20 receiving a request from a computer device to connect to said network;

connecting said computer device to said network in response to said request;

sending login data to said computer device after said connecting step, said login data being adapted to generate a login display on said computer device allowing entry of unique authentication data by a user of said device;

25 receiving said unique authentication data entered on the computer; and

allowing said user to access said network using said computer device when said authentication data is validated.

Preferably said method includes accessing profile data for said user after said allowing
30 step and controlling access to said network using said profile data. Advantageously, said method may include having a set of access profiles or states encoded in a switch, and said profile data accessed for said user represents one of said encoded profiles or states.

31
22 87

- 5 -

Advantageously, the login display may include advertising material and links to particular locations on the communications network. Advantageously, the communications network may be the Internet and said login data represents a login web page sent to said computer device after connecting to the network. Advantageously, said request receiving and
5 connecting steps may be executed using standard communication protocols, such as PPP, and a modem of the computer device and a RAS of the network. Advantageously, the steps of the method may be executed by equipment of an ISP.

The present invention also provides a communications network access system,
10 including:

means for receiving a request from a computer device to connect to said network and for connecting the computer device to the network in response to the request;

means for sending login data to the computer device after it is connected to the network, said login data being adapted to generate a login display on the computer device
15 which allows entry of unique authentication data by a user of the device; and

means for receiving said unique authentication data entered by the user and for allowing the user to access the network using the computer device on determining that the authentication data is valid.

20 Advantageously, the receiving and connecting means may include a RAS. The sending means may include a web server, and the receiving and allowing means may include, the web server and a user database.

The present invention also provides a communications network access method,
25 including:

sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device, based on the login data, said
30 display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network; and obtaining access to the network after said authentication data is validated.

93 88

A preferred embodiment of the present invention is hereinafter described, by way of example only with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of a communications network access system;

5 Figure 2 is a block diagram of a server system of the access system;

Figure 3 is a flow diagram of a communications network access method of the access system;

Figure 4 is a diagram of a login page of the system and method; and

Figure 5 is a diagram of a customised home page of the system and method.

10

A communications access system, as shown in Figure 1, includes a plurality of remote access servers (RASs) 4, a layer four or higher switch 6, a database server 8, a web server system 10 and a router 12. The RASs 4 are provided to allow the computers 14 of remote users to dial into the system using standard telecommunication lines and modems and connect
15 to the input ports of the RASs 4, respectively. On connection to a port of a RAS 4, the RAS 4 and the user's computer 14 establish a unique TCP/IP session and the IP traffic for that session is switched by the switch 6. Once the user is authenticated or approved, as described below, the user's computer 14 is allowed to access requested data on the Internet 16. The web server system 10 is used to control pages presented to a user 14 connected to the RAS 4 and
20 handle authentication using a member profile database maintained on the database server 8, as described below. A RADIUS (Remote Authentication Dial In User Service) authentication server 11 is also provided for use in authentication. As far as the user 14 is concerned, the equipment 4, 6, 8, 10, 11 and 12 of the access system is part of the Internet. The equipment 4 to 12 includes standard commercially available hardware and basic database, web server and
25 Internet access software which is known to those skilled in the art and is used in the access systems of most ISPs. The equipment 4 to 12 also includes unique program code to manage and control each session, as discussed below. The layer four or higher switch 6 is another exception. The switch 6 is normally used by ISPs to balance the traffic handled by the RASs 4. An example of a suitable layer four switch is the 700 Series Switch™ produced by Alteon
30 WebSystems Inc. The access system differs from that offered by ISPs, as described below, in that the layer four switch 6 is used to connect users to the web server system 10 and control access to the Internet 16 for the users 14 on the basis of a limited number of access states

24 89

- 7 -

encoded in the switch 6.

The switch 6 controls access to the Internet 16 by assigning an access state to each TCP session, as identified by a respective IP address. The states are each defined by one or more access rules which are encoded in the switch 6. The rules define how the switch 6 is to direct IP traffic by executing pattern matching on the received traffic. For example, the states may include a login state, a portal state, a general state, an affiliate state, a registration state, and an allow state, as described below. A rule, for example, may be take access to a first URL and redirect to a second URL or the rules may allow or deny access to a predetermined set or list of URLs. The state assigned to a given IP address is controlled by a login system 20, as shown in Figure 2. The web server system 10 includes the login system 20 and a web server 22, running Apache™, which maintains web pages for the access system.

When the user 14 wishes to connect to the Internet using the access system, the user 14 dials into the system using standard PPP software and is allocated a port at the RAS 4 which answers the call. On connecting to a RAS 4, the user 14 is assigned an IP address for the IP session. The IP address is allocated from an IP address pool which depends on the number which the user dialled to connect to the RAS 4. For example, the user may have a dial-in number which provides the user with free access to Internet web sites as part of a promotion, and the user 14 is assigned an IP address and port which signifies to the switch 6 that all traffic at that IP address is to be switched directly to the router 12 and out to the Internet 16. This would occur with all IP addresses within this pool being allocated to the affiliate state of allow state of the switch 6, described below. Every other IP address assigned by the RASs 4 is initially allocated to a login state of the switch until the state is changed by the login system 20. Traffic with IP addresses assigned to the login state is all redirected to the login system 20 by switch 6.

The login system 20, as shown in Figure 2, includes a RADIUS accounting server 30, a login server 32, a session coordinator 34, individual session managers 36, an authentication client 38, a redirector server 42 and a plan manager 44. The components 30 to 44 are all software components, but can if desired be partly or entirely replaced by application specific integrated circuits (ASICs). The login system 20 is configured to handle three different

95 90

- 8 -

authentication scenarios:

- (i) Legacy authentication using the RADIUS authentication server 11.
- (ii) Authentication using a login display, e.g. browser based authentication.
- (iii) No authentication required.

5

For the first scenario, the user 14 dials into the RASs 4 using standard PPP software and provides a username and password. Based on the dial in number used and the configuration of the PPP software, the RAS port assigned to handle the call will direct the data provided to the RADIUS authentication server 11 to authenticate the user based on the PPP username and the password. Once authenticated, the RADIUS authentication server 11 returns a connect status message to the RAS 4 and an IP address is assigned to the user. Based on the IP address, the switch 6 forwards from the RAS 4 the connect status message, the username, calling line identification and the IP address to the login system 20. This data is processed by the RADIUS accounting server 30 which acknowledges the new connection for the IP address and accesses the database server 8 to record the connection time for the user. The RADIUS accounting server 30 acknowledges and monitors all connections and disconnections for IP addresses, and issues connection and disconnection messages to other components in the access system. The session coordinator 34 uses the connection data, together with profile data accessed from the member profile database for the user 14, to create an instance of a session manager 36 for the connection. Session managers 36 are created for each connection or session, respectively, and provide instructions to the redirector server 42 to control the state at the switch 6 for the session.

A session manager 36 controls the traffic which the user can receive during the session by controlling the state of the switch for the user's IP address. The state control is executed on the basis of the user's member profile held in the member profile database of the server 8. The profile specifies which one of a limited number of access profiles the user belongs to. The access profiles each contain data which defines the access states that the user is able to enter. The different access states are encoded in the switch 6. On authentication of a TCP/IP session the session manager 36 for the session instructs the redirection server 42 to store data in the switch 6 indicating which one of the access states apply to the session. For example, during authentication the session is in a login state and can change to a general state or

9/6 91

- 9 -

affiliate state once authentication has been completed.

In the second authentication scenario, the access system executes browser based authentication using the access procedure shown in Figure 3. The user is able to connect to the Internet by simply dialling into the access system using standard PPP software, at step 22, and the RASs 4 will automatically connect the user 14 without requiring the entry of any username or password. The user is automatically connected, an IP address assigned and a TCP session established, when the user dials into a port of a RAS 4 using predetermined call numbers. The system informs the user's computer 14 of the connection and the PPP software will display for the user the fact that the connection has been established and any other details associated with the connection, such as the data rate. The IP address is assigned from an address pool for immediate connection.

Once the user is connected to the access system the switch 6 determines whether the user's machine 14 is requesting connection to another computer on the Internet 16, at step 24. The request for example, may be simply to the user's default home page when the user opens a web browser of the computer 14. The switch 6 then determines, at step 26 by checking a stored flag representing the switch state for the IP address, whether the user has been authenticated and that the state is not the login state. If the switch 6 is in the login state, the switch 6 connects the user 14 to a login page on the web server 22, and the login system 20 executes a login process 28. The login process 28 is similar to that for legacy authentication, in that the RAS accounting server 30 acknowledges that connection has occurred and a new session has been established for the IP address. Data for the session is passed to the session coordinator 34 to create an instance of a session manager 36 for the session. Based on the IP address, however, the session manager 36 determines that the user needs to be authenticated using browser based authentication and accordingly waits for the login server 32 to receive from the web server 22 details submitted on the login page shown in Figure 4. The login page presents the user with a number of options, which includes executing a registration process to become a new registered user, entering a username and password if already registered, or accessing help pages stored on the server 22. The page also includes a number of banner advertisements which may include links to other pages or web sites. To gain general access to the Internet 16, however, the user must enter a valid username and password combination

36
9792

- 10 -

which is authenticated by the login system 20. The login page allows the user to enter a username and password combination and then send the combination for authentication by clicking on the "sign in" button. Alternatively the combination may already be stored on the computer 14 by the user. The username and password combination is received by the session
5 manager 36 for the session and the combination is forwarded to the authentication client 38. The authentication client 38 passes the combination to an authentication daemon 40 running on the database server 8. The authentication daemon checks the combination against stored combinations for users to determine if it is valid, identify the user and access the unique member profile for the user from the database server 8.

10

In the third authentication scenario, no authentication is required. In this scenario the user is allocated a telephone number to dial in on which corresponds to no authentication. The user is automatically connected, as for browser based authentication, and assigned an IP address from a pool for no authentication. Operation proceeds as described above for browser
15 based authentication, except that the session manager 36 does not revert to the authentication client 38 to authenticate the user based on a username and password combination. The user is simply authenticated automatically by the session manager 36.

Once the user has been authenticated, either by the login process 28 or using the
20 RADIUS server 11, an individual session manager 36 uses the member profile data for the user to compile and send a customised home page, as shown in Figure 5 to the user 14. The customised home page may also include banner advertisements, in the same manner as for the login page. The session manager 36 instructs the redirector server 42 to change the state of the switch 6 to a portal state, after authentication, which directs the switch to connect to the
25 URL for the customised home page or portal shown in Figure 5. Details concerning the user and customised home page data from the member profile are passed by the session manager 36 to the login server 32 for access by the Apache server 22 which controls compilation of the customised home page. Subsequently, the session manager 36 instructs the redirector server so as to divert the switch to one of the browsing states, either an affiliate state or a
30 general state. For browser based authentication, as shown in Figure 3, the login authentication process is managed using the web browser of the user's machine 14, rather than the PPP software, and operation returns after the login process 28 to step 24. Accordingly, once the

37
93

- 11 -

user reverts to step 24 and is determined at step 26 as having been authenticated, the switch 6 determines at step 30, on the basis of the access state for the session, whether the user is allowed to access a requested computer or service. If so, the user is granted access to the computer or service on the Internet 16 at step 32. If not, the user 14 is advised at step 34 of the access denial. The access denial can be communicated by connecting the user to a denial page of the Apache server 22.

A user 14 having a session which is in the affiliate state is allowed access, at no charge, to sites maintained by affiliates of the provider of the access system. The affiliate sites 10 may be maintained on the Apache server 22 or on other servers of the Internet 16. The affiliate sites are all identified by URLs in the rules of the affiliate state. The affiliate sites can also be accessed using the links provided in the web pages of Figures 4 and 5. The rules for the affiliate state specify that access is denied to any URLs which do not belong to the affiliate sites. If however a user has a member profile that allows access to other sites on the Internet, 15 the user is able to move to the general state. For these users, when a request is made to access a site other than an affiliate site, the user's browser is redirected by the switch 6 to an interim blank page on the Apache server 22 while the session manager 36 determines whether to instruct the redirector server 42 to change the state of the switch to the general state. The interim blank page contains code to trap the requested URL and pass the URL and a message 20 to the login server 32 advising that the user is attempting to move from the affiliate state to the general state. This message is passed to the session manager 36, on the basis of the IP address, and the session manager 36 accesses the member's profile. If the session manager 36 determines on the basis of the profile that the user 14 is allowed to move the general state, a message is sent to the redirector server 42 to change the state of the switch to the general 25 state for the session. A message is also sent from the manager 36 to the login server 32 advising that the user 14 is allowed to move to the trapped URL. The login server 32 sends a message to the Apache server 22 to forward the user 14 from the interim page to the page of the requested trapped URL. If access is denied, the URL of a denied page is used to substitute the trapped URL at the login server 32, and the user 14 is forwarded to the denial 30 page.

Other access states are the registration state and the allow state. A session manager 36

38
99 94

- 12 -

will instruct the redirector server 42 to enter the switch into the registration state for a session when a user sends a message indicating they wish to register with the access system. This may be done when, for example, the user selects the registration option on the login page of Figure 4. In the registration state the switch 6 redirects the user 14 to registration pages on the Apache server 22 and the login system 20 collects the requested details on the pages from the user 14 for the user file in the data base server 8. A session manager 36 will instruct the redirector server to cause the switch 6 to enter the allow state when the IP address indicates that the user 14 is to be provided with unrestricted access to the Internet 16 without any monitoring or charge.

10

When the session is disconnected, the RAS 4 communicates disconnection to the RADIUS accounting server 30, which in turn advises the session manager 36. The manager 36 instructs the redirector server 42 to change the state of the switch to the login state for the IP address of the disconnected session.

15

The manner in which the user is charged is controlled by a plan manager 44 that is accessed by the session manager 36. The plan manager 44 maintains different charging plans which can be applied to users. For example, all users would not be charged for access to affiliate sites, but the rate of charge may differ for accesses when in the general state. For instance, users may be allocated a predetermined period of free access for pages to the general state and then charged at a set rate thereafter. The plan manager specifies the times and rates for the different plans, and this is accessed by the session managers 36 which monitor the time a user spends in different access states. The ultimate charge for a session is compiled by the session managers 36 and then stored against the user's file in the database server 8.

25

The access method and system are particularly advantageous as they allow ISPs, at least initially, to dynamically control the pages viewed by a user. As a minimum, the user must, and cannot avoid, viewing the login or customised home page, as these are an integral part of the login process. This allows the ISP to present advertising information, and in particular present targeted advertising information based on the user's profile, which the ISP can guarantee that all of its users will not be able to avoid. The login and customised home pages therefore act as an entry portal for all users.

30

1009534

- 13 -

By also allowing all users to connect to the system, including users which are not registered, the ISP is able to present and provide free access to selected and predetermined Internet content and services. For example, the login page may include links to certain web pages that provide banking, stock trading or home shopping, and the user will not have to pay
5 any fees to the ISP to access these pages. This allows the ISP to act as a free content provider for certain content, whilst charging a user to access other data on the Internet. To provide information to advertisers associated with the free content, the ISP can, if desired, still require and obtain certain information on and from users before providing the free content, and monitor their access.

10

Encoding the access states in the switch 6 also allows the ISP to restrict or allow access to selected content or services on the Internet, such as sports betting, adult orientated content or children's content.

15 Many modifications will be apparent for those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

20

DATED this 27th day of October, 1999

FREEONLINE.COM.AU PTY. LIMITED

25 By its Patent Attorneys

DAVIES COLLISON CAVE

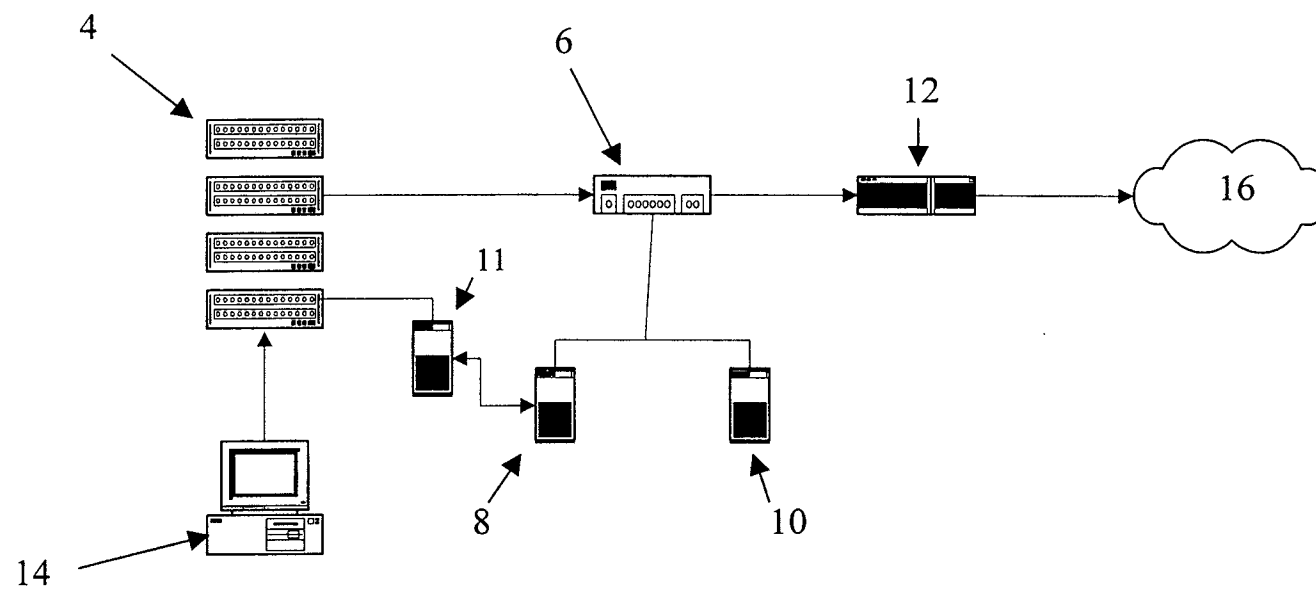


Figure 1

10/1

97
402
ST

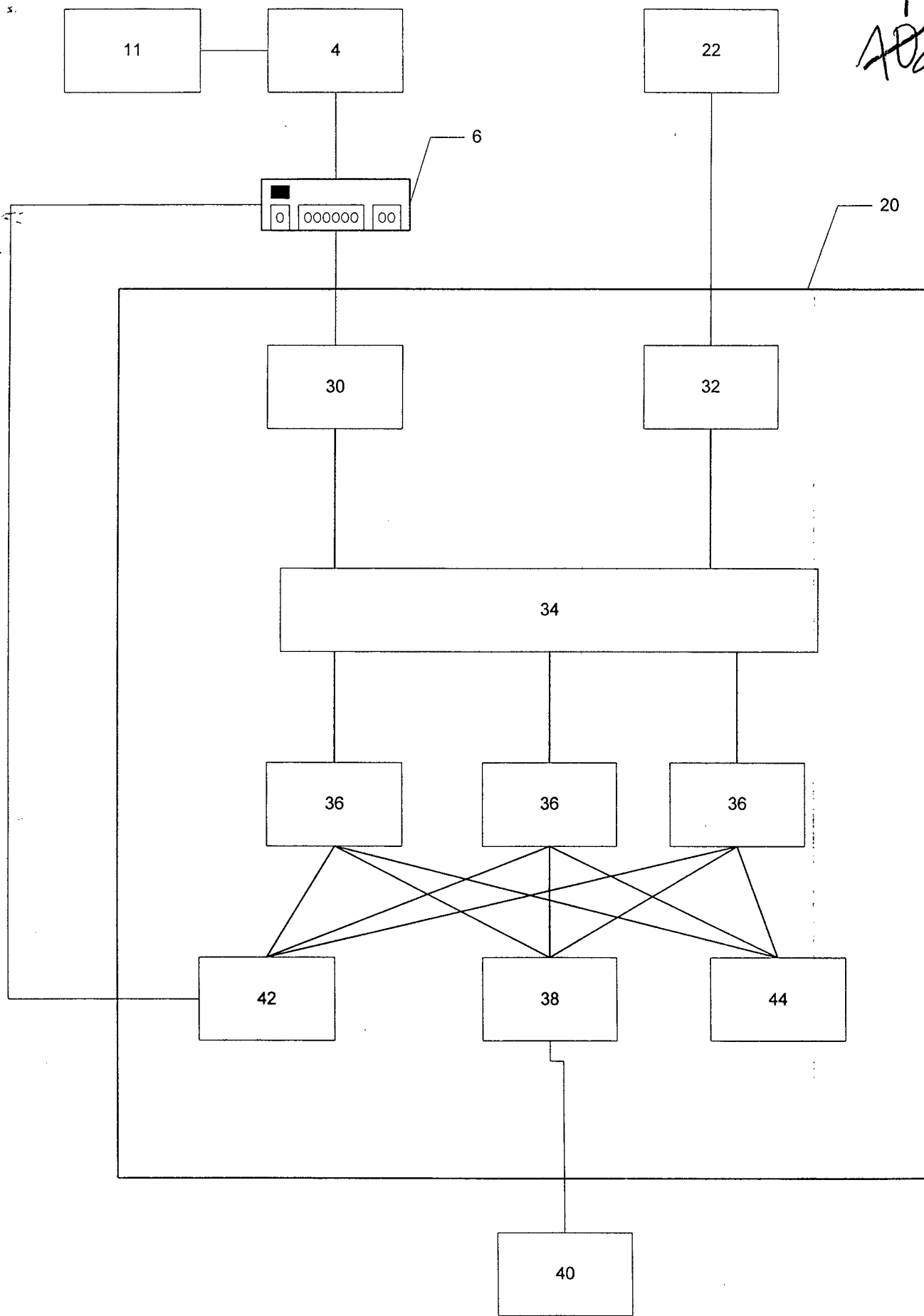


Figure 2

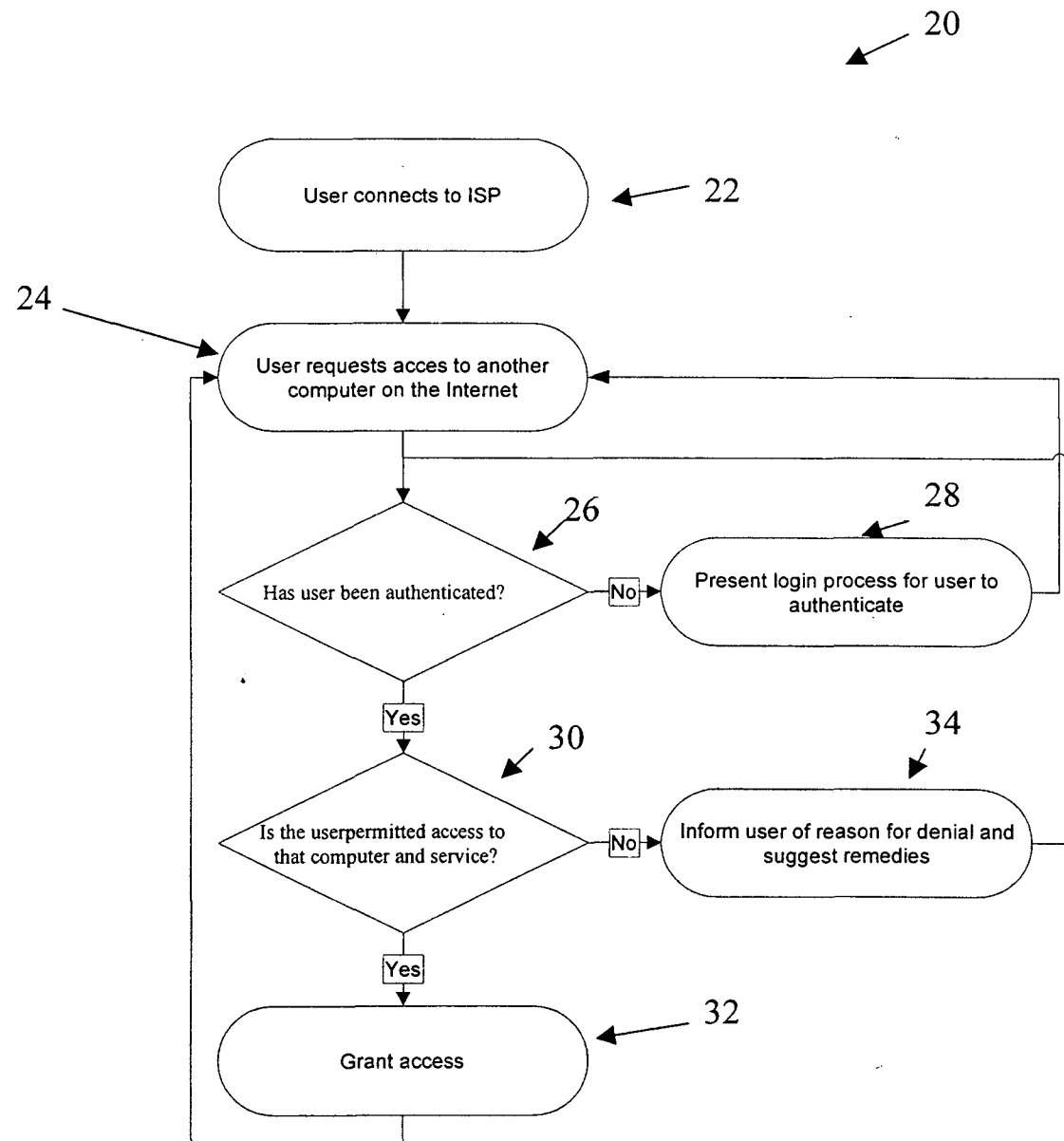


Figure 3

103
24



Figure 4

10/13



Figure 5

105

47

UN MÉTODO Y SISTEMA DE ACCESO A UNA RED DE COMUNICACIONES

La presente invención se relaciona con un método y sistema para
5 tener acceso a una red de comunicaciones, tal como Internet.

La mayoría de los usuarios de Internet se conectan a Internet
actualmente a través del equipo de un proveedor de servicio de
Internet (ISP). El ISP provee servidores de acceso remoto (RAS) que
10 tienen la capacidad de comunicarse con computadores remotos de los
usuarios utilizando modems y líneas telefónicas estándar. Los
computadores remotos y los RAS usan soporte lógico estándar el cual
ejecuta un protocolo, tal como el protocolo de punto a punto (PPP),
para permitir que los usuarios marquen hacia el RAS y se conecten a
15 Internet. Para lograr esto, el soporte lógico o PPP de conexión en el
computador del usuario requiere que éste ingrese datos propios de
autenticación, tales como el nombre y clave de acceso del usuario,
que son transmitidos al ISP cuando el soporte lógico marca y se
conecta al equipo del ISP. Si el equipo del ISP determina que los datos
20 de autenticación son válidos, el computador del usuario se conecta y
permite al usuario un acceso sin inhibiciones a Internet. De acuerdo
con esto, el usuario está en libertad de ver cualquier página de la Red
utilizando un programa explorador de la red en el computador del
usuario.

25

El éxito de los sitios de la Red en Internet, particularmente desde una
perspectiva comercial, depende casi exclusivamente de la habilidad

del sitio para atraer tráfico hacia sí. Por esta razón, un cierto número de sitios bien conocidos, tales como la página principal de Netscape y las páginas principales de los ISP, han sido reconfiguradas para operar como "portales" de comunicación hacia Internet en la
5 esperanza de que los usuarios retornarán continuamente a los sitios para determinar hacia donde dirigirán enseguida sus programas exploradores de la Red. Un cierto número de sitios han probado ser extremadamente lucrativos, de la misma forma que las estaciones de televisión las cuales son capaces de atraer grandes cantidades de
10 televidentes. El valor actual en el mercado de compañías tales como Yahoo y Excite, que mantienen sitios de alto volumen de tráfico, indican cuan lucrativos son. Puesto que el ISP constituye un primer punto de conexión para la mayoría de usuarios de Internet, cualquier paso o método que un ISP pueda implementar para dirigir a los
15 usuarios a páginas particulares, más que a la propia página inicial del usuario, serían altamente deseables. La presente invención busca proveer tal método o al menos proveer una alternativa útil.

De acuerdo con la presente invención, se provee un sistema de acceso
20 que incluye:

medios de conexión para conectar un dispositivo computador y establecer una sesión de conexión para lograr acceso a una red;

25 medios de conmutación con una pluralidad de estados de acceso, siendo asignado uno de dichos estados de acceso a dicha sesión por al menos parte de dicha sesión, determinando cada estado

de acceso el tráfico de red que puede ser recibido por dicho dispositivo
computador; y

medios para manejo de sesión para manejar dicha sesión y
5 asignar al menos uno de dichos estados de acceso durante dicha
sesión con base en los datos de conexión para dicha sesión y los
requerimientos de acceso para dicho dispositivo computador.

Ventajosamente, los requerimientos de acceso pueden ser
requerimientos de datos en el Internet, tales como páginas de la Red,
10 transferencia de audio y video, sesiones de charla interactiva, sitios de
correo electrónico o FTP, y dichos estados de acceso determinan si el
dispositivo de computador puede recibir los datos. Los medios de
manejo de sesión pueden asignar y ajustar dinámicamente los
estados de acceso durante la sesión. El sistema de acceso puede
15 controlar los datos entregados al dispositivo de computador, y un
estado de acceso puede dirigir el dispositivo de computador a una
localización predeterminada en la red.

La presente invención también provee un sistema de acceso para una
20 red pública de comunicaciones, tal como Internet, incluyendo:

medios para conectar un dispositivo de computador y establecer
una sesión TCP/IP para acceso a la red;

25 medios de conmutación que tienen una pluralidad de estados
de acceso, determinando los estados de acceso los sitios y páginas a

los que se puede tener acceso mediante el dispositivo computador durante la sesión; y

medios para manejar la sesión con el fin de localizar al menos
5 uno de los estados de acceso durante la sesión.

Los estados de acceso son localizados con base en los datos de conexión para la sesión, tales como la dirección IP para la sesión y/o datos de perfil mantenidos para un usuario del dispositivo de computador. La sesión puede ser ubicada en cierto número de
10 estados de acceso en tiempos respectivos durante la sesión basada en requerimientos de acceso desde el dispositivo de computador.

Ventajosamente, el sistema de acceso puede ejecutar una partición del Internet con base en estados de acceso respectivos, los cuales pueden ubicarse dinámicamente en diferentes sesiones.
15 Preferiblemente, uno de los estados de acceso es un estado afiliado que restringe el acceso a las ubicaciones en la red afiliada a un proveedor del sistema de acceso. El sistema de acceso puede ventajosamente efectuar una partición o subdividir los datos suministrados por terceras partes en una red pública, tal como el
20 Internet.

La presente invención también provee una método de acceso a una red de comunicaciones, incluyendo:

Establecer una sesión TCP/IP con un dispositivo de computador; y

25 Asignar estados de acceso durante dicha sesión, determinando dichos estados de acceso los datos TCP/IP recibidos por dicho dispositivo de computador.

La presente invención también provee un método de acceso a una red de comunicaciones, incluyendo:

Conectar un dispositivo de computador a una red de comunicaciones;

5 Dar acceso a datos desde las localizaciones de un afiliado en dicha red sin un cargo de acceso; y

Tener acceso a datos desde otras localizaciones en dicha red con un cargo de acceso.

10 La presente invención también provee un método de acceso a una red de comunicaciones, incluyendo:

Recibir un requerimiento desde un dispositivo de computador para conectar a dicha red;

15 Conectar dicho dispositivo de computador a dicha red, en respuesta a dicho requerimiento;

20 Enviar datos de ingreso a dicho dispositivo de computador después de dicha etapa de conexión, siendo adaptados dichos datos de ingreso para generar una pantalla de ingreso sobre dicho dispositivo de computador permitiendo la entrada de datos únicos de autenticación por un usuario de dicho dispositivo;

Recibir dichos datos únicos de autenticación ingresados al computador; y

25 Permitir a dicho usuario tener acceso a dicha red usando dicho dispositivo de computador cuando dichos datos de autenticación son validados.

Preferiblemente dicho método incluye tener acceso a datos de perfiles para dicho usuario después de dicha etapa de permisión y control del acceso a dicha red usando dichos datos de perfiles. Ventajosamente, dicho método puede incluir tener un conjunto de perfiles de acceso o
5 estados codificados en un conmutador, y dichos datos de perfiles a los cuales se ha tenido acceso por dicho usuario representan uno de dichos perfiles o estados codificados.

Ventajosamente, la pantalla de entrada puede incluir material publicitario y se enlaza a localizaciones particulares en la red de
10 comunicaciones. Ventajosamente, la red de comunicaciones puede ser el Internet y dichos datos de ingreso representan una página de ingreso a la Red para dicho dispositivo de computador después de conectarse a la red. Ventajosamente, dicho requerimiento que recibe y conecta etapas puede ser ejecutado usando protocolos de
15 comunicación estándar, tales como PPP, y un módem del dispositivo de computador y un RAS de la cadena. Ventajosamente, las etapas del método pueden ejecutarse mediante el equipamiento de un ISP.

La presente invención también provee un sistema de acceso a una red
20 de comunicaciones, incluyendo:

medios para recibir un requerimiento desde un dispositivo computador para conectar a dicha red y para conectar el dispositivo computador a la red en respuesta al requerimiento;

medios para enviar datos de nombre al dispositivo computador
25 después de éste se ha conectado a la red, siendo adaptados dichos datos de nombre para generar un despliegue de pantalla del nombre

107
A12
57

en el dispositivo computador lo cual permite la entrada de datos exclusivos de autenticación por parte de un usuario del dispositivo; y

medios para recibir dichos datos exclusivos de autenticación
5 ingresados por el usuario y para permitir al usuario tener acceso a la red usando el dispositivo computador al determinar que los datos de autenticación son válidos.

Ventajosamente, los medios de recepción y conexión pueden incluir un RAS. Los medios de envío pueden incluir un servidor de la Red, y
10 los medios de recepción y permisión pueden incluir el servidor de la Red y una base de datos de usuarios.

La presente invención también provee un método de acceso a una red comunicaciones, incluyendo:

15 enviar un requerimiento desde un dispositivo computador para conectarse a una red de comunicaciones; y ser conectado a la red en respuesta al requerimiento;

20 recibir datos de nombre de ingreso después de ser conectado;
generar un despliegue de pantalla del nombre de acceso en el dispositivo computador, con base en los datos de nombre de acceso, permitiendo dicho despliegue de pantalla la entrada de datos de autenticación exclusivos;

25 enviar los datos de autenticación exclusivos ingresados en el dispositivo computador a la red; y

obtener acceso a la red después de que dichos datos de autenticación sean validados.

Una modalidad preferida de la presente invención se describe a continuación, a manera de ejemplo solamente con referencia a los dibujos acompañantes, en los cuales:

La figura 1 es un diagrama de bloques de una modalidad preferida de un sistema de acceso a una red de comunicaciones;

La figura 2 es un diagrama de bloques de un método de acceso a una red de comunicaciones del sistema de acceso;

La figura 3 es un diagrama de flujo de un método de acceso a una red de comunicaciones del sistema de acceso;

La figura 4 es un diagrama de la página de ingreso del sistema y del método; y

La figura 5 es un diagrama de una página principal personalizada del sistema y el método.

Un sistema de acceso a comunicaciones, como se muestra en la figura 1, incluye una pluralidad de servidora de acceso remotos (RAS) 4, un conmutador de base cuatro o superior 6, un servidor de base de datos 8, un sistema servidor de la Red 10 y un enrutador 12. El RAS 4 se provee para permitir a los computadores 15 de los usuarios remotos

109
114
53

marcar hacia el sistema usando líneas de telecomunicación y modems estándar para conectarse a los puertos de entrada del RAS 4, respectivamente. Al conectarse a un puerto de un RAS 4, el RAS 4 y el computador 14 de usuario establecen una sesión exclusiva TCP/IP y el tráfico IP para esa sesión es conmutado por el conmutador 6. Una vez que el usuario es autenticado o aprobado, como se describe más abajo, el computador 14 del usuario es autorizado para tener acceso a los datos requeridos en Internet 16. El sistema servidor de la Red 10 se usa para controlar las páginas presentadas a un usuario 14 conectado al RAS y manejar la autenticación usando una base de datos de perfil de miembros mantenida en el servidor de base de datos 8, como se describe más abajo. Un servidor de autenticación RADIUS (Marcación Remota de Autenticación en Servicio de Usuario) 11 también se provee para uso en autenticación. En cuanto se relaciona con el usuario 14, los equipos 4, 6, 8, 10, 11 y 12 del sistema de acceso son parte de Internet. Los equipos 4 a 12 incluyen equipamiento estándar comercialmente disponible, un servidor de la Red y un soporte lógico de acceso a Internet que es conocido para los expertos en la técnica y se usan en los sistemas de acceso de la mayoría de los ISP. Los equipos 4 a 12 entonces incluyen también un código de programa único para manejar y controlar cada sesión, como se discute más abajo. El conmutador de base cuatro o superior 6 es otra excepción. El conmutador 6 se usa normalmente por los ISP para balancear el tráfico manejado por el RAS 4. Un ejemplo de un conmutador de base cuatro apropiado es el 700 Series Switch™ producido por Alteon WebSystems Inc. El sistema de acceso difiere del ofrecido por los ISP, como se describe más adelante, en que el

conmutador de base cuatro 6 se utiliza para conectar usuarios al sistema servidor de la Red 10 y para controlar el acceso a Internet 16 para los usuarios 14 sobre la base de un número limitado de estados de acceso codificados en el conmutador 6.

5 El conmutador 6 controla el acceso a Internet 16 asignando un estado de acceso a cada sesión TCP, según sea identificado por una dirección correspondiente IP. Cada estado es definido por una o más reglas de acceso que son codificadas en el conmutador 6. Las reglas definen cómo el conmutador 6 dirigirá tráfico IP ejecutando una comparación
 10 de patrones en el tráfico recibido. Por ejemplo, los estados pueden incluir un estado de ingreso, un estado de portal, un estado general, un estado de afiliado, un estado de registro y un estado de permiso, como se describe más adelante. Una regla, por ejemplo, puede ser recibir un primer URL y redireccionar a un segundo URL o las reglas
 15 pueden permitir o denegar el acceso a un conjunto o lista predeterminado de URL. El estado asignado a una dirección IP dada es controlado por un sistema de control 20, como se muestra en la Figura 2. El sistema servidor de la Red 10 incluye el sistema de control 20 y un servidor de la Red 22, corriendo Apache™, el cual
 20 mantiene las páginas de la Red para el sistema de acceso.

Cuando el usuario 14 quiere conectarse a Internet usando el sistema de acceso, el usuario 14 marca hacia el sistema usando el soporte lógico PPP estándar y se ubica en un puerto en el RAS 4 el cual
 25 responde la llamada. Al conectarse al RAS 4 se asigna al usuario 14 una dirección IP para la sesión IP. La dirección IP se selecciona de entre un grupo de direcciones IP la cual dependerá del número

marcado por el usuario al conectarse al RAS 4. Por ejemplo, el usuario puede tener un número de marcado que provea al usuario con acceso gratis a los sitios de la Red Internet como parte de una promoción, y al usuario 14 se le asigna una dirección IP y un puerto
5 lo que significa para el conmutador 6 que todo el tráfico de esa dirección IP debe ser conmutado directamente al enrutador 12 y hacia fuera a Internet 16. Esto ocurriría con todas las direcciones IP dentro de este grupo que seas dirigidas al estado de permiso del conmutador 6, descrito más adelante. Otras direcciones IP asignadas por el RAS 4
10 se dirigen inicialmente a un estado de ingreso del conmutador hasta que el estado es cambiado por el sistema de control 20. El tráfico con las direcciones IP asignadas al estado de ingreso es todo redireccionado hacia el sistema de control 20 por el conmutador 6.

15 El sistema de control 20, como se muestra en la Figura 2, incluye un servidor de cuenta RADIUS 30, un servidor de ingreso 32, un coordinador de sesión 34, manejadores individuales de sesión 36, un cliente de autenticación 38, un servidor redireccionador 42 y un manejador de plan 44. Los componentes 30 a 44 son todos
20 componentes de soporte lógico pero sise desea pueden ser parcial o totalmente reemplazados por circuitos integrados de aplicación específica (ASIC). El sistema de control 20 se configura para manejar tres diferentes escenarios de autenticación:

- (i) Autenticación de legalidad usando el servidor de autenticación RADIUS 11.
- 25

58

AA7 112

- (ii) Autenticación usando un despliegue de pantalla de ingreso, por ejemplo, una autenticación basada en un programa explorador de la Red.
- (iii) Sin requerimiento de autenticación.

5

Para el primer escenario, el usuario 14 marca hacia el RAS 4 usando un soporte lógico PPP estándar y proporciona un nombre de usuario y una clave de acceso. Con base en el número marcado y en la configuración del soporte lógico PPP, el puerto RAS asignado para
10 manejar la llamada dirigirá los datos proporcionados hacia el servidor de autenticación RADIUS 11 para autenticar al usuario con base en el nombre de usuario y clave de acceso PPP. Una vez autenticado, el servidor de autenticación RADIUS 11 retorna un mensaje de estado de conexión al RAS 4 y se asigna una dirección IP al usuario. Con
15 base en la dirección IP, el conmutador 6 envía desde el RAS 4 el mensaje de estado de conexión, el nombre de usuario, la identificación de la línea de llamada (CLI) y la dirección IP al sistema de control 20. Estos datos son procesados por el servidor de cuenta RADIUS 30 el cual reconoce la nueva conexión para la dirección IP y
20 cobra acceso al servidor de base de datos 8 para registrar el tiempo de conexión del usuario. El servidor de cuenta RADIUS 30 reconoce y monitorea todas las conexiones y desconexiones para las direcciones IP y emite mensajes de conexión y desconexión hacia otros componentes en el sistema de acceso. El coordinador de sesión 34
25 usa los datos de conexión, junto con los datos de perfil a los cuales se ha tenido acceso desde la base de datos de perfiles de miembro para el usuario 14, para crear una instancia de un manejador de sesión 36

para la conexión. Los datos de conexión transmitidos al coordinador de sesión 34 en el mensaje de conexión incluyen la dirección IP, el nombre de usuario y el CLI. Los manejadores de sesión 36 son creados para cada conexión o sesión, respectivamente, y proporcionan

5 instrucciones al servidor redireccionador 42 para controlar el estado en el conmutador 6 para la sesión.

Un manejador de sesión 36 controla el tráfico que el usuario puede recibir durante la sesión controlando el estado del conmutador para

10 la dirección IP del usuario. El control de estado es ejecutado con base en el perfil de miembro del usuario mantenido en la base de datos de perfil de miembros del servidor 8. El perfil especifica a cual, de un número limitado de perfiles de acceso, pertenece el usuario. Cada perfil de acceso contiene datos que definen los estados de acceso a los

15 cuales puede entrar el usuario. Los diferentes estados de acceso están codificados en el conmutador 6. AZ>l autenticar una sesión TCP/IP el manejador de sesión 36 para la sesión instruye al servidor redireccionador 42 para almacenar datos en el conmutador 6 indicando cual de los estados de acceso se aplica a la sesión. Por

20 ejemplo, durante la autenticación, la sesión está en un estado de ingreso y puede cambiar a un estado general o estado de afiliado una vez que la autenticación se ha completado.

En el segundo escenario de autenticación, el sistema de acceso

25 ejecuta una autenticación basada en un programa explorador de la Red usando el procedimiento de acceso mostrado en la Figura 3. El usuario está en capacidad de conectarse a Internet simplemente

marcando hacia el sistema de acceso usando el soporte lógico estándar PPP, en la etapa 62, y el RAS 4 conectará automáticamente al usuario 14 sin requerir la entrada de ningún nombre de usuario o clave de acceso. El usuario se conecta automáticamente, se asigna una dirección IP y se establece una sesión TCP, cuando el usuario marca hacia un puerto de un RAS 4 usando números de llamada predeterminados. El sistema informa al computador del usuario 14 de la conexión y el soporte lógico PPP presentará un despliegue de pantalla para el usuario indicando que la conexión ha sido establecida y cualquier otro detalle asociado con la conexión, tal como la velocidad de los datos. La dirección IP es asignada a partir de un grupo de direcciones para conexión inmediata.

Una vez que el usuario está conectado al sistema de acceso el conmutador 6 determina si la máquina del usuario 14 está requiriendo conexión a otro computador en Internet 16, en la etapa 64. El requerimiento, por ejemplo, puede ser simplemente a la página principal básica del usuario cuando el usuario abre un programa explorador de la Red de la Red del computador 14. El conmutador 6 determina entonces, en la etapa 66 revisando una bandera almacenada que representa el estado de conmutador para la dirección IP, si el usuario ha sido autenticado y que el estado no es el estado de ingreso. Si la sesión de conexión está en el estado de ingreso, el conmutador 6 conecta el usuario 14 a una página de ingreso en el servidor de la Red 22, y el sistema de control 20 ejecuta un proceso de ingreso 68. El proceso de ingreso 68 es similar al de autenticación de legalidad, en cuanto el servidor de cuenta RAS 30 reconoce que la

conexión ha ocurrido y que se ha establecido una nueva sesión para la dirección IP. Los datos para la sesión son transferidos al coordinador de sesión 34 para crear una instancia de un manejador de sesión 36 para la sesión. Con base en la dirección IP, sin embargo, el manejador de sesión 36 determina que el usuario necesita ser autenticado usando la autenticación basada en un programa explorador de la Red y de acuerdo a ello espera que el servidor de ingreso 32 reciba del servidor de la Red 22 los detalles enviados en la página de ingreso mostrada en la Figura 4. La página de ingreso presenta al usuario un cierto número de opciones, que incluye la ejecución de un proceso de registro para convertirse en un nuevo usuario registrado, entrando un nombre de usuario y una clave de acceso si ya está registrado, o páginas de ayuda para el acceso almacenadas en el servidor 22. La página también incluye cierto número de avisos o emblemas que pueden incluir enlaces a otras páginas o a sitios de la Red. Sin embargo, para ganar acceso general a Internet 16 el usuario debe ingresar una combinación válida de nombre de usuario y clave de acceso la cual es autenticada por el sistema de control 20. La página de ingreso permite al usuario ingresar una combinación de nombre de usuario y clave de acceso y luego enviar la combinación para su autenticación señalando sobre el botón de "sign in". Alternativamente la combinación puede haber sido ya almacenada en el computador por parte del usuario 14. La combinación de nombre de usuario y clave de acceso es recibida por el manejador de sesión 36 para la sesión y la combinación es enviada al cliente de autenticación 38. El cliente de autenticación 38 pasa la combinación a un mensajero de autenticación 40 que corre sobre el

servidor de bases de datos 8. El mensajero de autenticación revisa la combinación contra las combinaciones almacenadas para los usuarios para determinar si es válida, identifica el usuario y da acceso al perfil único de miembro para el usuario a partir del servidor de base de datos 8.

En el tercer escenario de autenticación, no se requiere autenticación.

En este escenario se da al usuario un número telefónico al cual marcar y que corresponde a no-autenticación. El usuario es conectado automáticamente, en forma de autenticación basada en un programa explorador de la Red, y se asigna una dirección IP a partir de un grupo para no-autenticación. La operación procede como se describió anteriormente para autenticación basada en un programa explorador de la Red, excepto que el manejador de sesión no revierte al cliente de autenticación 38 para autenticar al usuario con base en una combinación de un nombre de usuario y una clave de acceso. El usuario simplemente es autenticado de forma automática por parte del manejador de sesión 36.

Una vez que el usuario ha sido autenticado, bien sea a través del proceso de ingreso 28 o usando el servidor RADIUS 11, un manejador de sesión individual 36 utiliza los datos de perfil de miembro para el usuario para compilar y envía una página principal personalizada, como se muestra en la Figura 5, al usuario 14. La página principal personalizada también puede incluir aviso o emblemas, de la misma forma que la página de ingreso. El manejador de sesión 36 instruye al servidor redireccionador 42 para cambiar el estado del conmutador 6

a un estado de portal, después de la autenticación, el cual dirige el conmutador para conectarse al URL para la página principal personalizada o portal mostrado en la Figura 5. Los detalles concernientes a los datos del usuario y la página principal personalizada a partir del perfil de miembro son pasados por el
5 manejador de sesión 36 al servidor de ingreso 32 para tener acceso por el servidor Apache 22 el cual controla la compilación de la página principal personalizada. Subsecuentemente, el manejador de sesión 36 instruye al servidor redireccionador para divergir el conmutador
10 hacia uno de los estados del programa explorador de la Red, bien sea un estado de afiliado o un estado general. Para la autenticación basada en un programa explorador de la Red, como se muestra en la Figura 3, el proceso de autenticación de ingreso se maneja utilizando el programa explorador de la Red de la máquina del usuario 14, en
15 vez del soporte lógico PPP, y la operación retorna después del proceso de ingreso 68 a la etapa 64. De acuerdo a ello, una vez que el usuario revierte a la etapa 64 y es determinado en la etapa 66 como habiendo sido autenticado, el conmutador 6 determina en la etapa 70, con base en el estado de acceso para la sesión, si el usuario tiene permitido el
20 acceso al computador o servicio requerido. Si es así, se otorga acceso al usuario al computador o servicio en Internet 16 en la etapa 62. Si no, se avisa al usuario en la etapa 62 de la negación de acceso. La negación de acceso puede comunicarse conectando al usuario a una página de denegación del servidor Apache 22.

25 A un usuario 14 que tiene una sesión que está en el estado de afiliado se le permite el acceso, sin costo, a sitios mantenidos por afiliados del

proveedor del sistema de acceso. Los sitios de afiliados pueden mantenerse en el servidor Apache 22 o en otros servidores de Internet 16. Los sitios de afiliados se identifican por parte del URL en las reglas de estado de afilado. A los sitios de afiliados también se puede

5 tener acceso usando los enlaces provistos en las páginas de la Red de las Figuras 4 y 5. Las reglas para el estado de afiliado especifican que el acceso es negado a cualquier URL que no pertenezca a los sitios de afiliados. Sin embargo, si un usuario tiene un perfil de miembro que permita el acceso a otros sitios de Internet, el usuario está en

10 capacidad de moverse al estado general. Para estos usuarios, cuando se hace un requerimiento para tener acceso a un sitio diferente al sitio de afiliados, el programa explorador de la Red del usuario es redireccionado por el conmutador 6 a una página en blanco de transición en el servidor Apache 22 mientras que el manejador de

15 sesión 36 determina si instruye al servidor redireccionador 42 para cambiar el estado del conmutador a estado general. La página en blanco de transición contiene un código para retener el URL requerido, y pasar el URL y un mensaje al servidor de ingreso 32 advirtiéndole que el usuario está tratando de moverse del estado de

20 afiliado al estado general. Este mensaje es transferido al manejador de sesión 36, con base en la dirección IP, y el manejador de sesión 36 toma acceso al perfil de miembro. Si el manejador de sesión 36 determina sobre la base del perfil que el usuario 14 se le permite moverse al estado general, se envía un mensaje al servidor

25 redireccionador 42 para cambiar el estado del conmutador al estado general para la sesión. También se envía un mensaje desde el manejador 36 al servidor de clave de acceso 32 anunciando que al

usuario 14 le es permitido moverse al URL atrapado. El servidor de clave de acceso 32 envía un mensaje al servidor apache 22 para adelantar el usuario 14 desde la página interim a la página del URL solicitada atrapada. Si el acceso es denegado, el URL de una página denegada se utiliza para sustituir el URL atrapado, en el servidor de clave de entrada 32, y el usuario 14 es adelantado a la página de denegación.

Otros estados de acceso son el estado de registro y el estado de permisibilidad. El manejador de sesión 36 instruirá al servidor redireccionador 42 para colocar el conmutador en estado de registro para una sección cuando el usuario envía un mensaje que indica que ellos desean registrarse con el sistema de acceso. Esto podría ser echo cuando, por ejemplo, el usuario selecciona la opción de registro sobre la página de clave de entrada de la figura 4. En el estado de registro el conmutador 6 redirecciona al usuario 14 a las páginas de registro sobre el servidor apache 22 y el sistema de control 20 recolecta los detalles solicitados sobre las páginas provenientes del usuario 14 para el archivo del usuario en el servidor 8 con base de datos. El archivo de usuario normalmente incluye los datos del perfil del miembro para el usuario que se establece inicialmente sobre la base de los detalles solicitados. Un manejador de sesión 36 instruirá al servidor redireccionador para que haga que el conmutador 6 ingrese al estado de permisividad cuando la dirección IP indica que el usuario 14 va a ser proporcionado con acceso no restringido al Internet 16 sin ningún monitoreo o cargo.

64

125

120

Cuando la sección se desconecta, el RAS 4 comunica la desconexión al servidor de conteo RADIUS 30, el cual a su vez avisa al manejador de sesión 36. El manejador 36 instruye al servidor redireccional 42 para cambiar el estado del conmutador al estado de clave de acceso para la dirección IP de la sesión desconectada.

La manera en la cual el usuario es cargado se controla por un manejador de plan 44 que es ingresado por el manejador de sesión 36. El manejador de plan 44 mantiene diferentes planes de carga que pueden ser aplicados a los usuarios. Por ejemplo, todos los usuarios no serían cargados para acceso a los sitios de afiliado, pero la proporción de carga puede diferir para el acceso cuando se encuentra en estado general. Por ejemplo, los usuarios pueden ser colocados en un periodo predeterminado de acceso libre para las páginas en un estado general y luego cargados a una proporción de adecuación luego de esto. El manejador del plan especifica los tiempos y proporciones para los diferentes planes, y esto se ingresa por medio de los manejadores de sesión 36 que vigilan el tiempo que un usuario gasta en diferentes estados de ingreso. La carga final para una sesión es compilada por los manejadores de sesión 36 y luego almacenada contra los archivos de usuario en el servidor 8 con base de datos.

El método y sistema de acceso son particularmente ventajosos en la medida en que permiten que los ISP, al menos inicialmente, controlen dinámicamente las páginas observadas por un usuario. Como mínimo, el usuario debe, sin poder evitarlo, observar la página básica o de ingreso, puesto que ello constituye una parte integral del proceso de acceso. Esto permite que el ISP presente información publicitaria y

89

126 121

en particular información publicitaria particularmente dirigida con base en el perfil del usuario, lo cual puede ser garantizado por el ISP en cuanto a que ninguno de los usuarios podrá evitarla. Las páginas de ingreso y básicas particularizadas actúan entonces como un portal
5 de entrada para todos los usuarios.

El permitir también a todos los usuarios conectarse al sistema, incluyendo los usuarios que no están registrados, el ISP es capaz de presentar y proporcionar libre acceso al contenido y a servicios seleccionados y predeterminados e Internet. Por ejemplo, la
10 página de clave de entrada también puede incluir nexos a ciertas páginas de la red que proporciona acceso a bancos, negocios de acciones o compras para el hogar, y el usuario no tendrá que pagar ninguna tarifa al ISP para ingresar a estas páginas. Esto le permite al ISP actuar como un suministrador de contenido libre para ciertos
15 contenidos, mientras que carga un usuario para ingresar otros datos al Internet. Para proporcionar información a los anunciantes asociados con el contenido libre, el ISP puede, si desea, solicitar y obtener cierta información de los usuarios antes de proporcionar el contenido libre, y monitorear su acceso.

20

Codificar los estados de acceso en el conmutador 6 también le permite al ISP restringir o permitir el acceso al contenido o a los servicios seleccionados en la Internet, tal como contenido de deportes, contenido orientado para adultos o para niños.

25

Muchas modificaciones serán evidentes para aquellos expertos en la técnica sin apartarse del alcance de la presente invención como se describe aquí con referencia a los dibujos que la acompañan.

122 68
127

TRADUCCION OFICIAL No. 343/2000.-

EL TEXTO QUE SIGUE ES TRADUCCION FIEL Y COMPLETA DE UN DOCUMENTO ESCRITO EN INGLES, Y LLEVA EL SELLO Y LA FIRMA DE HELENA URIBE DE LEMOINE, TRADUCTORA E INTERPRETE OFICIAL, SEGÚN RESOLUCION No. 3618 EXPEDIDA POR EL MINISTERIO DE JUSTICIA EL 6 DE SEPT.DE 1972.

AUSTRALIA

Oficina de Patentes
Camberra

Yo, KAY WARD, LIDER DEL GRUPO DE RESPALDO DE EXAMENES Y VENTAS por el presente certifico que el documento adjunto es una copia verdadera de la especificación Provisional en relación con la Solicitud de patente No. PQ 0213 hecha por SYDNEY GORDON LOW radicada el 6 de mayo de 1999.

Certifico además que la anterior solicitud está ahora a nombre de SHARINGA NETWORKS INC. de conformidad con las disposiciones de la Sección 113 de la Ley de Patentes de 1990

EN EVIDENCIA DE LO CUAL, he puesto mi firma hoy día veinticinco de Mayo de 2000.

FIRMADO POR: KAY WARD, LIDER DEL GRUPO DE RESPALDO DE EXAMENES Y VENTAS. HAY SELLO EN RELIEVE DE LA OFICINA DE PATENTES DE AUSTRALIA.

LA TRADUCTORA OFICIAL



HELENA URIBE DE LEMOINE.



67
128 123

Patent Office
Canberra

I, KAY WARD, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PQ 0213 for a patent by SYDNEY GORDON LOW filed on 06 May 1999.

I further certify that the above application is now proceeding in the name of SHARINGA NETWORKS INC pursuant to the provisions of Section 113 of the Patents Act 1990.

WITNESS my hand this
Twenty-fifth day of May 2000

K Ward

KAY WARD
TEAM LEADER EXAMINATION
SUPPORT AND SALES



68
129 124

Regulation 3.2



Sharinga Networks Inc.
~~Freemove.com.au Pty. limited~~
Sydney Gordon Low



A U S T R A L I A
Patents Act 1990

PROVISIONAL SPECIFICATION
for the invention entitled:

"A Communications Network Access Method and System"

The invention is described in the following statement:

125-69
130

A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

The present invention relates to a method and system for accessing a communications network, such as the Internet.

5

Most Internet users currently connect to the Internet via the equipment of an Internet service provider (ISP). The ISP provides remote access servers (RASs) which are able to communicate with remote computers of the users using modems and standard telephone lines. The remote computers and the RASs use standard software that executes a protocol, such as
10 the point to point protocol (PPP), to allow the users to dial into the RASs and connect to the Internet. To achieve this, the connection or PPP software on the user's computer requires the user to enter unique authentication data, such as the user's login name and password, and this is transmitted to the ISP when the software dials and contacts to the ISP equipment. If the ISP equipment determines that the authentication data is valid, the user's computer is connected
15 and the user is allowed uninhibited access to the Internet. The user is accordingly free to view any desired web pages using a web browser on the user's computer.

The success of web sites on the Internet, particularly from a commercial perspective, is almost solely dependent on a site's ability to attract traffic to it. For this reason, a number
20 of well known sites, such as Netscape's home page and the home pages of ISPs have been reconfigured to operate as communication "portals" to the Internet in the hope that users will continually revert to the sites to determine where to direct their browsers next. A number of sites have proved to be extremely lucrative, in the same manner as television stations which are able to attract large numbers of viewers. The current market value of companies such as
25 Yahoo and Excite, which maintain high traffic volume sites, indicates how lucrative. As ISPs constitute a first point of connection for most Internet users, any steps or method which an ISP can implement to direct users to particular pages, rather than the user's own default home page, would be highly desirable. The present invention seeks to provide such method or at least provide a useful alternative.

30

In accordance with the present invention there is provided a communications network

70
13A 12.6

access method, including:

- receiving a request from a computer device to connect to said network;
- connecting said computer device to said network in response to said request;
- sending login data to said computer device after said connecting step, said login data
- 5 being adapted to generate a login display on said computer device allowing entry of unique authentication data by a user of said device;
- receiving said unique authentication data entered on the computer; and
- allowing said user to access said network using said computer device when said authentication data is validated.

10

Preferably said method includes accessing profile data for said user after said allowing step and controlling access to said network using said profile data. Advantageously, said method may include having a set of access profiles encoded in a switch, and said profile data accessed for said user represents one of said encoded profiles.

15

Advantageously, the login display may include advertising material and links to particular locations on the communications network. Advantageously, the communications network may be the Internet and said login data represents a login web page sent to said computer device after connecting to the network. Advantageously, said request receiving and

20 connecting steps may be executed using standard communication protocols, such as PPP, and a modem of the computer device and a RAS of the network. Advantageously, the steps of the method may be executed by equipment of an ISP.

The present invention also provides a communications network access system,

25 including:

- means for receiving a request from a computer device to connect to said network and for connecting the computer device to the network in response to the request;
- means for sending login data to the computer device after it is connected to the network, said login data being adapted to generate a login display on the computer device
- 30 which allows entry of unique authentication data by a user of the device; and
- means for receiving said unique authentication data entered by the user and for

127
~~137~~

allowing the user to access the network using the computer device on determining that the authentication data is valid.

Advantageously, the receiving and connecting means may include a RAS. The sending
5 means may include a web server, and the receiving and allowing means may include, the web server and a user database.

The present invention also provides a communications network access method, including:

- 10 sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;
- receiving login data after being connected;
- generating a login display on the computer device, based on the login data, said display allowing entry of unique authentication data;
- 15 sending unique authentication data entered on the computer device to the network; and
- obtaining access to the network after said authentication data is validated.

A preferred embodiment of the present invention is hereinafter described, by way of example only with reference to the accompanying drawings, wherein:

- 20 Figure 1 is a block diagram of a preferred embodiment of a communications network access system;
- Figure 2 is a flow diagram of a preferred embodiment of a communications network access method;
- Figure 3 is a diagram of a login page of the system and method; and
- 25 Figure 4 is a diagram of a customized home page of the system and method.

A communications access system, as shown in Figure 1, includes a plurality of remote access servers (RASs) 4, a layer four switch 6, a member profile database 8, a web server 10 and a router 12. The RASs 4 are provided to allow the computers 14 of remote users to dial
30 into the system using standard telecommunication lines and modems and connect to the input ports of the RASs 4, respectively. On connection to a port of an RAS 4 the user's computer

128 72
~~123~~

- 5 -

14 establishes a unique TCP session and the IP traffic for that session is switched by the switch 6. Once the user is authenticated, as described below, the user's computer 14 is allowed to access requested data on the Internet 16. The web server 10 is used to present pages to a user 14 connected to an RAS 4 and the member profile database 8 is used in 5 controlling authentication of the user and access to the Internet, as described below. As far as the user 14 is concerned, the equipment 4, 6, 8, 10 and 12 of the access system is part of the Internet. The equipment 4, 6, 8, 10 and 12 includes standard commercially available hardware and basic database, web server and Internet access software which is known to those skilled in the art and is used in the access systems of most ISPs. The layer four switch is the 10 exception, and if used by an ISP, is normally used to balance the traffic handled by the RASs 4. An example of a suitable layer four switch is the Cache Director TM produced by Alteon WebSystems Inc. The access system differs from that offered by ISPs, as described below, in that the layer four switch 6 is used to connect users to the web server 10 and then control access to the Internet 16 for the users 14 on the basis of a limited number of access profiles 15 encoded in the switch 6.

When a user 14 wishes to connect to the Internet using the access system, the user 14 simply dials into the system using standard PPP software, at step 22 of the access procedure 20 shown in Figure 2. The RASs 4 and the layer four switch 6 however do not require the 20 user 14 to enter any username or password when using the PPP software in order to connect to the system. The user is automatically connected, and a TCP session established, when the user dials into a port of an RAS 4, without any authentication. The system informs the user's computer 14 of the connection and the PPP software will display for the user the fact that the connection has been established and any other details associated with the connection, such as 25 the data rate.

Once the user is connected to the access system the switch 6 determines whether the user's machine 14 is requesting connection to another computer on the Internet 16, at step 24. The request for example, may be simply to the user's default home page when the user opens 30 a web browser of the computer 14. The switch 6 then determines, at step 26 by checking a stored flag, whether the user has been authenticated. If not, the switch 6 connects the user 14

23
134 129

- 6 -

directly to the web server 10. The web server 10 executes a login process 28 which involves sending the web pages shown in Figures 3 and 4 to the user 14. The login page shown in Figure 3 is sent first to the user 14. The page presents the user with a number of options, which includes executing a registration process to become a new registered user, entering a username and password if already registered, or accessing help pages stored on the server 10. The page also includes a number of banner advertisements which may include links to other pages or web sites. To gain general access to the Internet 16 however, the user must enter a valid username and password combination which is authenticated by the server 10. The login page allows the user to enter a username and password combination and then send the combination for authentication to the server 10 by clicking on the "sign in" button. Alternatively the combination may already be stored on the computer 14 by the user. The server 10 checks the combination and if valid, identifies the user and accesses a unique member profile for the user from the database 8. The member profile contains details concerning the user and customized home page data which allows the server to then compile and send a customized home page, as shown in Figure 4, to the user 14 on successfully completing the login process 28. The customized home page may also include banner advertisements, in the same manner as for the login page. The login and authentication process is therefore managed using the web browser of the user's machine 14, rather than the PPP software.

20

The member profile also specifies which one of a limited number of access profiles the user belongs to. The different access profiles are encoded in the layer four switch 6, and on authentication of a TCP session managed by the switch, a data value is stored indicating for the switch 6 which of the access profiles the session belongs to. The number of access profiles may be only, for example, four and each contains a list of IP addresses which can or cannot be accessed for a session. Accordingly, once the user reverts to step 24 and is determined at step 26 as having been authenticated, the switch 6 determines at step 30, on the basis of the access profile for the session, whether the user is allowed to access a requested computer or service. If so, the user is granted access to the computer or service on the Internet 16 at step 32. If not, the user 14 is advised at step 34 of the access denial. The access denial can be communicated by connecting the user to a denial page of the server 10.

130 74
135

- 7 -

The access method and system are particularly advantageous as they allow ISPs, at least initially, to control the pages viewed by a user. As a minimum, the user must, and cannot avoid, viewing the login and customized home pages, as these are an integral part of the login process. This allows the ISP to present advertising information, and in particular
5 present target advertising information based on the user's profile, which the ISP can guarantee that all of its users will not be able to avoid. The login and customized home pages therefore act as an entry portal for all users.

By allowing all users to directly connect to the system, including users which are not
10 registered, the ISP is able to present and provide free access to selected Internet content and services via the login page. For example, the login page may include links to certain web pages that provide banking, stock trading or home shopping, and the user will not have to pay any fees to the ISP to access these pages. This allows the ISP to act as a free content provider for certain content, whilst charging a user to access other data on the Internet. To provide
15 information to advertisers associated with the free content, the ISP can, if desired, still require and obtain certain information on and from users before providing the free content.

Encoding the access profiles in the switch 6 also allows the ISP to restrict or allow access to selected content or services on the Internet, such as sports betting, adult orientated
20 content or children's content.

Many modifications will be apparent for those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

25

DATED this 6th day of May 1999.

Sydney Gordon Low

30 By DAVIES COLLISON CAVE

Patent Attorneys for the Applicant.

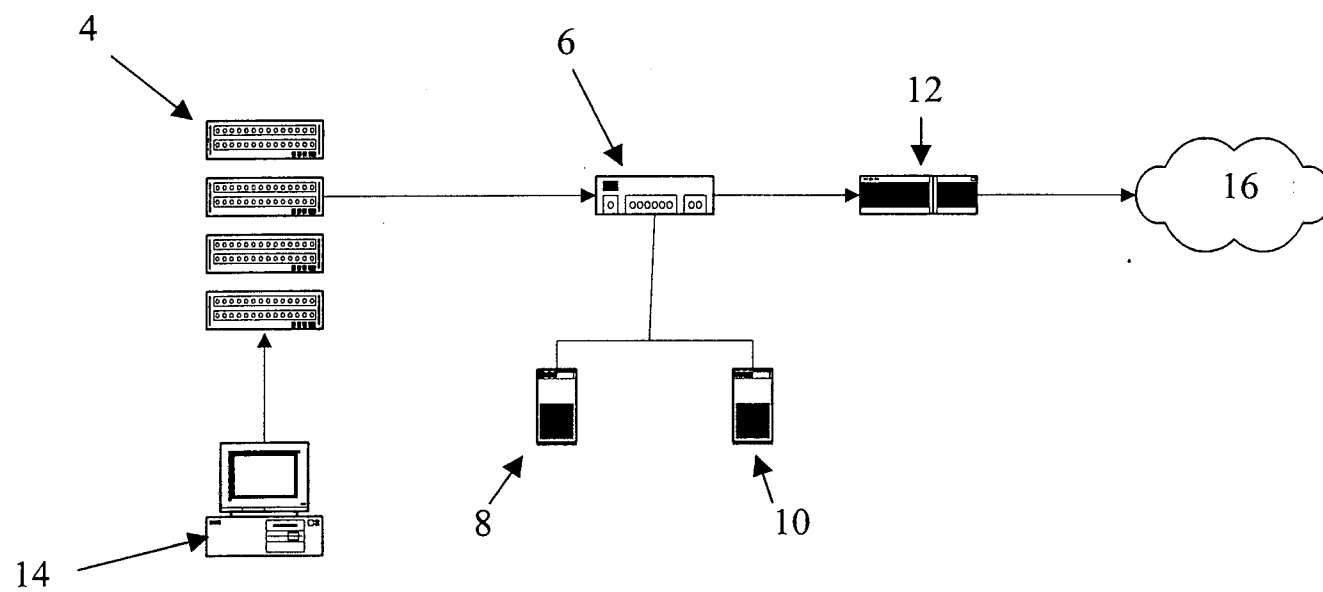
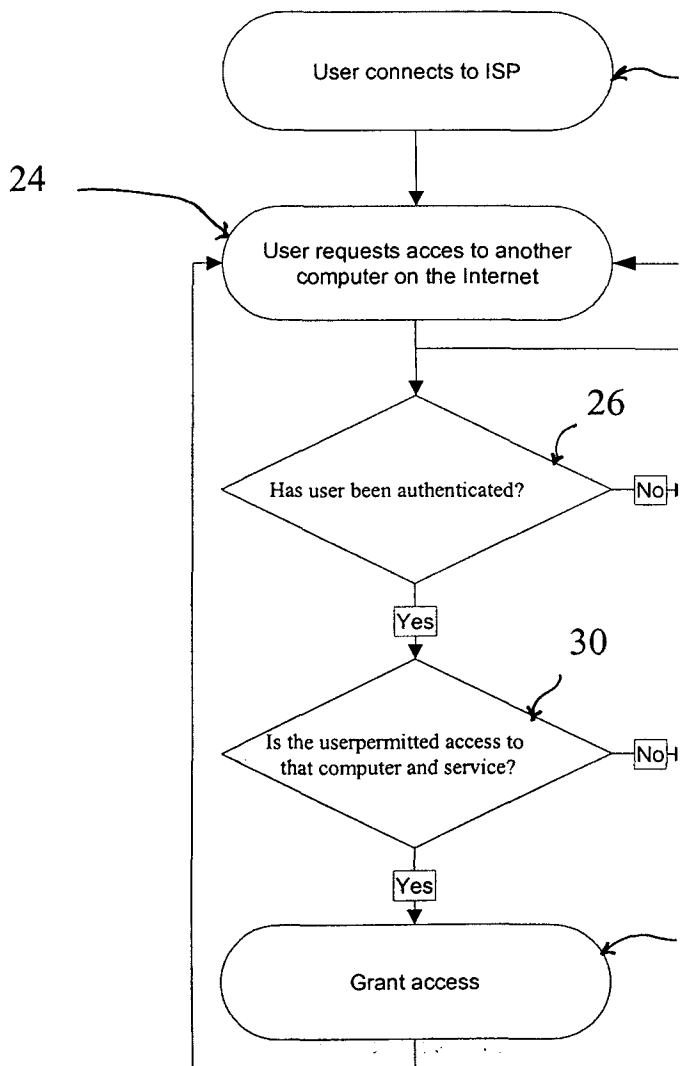


Figure 1

132

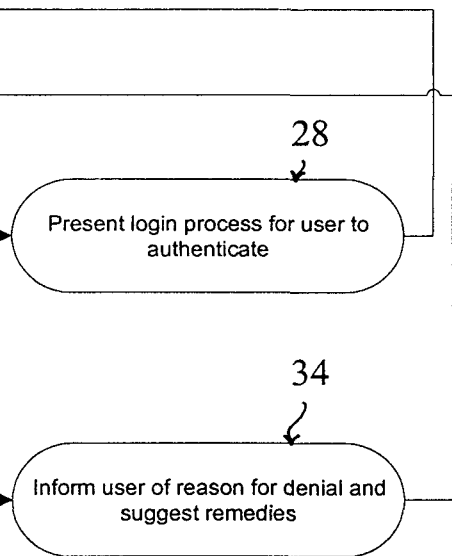
Figure 2



132

20

22



32

137

26

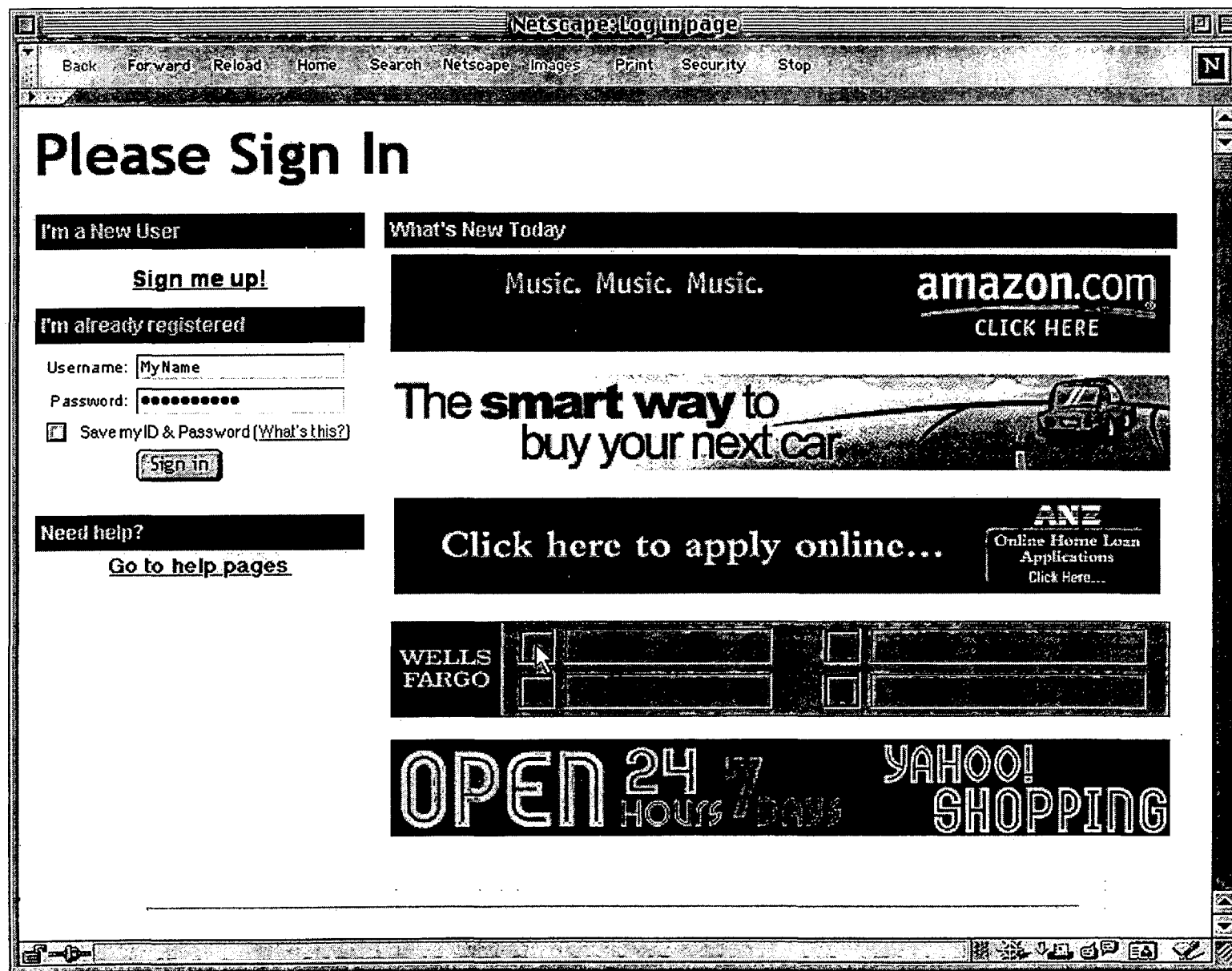


Figure 3

133

138

77

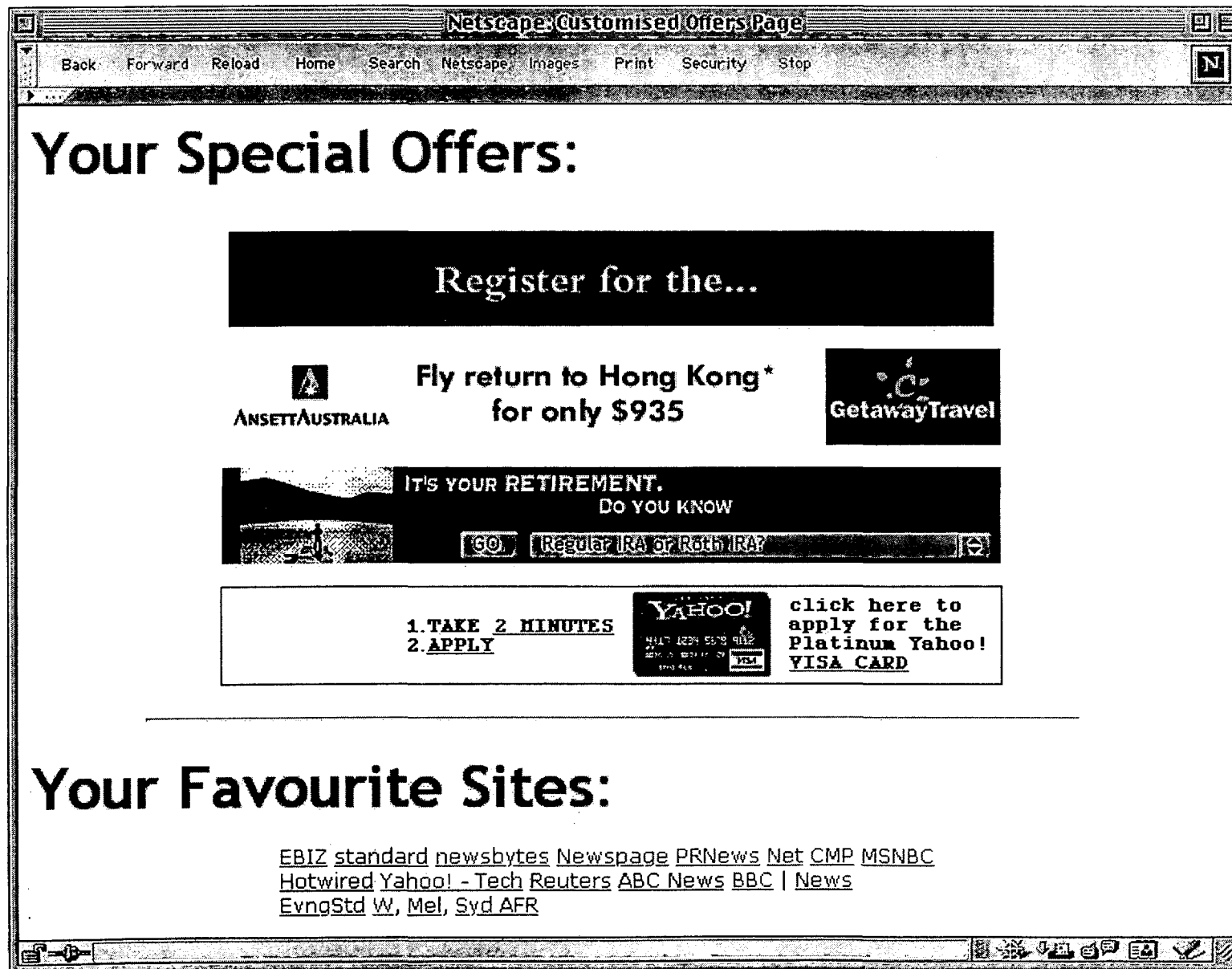


Figure 4

157

88

UN MÉTODO Y SISTEMA DE ACCESO A UNA RED DE COMUNICACIONES

La presente invención se relaciona con un método y sistema para
5 tener acceso a una red de comunicaciones, tal como Internet.

La mayoría de los usuarios de Internet se conectan a Internet
actualmente a través del equipo de un proveedor de servicio de
Internet (ISP). El ISP provee servidores de acceso remoto (RAS) que
10 tienen la capacidad de comunicarse con computadores remotos de los
usuarios utilizando módems y líneas telefónicas estándar. Los
computadores remotos y los RAS usan soporte lógico estándar el cual
ejecuta un protocolo, tal como el protocolo de punto a punto (PPP),
para permitir que los usuarios marquen hacia el RAS y se conecten a
15 Internet. Para lograr esto, el soporte lógico o PPP de conexión en el
computador del usuario requiere que éste ingrese datos propios de
autenticación, tales como el nombre y clave de acceso del usuario,
que son transmitidos al ISP cuando el soporte lógico marca y se
conecta al equipo del ISP. Si el equipo del ISP determina que los datos
20 de autenticación son válidos, el computador del usuario se conecta y
permite al usuario un acceso sin inhibiciones a Internet. De acuerdo
con esto, el usuario está en libertad de ver cualquier página de la Red
utilizando un programa explorador de la red en el computador del
usuario.

25

El éxito de los sitios de la Red en Internet, particularmente desde una
perspectiva comercial, depende casi exclusivamente de la habilidad

del sitio para atraer tráfico hacia sí. Por esta razón, un cierto número de sitios bien conocidos, tales como la página principal de Netscape y las páginas principales de los ISP, han sido reconfiguradas para operar como "portales" de comunicación hacia Internet en la
5 esperanza de que los usuarios retornarán continuamente a los sitios para determinar hacia donde dirigirán enseguida sus programas exploradores de la Red. Un cierto número de sitios han probado ser extremadamente lucrativos, de la misma forma que las estaciones de televisión las cuales son capaces de atraer grandes cantidades de
10 televidentes. El valor actual en el mercado de compañías tales como Yahoo y Excite, que mantienen sitios de alto volumen de tráfico, indican cuan lucrativos son. Puesto que el ISP constituye un primer punto de conexión para la mayoría de usuarios de Internet, cualquier paso o método que un ISP pueda implementar para dirigir a los
15 usuarios a páginas particulares, más que a la propia página inicial del usuario, serían altamente deseables. La presente invención busca proveer tal método o al menos proveer una alternativa útil.

De acuerdo con la presente invención se provee un método de acceso
20 a una red de comunicaciones, incluyendo:

Recibir un requerimiento desde un dispositivo de computador para conectar a dicha red;

Conectar dicho dispositivo de computador a dicha red, en respuesta a dicho requerimiento;

25 Enviar datos de ingreso a dicho dispositivo de computador después de dicha etapa de conexión, siendo adaptados dichos datos de ingreso para generar una pantalla de ingreso sobre dicho

dispositivo de computador permitiendo la entrada de datos únicos de autenticación por un usuario de dicho dispositivo;

Recibir dichos datos únicos de autenticación ingresados al computador; y

5 Permitir a dicho usuario tener acceso a dicha red usando dicho dispositivo de computador cuando dichos datos de autenticación son validados.

Preferiblemente dicho método incluye tener acceso a datos de perfiles
10 para dicho usuario después de dicha etapa de permisión y control del acceso a dicha red usando dichos datos de perfiles. Ventajosamente, dicho método puede incluir tener un conjunto de perfiles de acceso codificados en un conmutador, y dichos datos de perfiles a los cuales se ha tenido acceso por dicho usuario representan uno de dichos
15 perfiles codificados.

Ventajosamente, la pantalla de entrada puede incluir material publicitario y se enlaza a localizaciones particulares en la red de comunicaciones. Ventajosamente, la red de comunicaciones puede ser el Internet y dichos datos de ingreso representan una página de
20 ingreso a la Red para dicho dispositivo de computador después de conectarse a la red. Ventajosamente, dicho requerimiento que recibe y conecta etapas puede ser ejecutado usando protocolos de comunicación estándar, tales como PPP, y un módem del dispositivo de computador y un RAS de la cadena. Ventajosamente, las etapas
25 del método pueden ejecutarse mediante el equipamiento de un ISP.

La presente invención también provee un sistema de acceso a una red de comunicaciones, incluyendo:

medios para recibir un requerimiento desde un dispositivo computador para conectar a dicha red y para conectar el dispositivo computador a la red en respuesta al requerimiento;

medios para enviar datos de nombre al dispositivo computador después de éste se ha conectado a la red, siendo adaptados dichos datos de nombre para generar un despliegue de pantalla del nombre en el dispositivo computador lo cual permite la entrada de datos exclusivos de autenticación por parte de un usuario del dispositivo; y

medios para recibir dichos datos exclusivos de autenticación ingresados por el usuario y para permitir al usuario tener acceso a la red usando el dispositivo computador al determinar que los datos de autenticación son válidos.

Ventajosamente, los medios de recepción y conexión pueden incluir un RAS. Los medios de envío pueden incluir un servidor de la Red, y los medios de recepción y permisión pueden incluir el servidor de la Red y una base de datos de usuarios.

La presente invención también provee un método de acceso a una red de comunicaciones, incluyendo:

enviar un requerimiento desde un dispositivo computador para conectarse a una red de comunicaciones; y ser conectado a la red en respuesta al requerimiento;

recibir datos de nombre de ingreso después de ser conectado;

generar un despliegue de pantalla del nombre de acceso en el dispositivo computador, con base en los datos de nombre de acceso, permitiendo dicho despliegue de pantalla la entrada de datos de autenticación exclusivos;

enviar los datos de autenticación exclusivos ingresados en el dispositivo computador a la red; y

obtener acceso a la red después de que dichos datos de autenticación sean validados.

Una modalidad preferida de la presente invención se describe a continuación, a manera de ejemplo solamente con referencia a los dibujos acompañantes, en los cuales:

La figura 1 es un diagrama de bloques de una modalidad preferida de un sistema de acceso a una red de comunicaciones;

La figura 2 es un diagrama de flujo de un método de acceso a una red de comunicaciones del sistema de acceso;

La figura 3 es un diagrama de la página de ingreso del sistema y del método; y

La figura 4 es un diagrama de una página básica personalizada del sistema y el método.

Un sistema de acceso a comunicaciones, como se muestra en la figura 1, incluye una pluralidad de servidora de acceso remotos (RAS)4, un conmutador de base cuatro o superior 6, un servidor de base de datos

8, un sistema servidor de la Red 10 y un enrutador 12. El RAS 4 se provee para permitir a los computadores 15 de los usuarios remotos marcar hacia el sistema usando líneas de telecomunicación y módems estándar para conectarse a los puertos de entrada del RAS 4, respectivamente. Al conectarse a un puerto de un RAS 4, el RAS 4 y el computador 14 de usuario establecen una sesión exclusiva TCP/IP y el tráfico IP para esa sesión es conmutado por el conmutador 6. Una vez que el usuario es autenticado o aprobado, como se describe más abajo, el computador 14 del usuario es autorizado para tener acceso a los datos requeridos en Internet 16. El sistema servidor de la Red 10 se usa para controlar las páginas presentadas a un usuario 14 conectado al RAS y manejar la autenticación usando una base de datos de perfil de miembros mantenida en el servidor de base de datos 8, como se describe más abajo. Un servidor de autenticación RADIUS (Marcación Remota de Autenticación en Servicio de Usuario) también se provee para uso en autenticación. En cuanto se relaciona con el usuario 14, los equipos 4, 6, 8, 10, 11 y 12 del sistema de acceso son parte de Internet. Los equipos 4 a 12 incluyen equipamiento estándar comercialmente disponible, un servidor de la Red y un soporte lógico de acceso a Internet que es conocido para los expertos en la técnica y se usan en los sistemas de acceso de la mayoría de los ISP. Los equipos 4 a 12 entonces incluyen también un código de programa único para manejar y controlar cada sesión, como se discute más abajo. El conmutador de base cuatro o superior 6 es otra excepción. El conmutador 6 se usa normalmente por los ISP para balancear el tráfico manejado por el RAS 4. Un ejemplo de un conmutador de base cuatro apropiado es el Cache Director™

producido por Alteon WebSystems Inc. El sistema de acceso difiere del ofrecido por los ISP, como se describe más adelante, en que el conmutador de base cuatro 6 se utiliza para conectar usuarios al sistema servidor de la Red 10 y para controlar el acceso a Internet 16 para los usuarios 14 sobre la base de un número limitado de estados de acceso codificados en el conmutador 6.

Cuando el usuario 14 quiere conectarse a Internet usando el sistema de acceso, el usuario 14 marca hacia el sistema usando el soporte lógico PPP estándar, en la etapa 22 del procedimiento de acceso 20 mostrado en la Figura 2. El RAS 4 y el conmutador de capa cuatro 6 no requieren sin embargo que el usuario 14 ingrese un nombre de usuario o clave de acceso cuando se usa el soporte lógico PPP para conectarse al sistema. El usuario es conectado automáticamente, y se establece una sesión TCP, cuando el usuario marca hacia un puerto de un RAS 4, sin autenticación alguna. El sistema informa al computador del usuario 14 acerca de la conexión y el soporte lógico PPP presentará al usuario el hecho de que la conexión ha sido establecida y cualquier otro detalle asociado con la conexión, tal como la velocidad de los datos.

Una vez que el usuario está conectado al sistema de acceso el conmutador 6 determina si la máquina del usuario 14 está requiriendo conexión a otro computador en Internet 16, en la etapa 24. El requerimiento, por ejemplo, puede ser simplemente a la página principal básica del usuario cuando el usuario abre un programa explorador de la Red de la Red del computador 14. El conmutador 6

ingreso 28. La página principal particularizada también puede incluir avisos publicitarios, de la misma forma que la página de ingreso. El proceso de ingreso y autenticación se maneja entonces usando el programa explorador de la Red de la máquina del usuario 14, en vez
5 del soporte lógico PPP.

El perfil de miembro también especifica a cual de un número limitado de perfiles de acceso pertenece el usuario. Los diferentes perfiles de acceso están codificados en el conmutador de capa cuatro 6, y por la autenticación de una sesión TCP manejada por el conmutador, se
10 almacena un valor de datos indicativo para conmutador 6 acerca de a cual de los perfiles de acceso pertenece la sesión. El número de perfiles de acceso puede ser solamente, por ejemplo, cuatro y cada uno contiene una lista de direcciones IP a las cuales se puede o no tener acceso para una sesión. De acuerdo a ello, una vez que el
15 usuario revierte a la etapa 24 y está determinado en la etapa 26 como habiendo sido autenticado, el conmutador 6 determina en la etapa 30, sobre la base del perfil de acceso para la sesión, si al usuario se le permite tener acceso a un computador o servicio requerido. Si es así, se otorga acceso al usuario al computador o servicio en el Internet 16
20 en la etapa 32. Si no, se avisa al usuario 14 en la etapa 34 acerca del acceso denegado. El acceso denegado puede ser comunicado conectando al usuario a una página de denegación del servidor 10.

El método y sistema de acceso son particularmente ventajosos en la
25 medida en que permiten que los ISP, al menos inicialmente, controlen dinámicamente las páginas observadas por un usuario. Como mínimo, el usuario debe, sin poder evitarlo, observar la página básica

o de ingreso, puesto que ello constituye una parte integral del proceso de acceso. Esto permite que el ISP presente información publicitaria y en particular información publicitaria particularmente dirigida con base en el perfil del usuario, lo cual puede ser garantizado por el ISP en cuanto a que ninguno de los usuarios podrá evitarla. Las páginas de ingreso y básicas particularizadas actúan entonces como un portal de entrada para todos los usuarios.

Al permitir también a todos los usuarios conectarse al sistema, incluyendo los usuarios que no están registrados, el ISP es capaz de presentar y proporcionar libre acceso al contenido y a servicios seleccionados y predeterminados e Internet. Por ejemplo, la página de clave de entrada también puede incluir nexos a ciertas paginas de la red que proporciona acceso a bancos, negocios de acciones o compras para el hogar, y el usuario no tendrá que pagar ninguna tarifa al ISP para ingresar a estas páginas. Esto le permite al ISP actuar como un suministrador de contenido libre para ciertos contenidos, mientras que carga un usuario para ingresar otros datos al Internet. Para proporcionar información a los anunciadores asociados con el contenido libre, el ISP puede, si desea, solicitar y obtener cierta información sobre y de los usuarios antes de proporcionar el contenido libre.

Codificar los estados de acceso en el conmutador 6 también le permite al ISP restringir o permitir el acceso al contenido o a los servicios seleccionados en la Internet, tal como contenido de deportes, contenido orientado para adultos o para niños.

145-88
A49

determina entonces, en la etapa 26 revisando una bandera almacenada, si el usuario ha sido. Si no, el conmutador 6 conecta el usuario 14 directamente al servidor de la Red 10. El servidor de la Red 10 ejecuta un proceso de ingreso 28 que involucra enviar las

5 páginas de la Red mostradas en las Figuras 3 y 4 al usuario 14. La página de ingreso mostrada en la Figura 3 es enviada primero al usuario 14. La página de ingreso presenta al usuario un cierto número de opciones, que incluye la ejecución de un proceso de registro para convertirse en un nuevo usuario registrado, entrando un

10 nombre de usuario y una clave de acceso si ya está registrado, o páginas de ayuda para el acceso almacenadas en el servidor 10. La página también incluye cierto número de avisos o emblemas que pueden incluir enlaces a otras páginas o a sitios de la Red. Sin embargo, para ganar acceso general a Internet 16 el usuario debe

15 ingresar una combinación válida de nombre de usuario y clave de acceso la cual es autenticada por el servidor 10. La página de ingreso permite al usuario ingresar una combinación de nombre de usuario y clave de acceso y luego enviar la combinación para su autenticación al servidor 10 señalando sobre el botón de "sign in". Alternativamente

20 la combinación puede haber sido ya almacenada en el computador por parte del usuario 14. El servidor 10 revisa la combinación y si es válida, identifica el usuario y da acceso al perfil único de miembro para el usuario a partir del servidor de base de datos 8. El perfil de miembro contiene detalles concernientes al usuario y a los datos de la

25 página principal particularizada que permiten que el servidor compile y envíe una página principal particularizada, como se muestra en la Figura 4, al usuario 14 completando exitosamente el proceso de

146 89
ASO

Muchas modificaciones serán evidentes para aquellos expertos en la técnica sin apartarse del alcance de la presente invención como se describe aquí con referencia a los dibujos que la acompañan.

147 90
151

-29-

enviar datos de autenticación únicos ingresados en el dispositivo de computador a la red;

Obtener ingreso a la red después de que dichos datos de autenticación se validan.

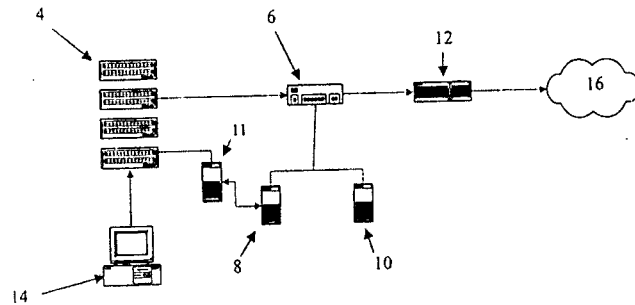


Figure 1

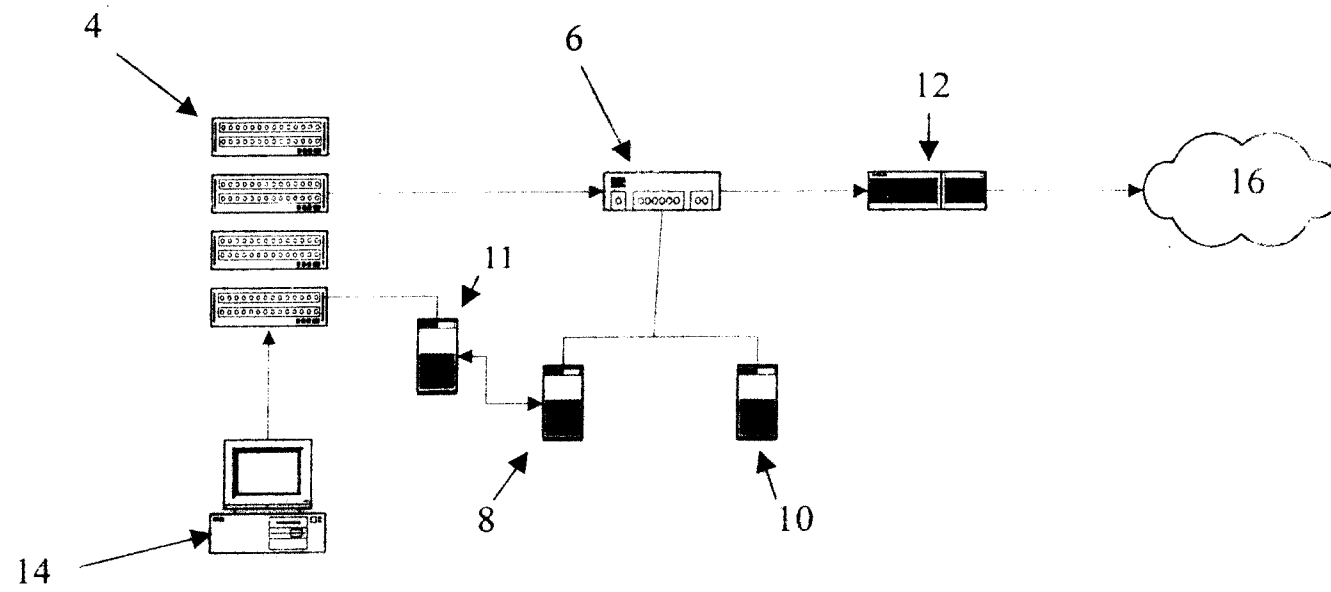


Figure 1

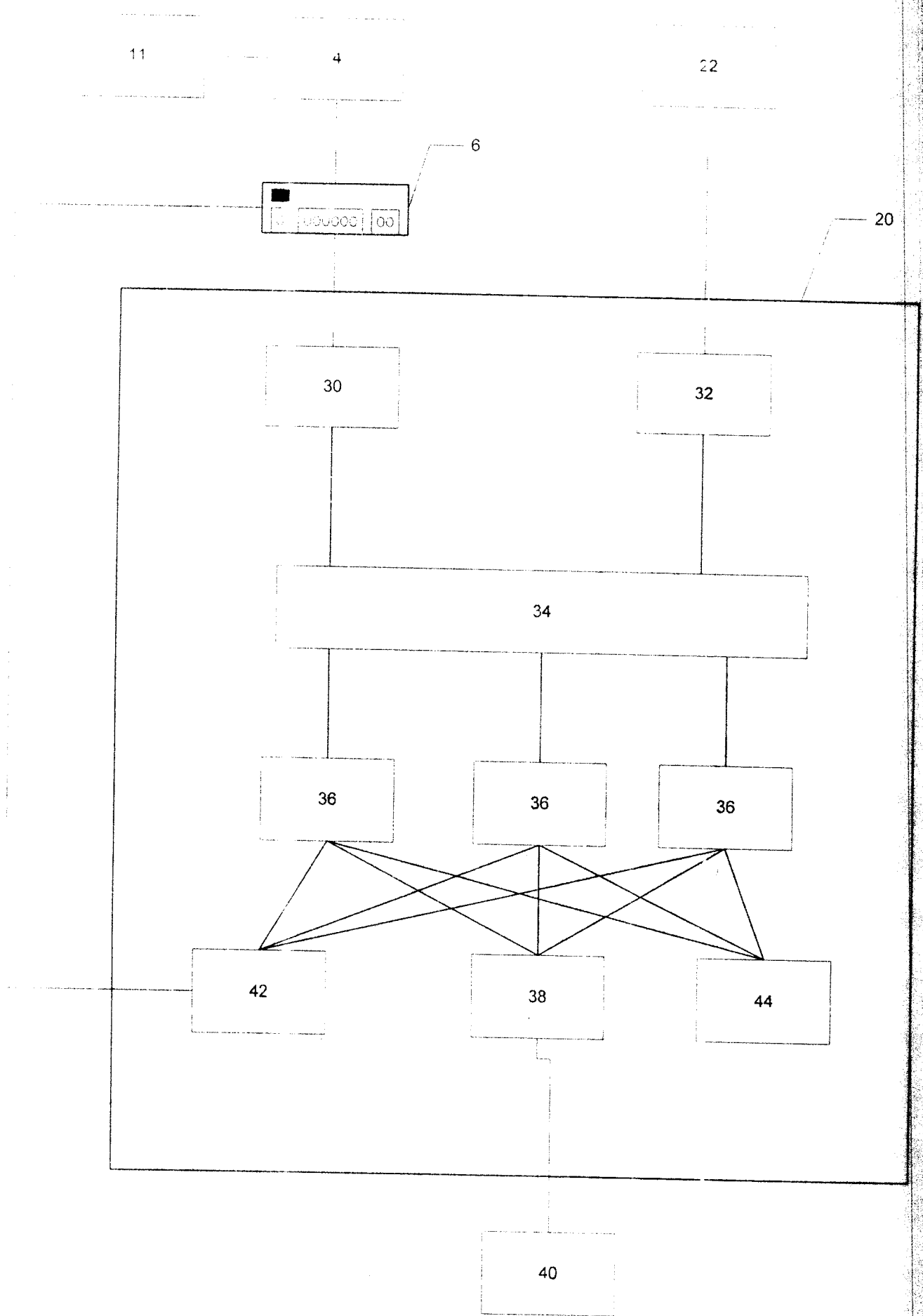


Figure 2

60

62
Usuario se conecta
o / ISP

64

Usuario requiere acceso
o otro computador
en el Internet

66
Ha sido autenticado
el usuario?

68
Proceso de ingreso en
curso para autenti-
cación del usuario.

70
Está permitido
el acceso del usuario
a ese computador
y servicio?

74
Se informa al usuario
de lo curso lo negada
y se sugieren remedios

72
Se otorga acceso

FIGURA 3

154

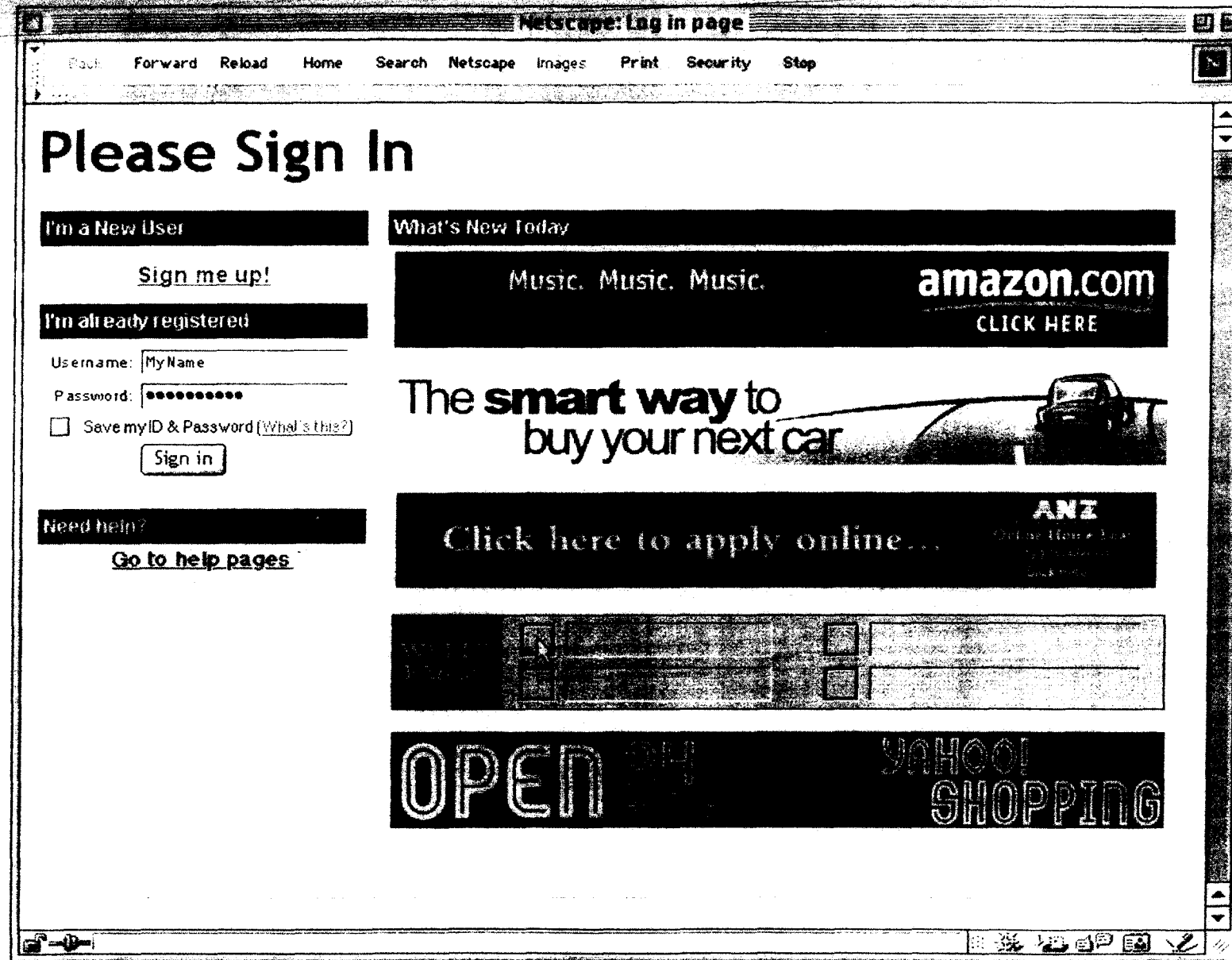


Figure 4



Figure 5

FORMATO DE DIGITALIZACION RELACION DE ANEXOS

153

Expediente No		00032800	No de Folio
		No de unidades	✓
1	CD		
2	DVD		
3	REVISTA		
4	LIBRO		
5	PERIODICO		
6	DISQUETES		
7	SOBRE DE MANILA	1	
8	SOBRE BLANCO TAMAÑO CARTA		
9	SOBRE BLANCO TAMAÑO OFICIO		
10	OTROS:		

Observaciones: SOBRE VACIO

2do. EXAMEN DE FORMA PATENTE DE INVENCION

Folio 158

Radicación no 00-32800
Concepto Técnico no . 395
Clasificación Internacional de Patentes : 6 GO6F17/60

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486 se determinó que esta solicitud de **Patente de Invención**:

- | | |
|---|---|
| SI [☒] NO [] | Contiene un resumen de la invención (Art.26-e). |
| SI [☒] NO [] | Contiene el título o nombre de la invención (Art.27-d). |
| SI [☒] NO [] | Contiene la descripción de la invención (Art.26-b). |
| SI [☒] NO [] | NO ES APLICABLE [] Contiene los dibujos necesarios para comprender la invención (Art.26-d) |
| SI [☒] NO [] | Contiene una o más reivindicaciones. (Art.26-c). |
| SI [] NO [] | NO ES APLICABLE [☒] Han sido desarrollados los productos y/o procedimientos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen. (Art. 26- h). |
| SI [] NO [] | NO ES APLICABLE [☒] Los productos y/o procedimientos han sido obtenidos o desarrollados a partir de los conocimientos tradicionales de las comunidades indígenas, afroamericanas, o locales de los países miembros, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes.(Art.26-i). |
| SI [] NO [☒] | La invención se refiere a un producto relativo a un material biológico. (Art.26-J). |
| SI [☒] NO [] | La prioridad coincide con la materia reivindicada. |
| SI [☒] NO [] | CUMPLE LOS REQUISITOS TÉCNICOS |

OBSERVACIONES Y OTROS: SI [☒] NO [] ver hoja(s) anexa(s)

EXAMINADOR TÉCNICO
202044

Bogotá D. C. Febrero 13 de 2003.

Folio 159

Concepto técnico no. 395

OBSERVACIONES

- Envía el documento mediante el cual reivindica la prioridad PQ 3682/99 Folios 86-105 y la prioridad PQ 0213 Folios 128-139.
- Anexa la traducción del documento de prioridad PQ 3682/99 Folios 106-126 y la traducción de la prioridad PQ 0213 Folios 140-151.
- Anexa el poder folios 64 -71 y la representación legal de la persona jurídica del solicitante Folios 64-85.
- Anexa los dibujos alucivos a la invención. Folios 152-156.
- Anexa un nuevo capítulo reivindicatorio. Folio 151.
- Anexa artes finales . Folio 157.

EXAMINADOR TECNICO
202044

Bogotá, Febrero 13 de 2003.

Folio 160

2020
Bogotá DC

Doctor(a)
DILIA MARIA RODRIGUEZ D'ÁLEMAN
Apoderado(a)

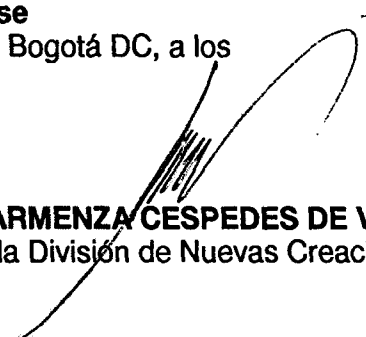
REFERENCIA:	Radicación No.	00-32800
	Trámite	002
	Evento	001
	Actuación	416
	Oficio No.	495
	Folios	001

Teniendo en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las demás disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial, conforme lo establece el artículo 40 de la misma Decisión.

Cúmplase

Dado en Bogotá DC, a los

25 MAR. 2003


ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones

202044

DIVISION DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No. 00-032800

EL EXTRACTO DE LA PRESENTE SOLICITUD DE **PATENTE DE INVENCION**
FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No **530**, DE
FECHA **31 DE JULIO DE 2003**, EL TERMINO HABIL SEÑALADO POR LA LEY
EXPIRA EL **28 DE OCTUBRE DE 2003**.

NOTA: Dentro del plazo de los seis (6) meses siguientes a partir de la fecha de publicación en la gaceta de Propiedad Industrial, deberá solicitar y cancelar el examen de patentabilidad so pena de que la solicitud caiga en abandono, de acuerdo con lo establecido en el Artículo 44 de la Decisión 486/2000.

SE PRESENTARON OPOSICIONES POR PARTE DE TERCEROS.

SI

NO ☒

Bogotá D.C., Febrero de 2004