AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Central District - Southern Division on the following

□ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. SACV12-00522 JST (ANx)	DATE FILED 4/5/2012	U.S. DISTRICT COURT Central District - Southern Division

PLAINTIFF Linksmart Wireless Technology, LLC	DEFENDANT T-Mobile USA, Inc., et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,779,118	8/17/2004	Linksmart Wireless Technolgy, LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
Order by Judge Andrew J. Guilford granting to stay case. Case Terminated 6/26/13

CLERK	(BY) DEPUTY CLERK	DATE
Terry Nafisi	Trina DeBose	7/26/13

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Central District - Southern Division on the following □ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
SACV12-00522 JST (ANx)	4/5/2012	Central District - Southern Division

PLAINTIFF	DEFENDANT
Linksmart Wireless Technology, LLC	T-Mobile USA, Inc., et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,779,118	8/17/2004	Linksmart Wireless Technolgy, LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

P1341006.A01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of	: IKUDOME *et al.*	Docket No.: P1341006
U.S. Patent No.	: 6,779,118	Group Art Unit.: 3621
Application No.	: 09/295,966	Confirmation No.: 7800
Filed	: April 21,1999	Examiner: Pierre E. ELISCA
For	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM	

LOSS OF ENTITLEMENT TO SMALL ENTITY STATUS

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

Dear Commissioner:

Pursuant to 37 C.F.R. §1.27(g)(2), Patent Owner hereby informs the PTO that the above-identified patent is no longer eligible for small entity status.

Should the Deciding Official have any questions or comments regarding this matter, the undersigned may be contacted at the below-listed telephone number.

Respectfully submitted,
IKUDOME *et al.*

Abraham Hershkovitz, Reg. No. 45,294
Dinh X. Nguyen, Reg. No. 54,923

August 30, 2011
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314
Tel. (703) 370-4800
Fax. (703) 370-4809
patent@hershkovitz.net

P1341006.A01; AH/DN/cgvr

08/30/2011 10:55

=== COVER PAGE ===

TO: ____________________

FROM: HERSHKOVITZ & ASSOC.

FAX: 7033704809

TEL: 7033704800

COMMENT:

HERSHKOVITZ & ASSOCIATES, LLC
PATENT AGENCY
2845 DUKE STREET, ALEXANDRIA, VA 22314
TEL. 703-370-4800 ~ FACSIMILE 703-370-4809
patent@hershkovitz.net ~ www.hershkovitz.net

Fax

To:	US PTO	From:	Abe Hershkovitz/ Dinh X. Nguyen
Fax:	571-273-6500	Date:	August 30, 2011
Phone:		Pages:	3

Re: U.S. Patent No: **6,779,118**; Docket No: **P1341006**

☑ Urgent ☑ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle

**********************CONFIDENTIALITY NOTE***************************
The documents accompanying this facsimile transmission contain information from the patent firm of Hershkovitz & Associates which is confidential and/or privileged. The information is intended to be for the use of the individual or entity named on this transmission sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this facsimile information is prohibited. If you have received this facsimile in error, please notify us by telephone at (703) 370-4800 immediately so that we can arrange for the retrieval of the original documents at no cost to you.
****

Dear Commissioner:

PLEASE SEE ATTACHED

HERSHKOVITZ & ASSOCIATES, LLC

P1341006.A01; AH/DN/cgvr

HERSHKOVITZ & ASSOCIATES, LLC
PATENT AGENCY
2845 DUKE STREET, ALEXANDRIA, VA 22314
TEL. 703-370-4800 ~ FACSIMILE 703-370-4809
patent@hershkovitz.net ~ www.hershkovitz.net

In re Patent of	: IKUDOME *et al.*	Docket No.: P1341006	
U.S. Patent No.	: 6,779,118	Group Art Unit.: 3621	
Application No.	: 09/295,966	Confirmation No.: 7800	
Filed	: April 21,1999	Examiner: Pierre E. ELISCA	
For	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM		

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

Transmitted herewith is a **Loss of Entitlement to Small Entity Status** in the above-captioned application.

The fee has been calculated as shown below:

Claims After Amendment	No. of Claims Previously Paid	Present Extra	*Small Entity*		*Large Entity*	
			Rate	Fee	Rate	Fee
Total Claims:		0	x 26=	$ 0	x 52=	$
Indep. Claims:		0	x 110=	$ 0	x 220=	$
		Total:		$ 0		$

__ Fee Payment made through EFS.
__ Payment is made herewith by Credit Card (see attached Form PTO-2038).
X The Director is hereby authorized to charge all fees under 37 CFR §§ 1.16 and 1.17 which may be required to maintain pendency of this application to Deposit Account No. 50-2929.
__The Director is hereby authorized to charge all fees under 37 CFR § 1.18 which may be required to complete issuance of this application to Deposit Account No. 50-2929.

August 30, 2011
Date

Abraham Hershkovitz, Reg. No. 45,294
Dinh X. Nguyen, Reg. No. 54,923

P1341006.A01; AH/DN/cgvr

AO 120 (Rev. 3/04)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following ☒ Patents or □ Trademarks:

DOCKET NO. 02:10-cv-00277	DATE FILED 7/28/2010	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF LINKSMART WIRELESS TECHNOLOGY, LLC	DEFENDANT TJ HOSPITALITY LTD, et al.	

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,779,118	8/17/2004	Auriq Systems, Inc.
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5

CONFIRMATION NO. 7800

23363
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

POWER OF ATTORNEY NOTICE

OC000000039039316

Date Mailed: 12/02/2009

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/04/2009.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/deelliott/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/295,966	04/21/1999	KOICHIRO IKUDOME	P1341006

CONFIRMATION NO. 7800

POA ACCEPTANCE LETTER

40401
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

OC000000039039460

Date Mailed: 12/02/2009

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/04/2009.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/deelliott/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Substitute Form PTO/SB/81 (01-09)

POWER OF ATTORNEY
OR
REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY
AND
CHANGE OF CORRESPONDENCE ADDRESS

I hereby revoke all previous powers of attorney given in the patent(s) and/or application(s) identified herein.

[ ] A Power of Attorney is submitted herewith.
OR
[X] *I hereby appoint the practitioners associated with the Customer Number:* **000040401** *for the patent(s)/application(s) identified herein.*
Practitioner Under Customer No.: Abraham Hershkovitz, Reg. No. 45,294

[X] *Please change the correspondence address for the patent(s)/application(s) identified below to:*

CORRESPONDENCE ADDRESS

[X] Customer Number: **000040401** OR [ ] Correspondence address below

Name	**HERSHKOVITZ & ASSOCIATES, LLC**				
Address					
City		*State*		*Zip Code*	
Country	*Email*		*Telephone*	*Facsimile*	
	patent@hershkovitz.net		**703-370-4800**		

I am the:
[ ] Applicant/Inventor
[X] Assignee of record of the entire interest in the patent(s)/application(s) identified herein. See 37 CFR §3.71.
[X] Statement under 37 CFR 3.73(b):
The documentary evidence of a chain of title from the original owner to the Assignee, as recorded in the Assignment records of the Office, is attached hereto, for the patent(s)/application(s) identified herein:

Application Number	*Filing Date*	*Patent Number*	*Issue Date*
90/009,301	**12/17/2008**		
		6,779,118	**08/17/2004**

Substitute Form PTO/SB/81 (01-09) - Page 2

SIGNATURE OF APPLICANT(S) OR ASSIGNEE OF RECORD

The individual(s) whose signature(s) is/are supplied below is/are the Applicant(s)/Inventor(s), or is authorized to act on behalf of Assignee, in the patent(s)/application(s) identified herein.

Printed Name of Signatory (if acting for Assignee)	**Koichiro Ikudome** on behalf of **LINKSMART WIRELESS TECHNOLOGY, LLC.**		
Title (if acting for Assignee)			
Signature		*Date*	10/30/09

Any additional patent(s)/application(s), or additional signature(s) of Applicant(s)/Inventor(s), are submitted on the attached page(s).

Total Additional Pages Attached:__________

United States Patent and Trademark Office

Home | Site Index | Search | Guides | Contacts | eBusiness | eBiz alerts | News | Help

Assignments on the Web > Patent Query

Patent Assignment Abstract of Title

NOTE:Results display only for issued patents and published applications. For pending or abandoned applications please consult USPTO staff.

Total Assignments: 2

Patent #: 6779118 **Issue Dt:** 08/17/2004 **Application #:** 09295966 **Filing Dt:** 04/21/1999

Inventors: KOICHIRO IKUDOME, MOON TAI YEUNG

Title: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Assignment: 1

Reel/Frame: 010062/0040 **Recorded:** 06/29/1999 **Pages:** 3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: IKUDOME, KOICHIRO **Exec Dt:** 06/15/1999

YEUNG, MOON TAI **Exec Dt:** 06/15/1999

Assignee: AURIC WEB SYSTEMS
3452 EAST FOOTHILL BOULEVARD, SUITE 300
PASADENA, CALIFORNIA 91107

Correspondent: CHRISTIE, PARKER & HALE, LLP
WESLEY W. MONROE
P.O. BOX 7068
PASADENA, CA 91109-7068

Assignment: 2

Reel/Frame: 021185/0416 **Recorded:** 07/02/2008 **Pages:** 12

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: AURIO SYSTEMS, INC. **Exec Dt:** 06/25/2008

Assignee: LINKSMART WIRELESS TECHNOLOGY, LLC
3452 E. FOOTHILL BLVD.
SUITE 320
PASADENA, CALIFORNIA 91107

Correspondent: CLARK D. GROSS
12424 WILSHIRE BOULEVARD, STE. 1200
LOS ANGELES, CA 90025

Search Results as of: 10/28/2009 04:32 PM

| .HOME | INDEX| SEARCH | eBUSINESS | CONTACT US | PRIVACY STATEMENT

H&A

HERSHKOVITZ & ASSOCIATES, LLC

2845 DUKE STREET
ALEXANDRIA, VA 22314
Tel: 703-370-4800
Fax: 703-370-4809
patent@hershkovitz.net

Fax

To: US PTO From: Abe Hershkovitz

Fax: 571-273-8300 Date: November 4, 2009

Phone: Pages: 6

Re: U.S. Patent Application No: **09/295,966**; Docket No: **P1341006**

☑ Urgent ☑ For Review □ Please Comment □ Please Reply □ Please Recycle

************************CONFIDENTIALITY NOTE********************

The documents accompanying this facsimile transmission contain information from the patent firm of Hershkovitz & Associates which is confidential and/or privileged. The information is intended to be for the use of the individual or entity named on this transmission sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this facsimile information is prohibited. If you have received this facsimile in error, please notify us by telephone at (703) 370-4800 immediately so that we can arrange for the retrieval of the original documents at no cost to you.
****

Dear Commissioner:

PLEASE SEE ATTACHED

HERSHKOVITZ & ASSOCIATES, LLC

P1341006.F01; AH/dj

H&A

HERSHKOVITZ & ASSOCIATES, LLC
2845 DUKE STREET
ALEXANDRIA, VA 22314
703-370-4800

In re application of	: Ikudome KOICHIRO	Docket No.: P1341006
Application No.	: 09/295,966	Group Art Unit: 3621
Filed	: April 21, 1999	Examiner: Pierre ELISCA
For	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM	

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

Transmitted herewith is a **Revocation of Power of Attorney** and **Patent Assignment Abstract of Title** in the above-captioned application.
The fee has been calculated as shown below:

Claims After Amendment	No. of Claims Previously Paid	Present Extra	Small Entity		Large Entity	
			Rate	Fee	Rate	Fee
Total Claims:			x 26=	$	x 52=	$
Indep. Claims:			x 110=	$	x 220=	$
Issue Fee			755=	$	1,510=	$
Publication Fee			300	$	300	$
Advance Copy				$		$
			Total:	$	Total:	0

__Please charge my Deposit Account No. **50-2929** in the amount of $.

__ A Check in the amount of $ __ to cover the necessary fee is included.

_X_Please charge the above fees to a credit card as authorized by EFS-Web.

_X_ The U.S. Patent and Trademark Office is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. **50-2929**:

_X_ Any additional issue fees required under 37 C.F.R. 1.18.

_X_ Any patent application processing fees under 37 C.F.R. 1.17, including any required extension of time fees in any concurrent or future reply requiring a petition for extension of time for its timely submission (37 CFR 1 .136)(a)(3).

November 3, 2009
Date

Abraham Hershkovitz
Reg. No. 45,294

P1341006.A01: AH/dj

=== COVER PAGE ===

TO: ____________________

FROM: HERSHKOVITZ & ASSOC.

FAX: 7033704809

TEL: 7033704800

COMMENT:

AO 120 (Rev. 3/04)

TO: **Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following ☑ Patents or □ Trademarks:

DOCKET NO. 2:08-cv-304	DATE FILED 8/4/2008	U.S. DISTRICT COURT Eastern District of Texas	
PLAINTIFF LINKSMART WIRELESS TECHNOLOGY, LLC		DEFENDANT CISCO SYSTEMS, INC., et al	

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,779,118	8/17/2004	Linksmart Wireless Technology, LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

23363 7590 03/16/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO, on the date indicated below.

Susanne C. Garcia (Depositor's name)
Susanne C. Garcia (Signature)
June 15, 2004 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

TITLE OF INVENTION: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	06/16/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
ELISCA, PIERRE E	3621	713-201000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 **Christie, Parker &**
2 **Hale, LLP**
3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Auriq Systems, Inc.	**Pasadena, California**

Please check the appropriate assignee category or categories (will not be printed on the patent); □ individual ☒ corporation or other private group entity □ government

4a. The following fee(s) are enclosed:

☒ Issue Fee

□ Publication Fee

☒ Advance Order - # of Copies 10

4b. Payment of Fee(s):

☒ A check in the amount of the fee(s) is enclosed.

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

☒ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 03-1728 (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) Reg No. 39,778 (Date) 06/15/2004

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

06/22/2004 AWONDAF2 00000014 09295966

01 FC:2501	665.00 OP
02 FC:8001	30.00 OP

TRANSMIT THIS FORM WITH FEE(S)

Rep

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

23363 7590 03/16/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO, on the date indicated below.

Susanne C. Garcia (Depositor's name)
Susanne C. Garcia (Signature)
June 15, 2004 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

TITLE OF INVENTION: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	06/16/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
ELISCA, PIERRE E	3621	713-201000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Christie, Parker &
2 Hale, LLP
3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE
Auriq Systems, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Pasadena, California

Please check the appropriate assignee category or categories (will not be printed on the patent); □ individual ☒ corporation or other private group entity □ government

4a. The following fee(s) are enclosed:

☒ Issue Fee
□ Publication Fee
☒ Advance Order - # of Copies 10

4b. Payment of Fee(s):

☒ A check in the amount of the fee(s) is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 03-1728 (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) Reg No. 39,778 (Date) 06/15/2004

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

06/22/2004 AWONDAF2 00000014 09295966

01 FC:2501	665.00 OP
02 FC:8001	30.00 OP

TRANSMIT THIS FORM WITH FEE(S)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 05/06/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 05/06/2004

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

PTO-90C (Rev. 10/03)

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.

EXAMINER

ART UNIT	PAPER
	20040326

DATE MAILED:

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

Commissioner for Patents

The IDS filed on 3/26/2004 has been considered. A signed copy of the 1449 form is enclodsed.

PTO-90C (Rev.04-03)

PRIMARY PATENT EXAMINER

FORM PTO/SB/08A/B (10-01) Substitute for PTO-1449A/B **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (use as many sheets as necessary)	**Attorney Docket Number**	**34503/WWM/A522**
	Application Number	09/295,966
	Filing Date	April 21, 1999
	Applicant(s)	Koichiro Ikudome, et al.
	Group Art Unit	3621
	Examiner Name	Pierre E. Elisca

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	DOCUMENT NUMBER Number - Kind Code[2] (If Known)	PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE
P.E		6,233,686	05-15-2001	Dutta

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (If Known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6] (✓)
P.E		WO98/03927	01-29-1998	O'Neil	
P.E		CA2,226,814	03-25-2003	Dutta	

OTHER DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

MAC PAS538044.1-*-11/21/03 5:36 PM

EXAMINER SIGNATURE		DATE CONSIDERED	4/28/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.pto.gov or MPEP 901.4. [3]Enter Office that issued the document, by the two-letter code (WIPO standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English Language Translation is attached.

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

WWM/mac

RFR

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 05/06/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER
ELISCA, PIERRE E

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/06/2004

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

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

24

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.

EXAMINER

ART UNIT	PAPER
	20040326

DATE MAILED:

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

Commissioner for Patents

The IDS filed on 3/26/2004 has been considered. A signed copy of the 1449 form is enclodsed.

PTO-90C (Rev.04-03)

PRIMARY PATENT EXAMINER

33

FORM PTO/SB/08A/B (10-01) Substitute for PTO-1449A/B INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)	Attorney Docket Number	34503/WWM/A522
	Application Number	09/295,966
	Filing Date	April 21, 1999
	Applicant(s)	Koichiro Ikudome, et al.
	Group Art Unit	3621
	Examiner Name	Pierre E. Elisca

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	DOCUMENT NUMBER Number - Kind Code[2] (If Known)	PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE
P.E		6,233,686	05-15-2001	Dutta

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (If Known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6] (✓)
P.E		WO98/03927	01-29-1998	O'Neil	
P.E		CA2,226,814	03-25-2003	Dutta	

OTHER DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

MAC PAS538044.1-*-11/21/03 5:36 PM

EXAMINER SIGNATURE		DATE CONSIDERED	4/28/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.pto.gov or MPEP 901.4. [3]Enter Office that issued the document, by the two-letter code (WIPO standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English Language Translation is attached.

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

WWM/mac

facsimile
TRANSMITTAL

Date:	March 26, 2004
No. of Pages:	8 (including this cover sheet)
Fax No.:	(703) 872-9306

PLEASE DELIVER THE FOLLOWING PAGES IMMEDIATELY TO:

Name:	Commissioner of Patents
Art Unit:	3621
Examiner:	Pierre E. Elisca
Phone:	(703) 305-3987
From:	Wesley W. Monroe Reg No. 39,778
Re:	Application No. 09/295,966 Filed April 21, 1999 Entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
File:	34503/WWM/A522

I HEREBY CERTIFY THAT THIS ***LETTER REQUESTING ACKNOWLEDGEMENT OF REFERENCES AS ASSOCIATED*** PAPER ARE BEING FACSIMILE TRANSMITTED TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **March 26,2004.**

Marti Carrillo

Marti Carrillo

*Correspondence: IDS

For Office Services Use Only
Return Fax to Marti Carrillo

Christie, Parker & Hale, LLP
350 West Colorado Boulevard
Post Office Box 7068
Pasadena, CA 91109-7068
626-795-9900
Fax: 626-577-8800

confidential

The information in this transmission is confidential and is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone collect, and return the original message to us at the above address via U.S. mail. We will reimburse you for postage. Thank you.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on March 26, 2004.

Marti Carrillo
Marti Carrillo

Applicant	: Koichiro Ikudome, et al.
Application No.	: 09/295,966
Filed	: April 21, 1999
Title	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Date of Notice of Allowance	: March 16, 2004
Grp./Div.	: 3621
Examiner	: Pierre E. Elisca
Docket No.	: 34503/WWM/A522

LETTER REQUESTING ACKNOWLEDGMENT OF REFERENCES

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

PostOffice Box 7068
Pasadena, CA 91109-7068
March 26, 2004

Commissioner:

The enclosed copy of the PTO/SB/08A/B was submitted by the Applicant on November 21, 2003. None of the references listed on the form were initialed by the Examiner. Also enclosed are copies of the return postcard and canceled check which acknowledge receipt of the Information Disclosure Statement, PTO/SB/08A/B and fee on November 24, 2003.

It is respectfully requested that the Examiner return the form to the Applicant after initializing the references, thereby indicating that they were expressly considered by the Examiner.

Application No. 09/295,966

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ________________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mac
Enclosures

MAC PAS556988.1-*-03/26/04 10:23 AM

PLEASE SIGN AND RETURN TO ACKNOWLEDGE RECEIPT

Title User Specific Automatic Data Redirection System

Client ID A522
Case No 34503
Atty/Sec WHM/mac
Date Mailed 11/21/03
Date Due n/a
Cert of Mailing
Express Mail No.

Ser/Pat/Reg No: 09/295,966
Filed/Issued : 04/21/99

____ Assigned Enclosed (List Assignee)

Checked by:

DOCUMENT TITLE: (List enclosures) Information Disclosure Statement, Form PTO-SB/08A&B
$180

ACKNOWLEDGE HERE

REV 11/93 FORM P2

X PAT ____ COP ____ MARK ____ DBA

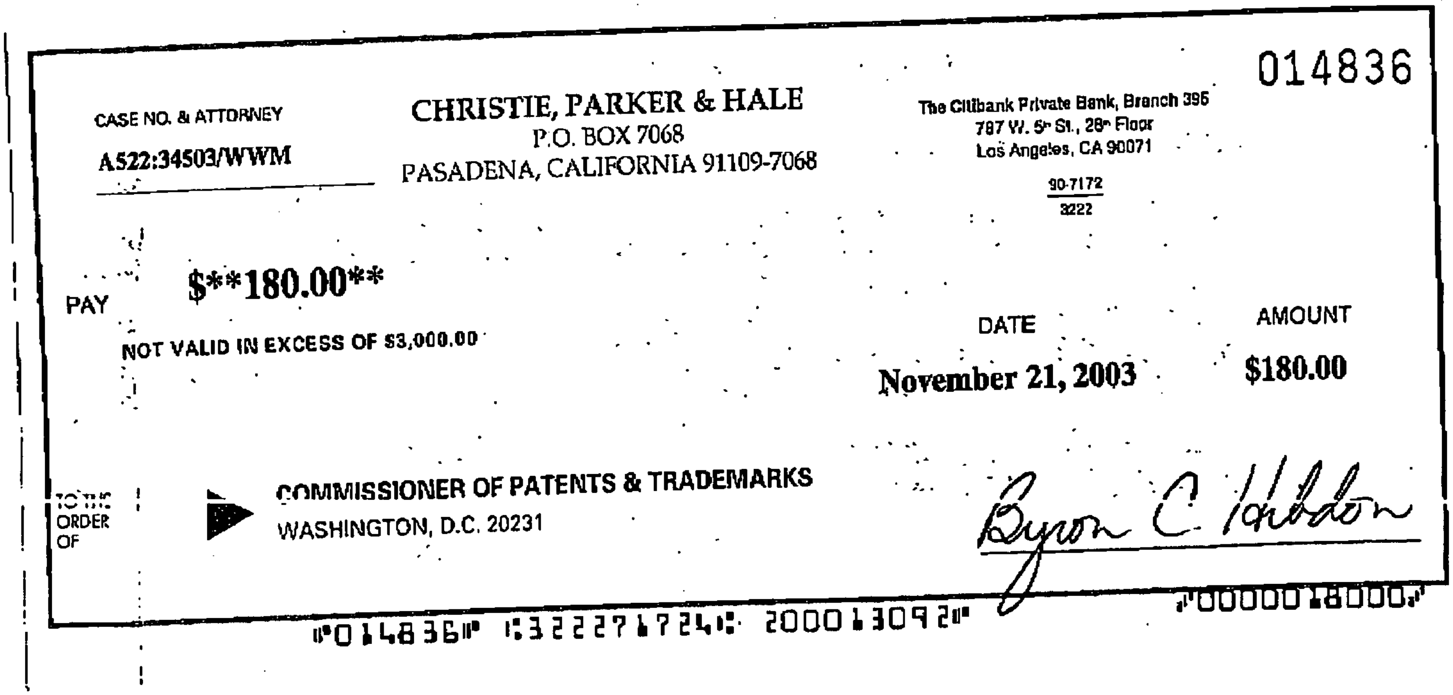
NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY CARD
FIRST CLASS PERMIT NO. 3370 PASADENA, CALIFORNIA

POSTAGE WILL BE PAID BY ADDRESSEE

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

3060 12144



014836

CASE NO. & ATTORNEY
A522:34503/WWM

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

The Citibank Private Bank, Branch 395
787 W. 5th St., 28th Floor
Los Angeles, CA 90071

90-7172
3222

PAY $**180.00**

NOT VALID IN EXCESS OF $3,000.00

DATE November 21, 2003

AMOUNT $180.00

TO THE ORDER OF
COMMISSIONER OF PATENTS & TRADEMARKS
WASHINGTON, D.C. 20231

Byron C Hubbon

⑈014836⑈ ⑆322271724⑆ 20001309⑈ ⑈0000018000⑈

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 21, 2003.

Marti Carrillo

Applicant	: Koichiro Ikudome, et al.
Application No.	: 09/295,966
Filed	: April 21, 1999
Title	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	: 3621
Examiner	: Pierre E. Elisca
Docket No.	: 34503/WWM/A522

INFORMATION DISCLOSURE STATEMENT WITH FEE UNDER 37 CFR §§ 1.97(d) AND 1.17(p)

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

PostOffice Box 7068
Pasadena, CA 91109-7068
November 21, 2003

Commissioner:

In compliance with the duty of disclosure under 37 CFR §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the Manual of Patent Examining Procedure §§ 609 and 707.05(b), enclosed is FORM PTO/SB/08A/B listing the references that are known to applicant. Copies of each of the listed references are enclosed.

It is respectfully requested that the listed references be considered in the examination of this application and identified on the list of references cited on the patent issuing for this application. Applicant also requests that an initialed copy of FORM PTO/SB/08A/B be entered in the application file and returned to applicant with the next communication from the Office in accordance with MPEP § 609.

Applicant's undersigned attorney hereby certifies, in accordance with 37 CFR § 1.97(e)(2), that no item of information contained in the information disclosure statement was

Application No. 09/295,966

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

Enclosed is the processing fee of $180 as required by 37 CFR § 1.17(p). The Commissioner is hereby authorized to charge any fees which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any Deposit Account transaction. **A copy of this paper is enclosed.**

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mac
Enclosures: Check $180
Copy of IDS
Form PTO/SB/08A/B, w/references
MAC PAS538041.1-*-11/21/03 5:28 PM

FORM PTO/SB/08A/B (10-01) Substitute for PTO-1449A/B **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** (use as many sheets as necessary)	Attorney Docket Number	34503/WWM/A522
	Application Number	09/295,966
	Filing Date	April 21, 1999
	Applicant(s)	Koichiro Ikudome, et al.
	Group Art Unit	3621
	Examiner Name	Pierre E. Elisca

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	DOCUMENT NUMBER Number - Kind Code[2] (If Known)	PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE
		6,233,686	05-15-2001	Dutta

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (If Known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6] (✓)
		WO98/03927	01-29-1998	O'Neil	
		CA2,226,814	03-25-2003	Dutta	

OTHER DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial), symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

MAC PAS538044.1-*-11/21/03 5:36 PM

EXAMINER SIGNATURE		DATE CONSIDERED	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.pto.gov or MPEP 901.4. [3]Enter Office that issued the document, by the two-letter code (WIPO standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English Language Translation is attached.

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

WWM/mac

BB

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on March 26, 2004.

Marti Carrillo

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Date of Notice of Allowance	:	March 16, 2004
Grp./Div.	:	3621
Examiner	:	Pierre E. Elisca
Docket No.	:	34503/WWM/A522

LETTER REQUESTING ACKNOWLEDGMENT OF REFERENCES

PostOffice Box 7068
Pasadena, CA 91109-7068
March 26, 2004

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

Commissioner:

The enclosed copy of the PTO/SB/08A/B was submitted by the Applicant on November 21, 2003. None of the references listed on the form were initialed by the Examiner. Also enclosed are copies of the return postcard and canceled check which acknowledge receipt of the Information Disclosure Statement, PTO/SB/08A/B and fee on November 24, 2003.

It is respectfully requested that the Examiner return the form to the Applicant after initializing the references, thereby indicating that they were expressly considered by the Examiner.

Application No. 09/295,966

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mac
Enclosures

MAC PAS556988.1-*-03/26/04 10:23 AM

PLEASE SIGN AND RETURN TO ACKNOWLEDGE RECEIPT

Title User Specific Automatic Data Redirection System

Ser/Pat/Reg No: 09/295,966
Filed/Issued : 04/21/99

____ Assigned Enclosed (List Assignee)

Client ID A522
Case No 34503
Atty/Sec WHM/mac
Date Mailed 11/21/03
Date Due n/a
Cert of Mailing ____
Express Mail No. ____

Checked by:

DOCUMENT TITLE: Information Disclosure
(List enclosures) Statement, Form PTO-SB/08A&B
$180

ACKNOWLEDGE HERE

X PAT ____ COP ____ MARK ____ DBA

REV 11/00 FORM P2

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY CARD
FIRST CLASS PERMIT NO. 3370 PASADENA, CALIFORNIA

POSTAGE WILL BE PAID BY ADDRESSEE

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

5060 12144

014836

CASE NO. & ATTORNEY
A522:34503/WWM

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

The Citibank Private Bank, Branch 396
787 W. 5th St., 29th Floor
Los Angeles, CA 90071

90-7172
3222

PAY $**180.00**

NOT VALID IN EXCESS OF $3,000.00

DATE	AMOUNT
November 21, 2003	$180.00

TO THE ORDER OF COMMISSIONER OF PATENTS & TRADEMARKS
WASHINGTON, D.C. 20231

Byron C Hobbson

[redacted]

facsimile TRANSMITTAL

Date:	March 26, 2004
No. of Pages:	8 (including this cover sheet)
Fax No.:	(703) 872-9306

PLEASE DELIVER THE FOLLOWING PAGES IMMEDIATELY TO:

Name:	Commissioner of Patents
Art Unit:	3621
Examiner:	Pierre E. Elisca
Phone:	(703) 305-3987
From:	Wesley W. Monroe Reg No. 39,778
Re:	Application No. 09/295,966 Filed April 21, 1999 Entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
File:	34503/WWM/A522

I HEREBY CERTIFY THAT THIS *LETTER REQUESTING ACKNOWLEDGEMENT OF REFERENCES AS ASSOCIATED* PAPER ARE BEING FACSIMILE TRANSMITTED TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON March 26, 2004.

Marti Carrillo

Marti Carrillo

*Correspondence: IDS

Christie, Parker & Hale, LLP
350 West Colorado Boulevard
Post Office Box 7068
Pasadena, CA 91109-7068
626-795-9900
Fax: 626-577-8800

For Office Services Use Only
Return Fax to Marti Carrillo

confidential

The information in this transmission is confidential and is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone collect, and return the original message to us at the above address via U.S. mail. We will reimburse you for postage. Thank you.

BB

X 22

PATENT

Dup Copy

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 21, 2003.

Mari Carrillo

Mari Carrillo

Applicant	: Koichiro Ikudome, et al.
Application No.	: 09/295,966
Filed	: April 21, 1999
Title	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	: 3621
Examiner	: Pierre E. Elisca
Docket No.	: 34503/WWM/A522

INFORMATION DISCLOSURE STATEMENT WITH FEE UNDER 37 CFR §§ 1.97(d) AND 1.17(p)

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

PostOffice Box 7068
Pasadena, CA 91109-7068
November 21, 2003

Commissioner:

In compliance with the duty of disclosure under 37 CFR §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the Manual of Patent Examining Procedure §§ 609 and 707.05(b), enclosed is FORM PTO/SB/08A/B listing the references that are known to applicant. Copies of each of the listed references are enclosed.

It is respectfully requested that the listed references be considered in the examination of this application and identified on the list of references cited on the patent issuing for this application. Applicant also requests that an initialed copy of FORM PTO/SB/08A/B be entered in the application file and returned to applicant with the next communication from the Office in accordance with MPEP § 609.

Applicant's undersigned attorney hereby certifies, in accordance with 37 CFR § 1.97(e)(2), that no item of information contained in the information disclosure statement was

Application No. 09/295,966

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

Enclosed is the processing fee of $180 as required by 37 CFR § 1.17(p). The Commissioner is hereby authorized to charge any fees which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any Deposit Account transaction. **A copy of this paper is enclosed.**

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mac
Enclosures: Check $180
Copy of IDS
Form PTO/SB/08A/B, w/references
MAC PAS538041.1-*-11/21/03 5:28 PM

FORM PTO/SB/08A/B (10-01) Substitute for PTO-1449A/B INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)	Attorney Docket Number	34503/WWM/A522
	Application Number	09/295,966
	Filing Date	April 21, 1999
	Applicant(s)	Koichiro Ikudome, et al.
	Group Art Unit	3621
	Examiner Name	Pierre E. Elisca

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	DOCUMENT NUMBER Number - Kind Code[2] (If Known)	PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE
P.E		6,233,686	05-15-2001	Dutta

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (If Known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6] (✓)
P.E		WO98/03927	01-29-1998	O'Neil	
P.E		CA2,226,814	03-25-2003	Dutta	

OTHER DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

MAC PAS538044.1-*-11/21/03 5:36 PM

EXAMINER SIGNATURE		DATE CONSIDERED	6/10/2004

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.pto.gov or MPEP 901.4. [3]Enter Office that issued the document, by the two-letter code (WIPO standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English Language Translation is attached.

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

WWM/mac

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

23363 7590 03/16/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 03/16/2004

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

TITLE OF INVENTION: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	06/16/2004

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status is changed, pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above and notify the United States Patent and Trademark Office of the change in status, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check the box below and enclose the PUBLICATION FEE and 1/2 the ISSUE FEE shown above.

□ Applicant claims SMALL ENTITY status.
See 37 CFR 1.27.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 11/03) Approved for use through 04/30/2004.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

23363 7590 03/16/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

TITLE OF INVENTION: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	06/16/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
ELISCA, PIERRE E	3621	713-201000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________

2____________________

3____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent); □ individual □ corporation or other private group entity □ government

4a. The following fee(s) are enclosed:

□ Issue Fee

□ Publication Fee

□ Advance Order - # of Copies ________________

4b. Payment of Fee(s):

□ A check in the amount of the fee(s) is enclosed.

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

□ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number ________________ (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) (Date)

NOTE; The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMIT THIS FORM WITH FEE(S)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 03/16/2004

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/16/2004

Determination of Patent Term Extension under 35 U.S.C. 154 (b)

(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) system (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (703) 305-1383. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

Notice of Allowability	**Application No.** 09/295,966	**Applicant(s)** IKUDOME ET AL
	Examiner Pierre E. Elisca	**Art Unit** 3621

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/30/2003*.

2. ☒ The allowed claim(s) is/are *1-18 and 20-28*.

3. □ The drawings filed on _____ are accepted by the Examiner.

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment ✓
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

PRIMARY PATENT EXAMINER

23

REASONS FOR ALLOWANCE

1. This is an Examiner's Statement of Reasons for Allowance. The closest prior art (Grube et al. (U.S. pat. No. 6,157,829) discloses a central service agent that assigns a temporary alias ID and a permanent ID that is communicated, on a temporary basis, to a specific calling unit.

However, Grube singularly or in combination fails to anticipate or render obvious the recited feature:

As per claims 1 and 8" wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set".

As per claim 15 " wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address".

As per claim 26 " modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server, and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the

B

redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server".

Examiner's Amendment

2. Please cancel claims 19 and 29 without prejudice.

Please amend claims 15 and 26 as follow:

Claim 15, line 5, after " public network ; " delete " and ".

Claim 15, line 7, after "address" delete " . " and add -- ; --.

Claim 15, line 7, after "; " and add -- and wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access~~.~~ .

B1

Claim 26, line 6, after " redirection server " delete " . " and add -- ; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server~~.~~ .

B2

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pierre E. Elisca whose telephone number is 703 305-3987. The examiner can normally be reached on 6:30 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703 305-9769. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pierre Eddy Elisca

Primary Patent Examiner

February 19, 2004

Notice of References Cited

Application/Control No. 09/295,966		Applicant(s)/Patent Under Reexamination IKUDOME ET AL.	
Examiner Pierre E. Elisca		Art Unit 2785	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
✗	A	US-6,157,829	12-2000	Grube et al.	455/414.1
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

3621

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 21, 2003.

Marti Carrillo
Marti Carrillo

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre E. Elisca
Docket No.	:	34503/WWM/A522

INFORMATION DISCLOSURE STATEMENT WITH FEE UNDER 37 CFR §§ 1.97(d) AND 1.17(p)

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

PostOffice Box 7068
Pasadena, CA 91109-7068
November 21, 2003

Commissioner:

In compliance with the duty of disclosure under 37 CFR §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the Manual of Patent Examining Procedure §§ 609 and 707.05(b), enclosed is FORM PTO/SB/08A/B listing the references that are known to applicant. Copies of each of the listed references are enclosed.

It is respectfully requested that the listed references be considered in the examination of this application and identified on the list of references cited on the patent issuing for this application. Applicant also requests that an initialed copy of FORM PTO/SB/08A/B be entered in the application file and returned to applicant with the next communication from the Office in accordance with MPEP § 609.

Applicant's undersigned attorney hereby certifies, in accordance with 37 CFR § 1.97(e)(2), that no item of information contained in the information disclosure statement was

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

Enclosed is the processing fee of $180 as required by 37 CFR § 1.17(p). The Commissioner is hereby authorized to charge any fees which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any Deposit Account transaction. **A copy of this paper is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mac

Enclosures: Check $180
Copy of IDS
Form PTO/SB/08A/B, w/references

MAC PAS538041.1-*-11/21/03 5:28 PM

FORM PTO/SB/08A/B (10-01)
Substitute for PTO-1449A/B

INFORMATION DISCLOSURE

STATEMENT BY APPLICANT

(use as many sheets as necessary)

Attorney Docket Number	**34503/WWM/A522**
Application Number	09/295,966
Filing Date	April 21, 1999
Applicant(s)	Koichiro Ikudome, et al.
Group Art Unit	3621
Examiner Name	Pierre E. Elisca

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	DOCUMENT NUMBER Number - Kind Code[2] (If Known)	PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE
P.E		6,233,686	05-15-2001	Dutta

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (If Known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6] (✓)
P.E		WO98/03927 ✓	01-29-1998	O'Neil	
P.E		CA2,226,814 ✓	03-25-2003	Dutta	

OTHER DOCUMENTS

EXAMINER INITIALS	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

MAC PAS538044.1-*-11/21/03 5:36 PM

EXAMINER SIGNATURE		DATE CONSIDERED	4/13/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.pto.gov or MPEP 901.4. [3]Enter Office that issued the document, by the two-letter code (WIPO standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English Language Translation is attached.

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

WWM/mac

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2226814 C 2003/03/25

(11)(21) 2 226 814

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 1998/01/12
(41) Mise à la disp. pub./Open to Public Insp.: 1998/07/17
(45) Date de délivrance/Issue Date: 2003/03/25
(30) Priorité/Priority: 1997/01/17 (08/785,501) US

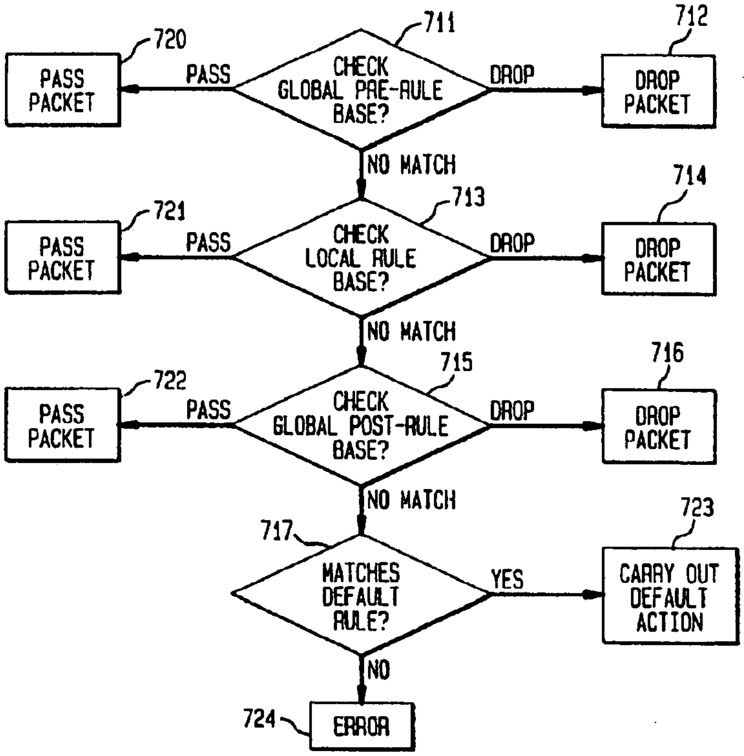
(51) Cl.Int.^{6}/Int.Cl.^{6} H04L 29/02, H04L 12/56

(72) Inventeurs/Inventors:
DUTTA, PARTHA P., US;
ZENCHELSKY, DANIEL N., US;
LONDON, THOMAS B., US;
VRSALOVIC, DALIBOR F., US;
SIIL, KARL A., US

(73) Propriétaire/Owner:
AT&T CORP., US

(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : SYSTEME ET METHODE DONNANT UN CONTROLE D'ACCES AU NIVEAU HOMOLOGUE SUR LES RESEAUX
(54) Title: SYSTEM AND METHOD FOR PROVIDING PEER LEVEL ACCESS CONTROL ON A NETWORK



(57) Abrégé/Abstract:

A system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier. The local rule base of a peer is dynamically loaded into a filter when the peer is authenticated, and ejected when the peer is loses authentication. The local rule base is efficiently searched through the use of hash tables wherein a hashed peer network address serves as a pointer the peer's local rules. Each rule comprises a 5-tuple and an action. The action of a rule is carried out on a packet when the 5-tuple of the rule corresponds to the 5-tuple of the packet.

SYSTEM AND METHOD FOR PROVIDING PEER LEVEL ACCESS CONTROL ON A NETWORK

Abstract of the Invention

A system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier. The local rule base of a peer is dynamically loaded into a filter when the peer is authenticated, and ejected when the peer is loses authentication. The local rule base is efficiently searched through the use of hash tables wherein a hashed peer network address serves as a pointer the peer's local rules. Each rule comprises a 5-tuple and an action. The action of a rule is carried out on a packet when the 5-tuple of the rule corresponds to the 5-tuple of the packet.

SYSTEM AND METHOD FOR PROVIDING PEER LEVEL ACCESS CONTROL ON A NETWORK

Field of the Invention

This invention relates to information systems security, in particular to providing access control between one set of automated information systems and another.

Background of the Invention

Known methods for implementing access control for a specific computer on a network are cumbersome and inflexible because access rules must be coded and entered by hand by a system administrator. This is impractical for networks whose members change frequently, or whose members' security needs change frequently.

Effective information systems security prevents the unauthorized disclosure, modification or execution of an automated information system's (AIS) data and processes. As used here, the term AIS refers to a computer, network of computers, internetwork of computers, or any subset thereof. The term "data" refers to any information resident on an AIS, including files and programs. The term "processes" refers to programs in any stage of execution on an AIS.

A "host" is a computer with an assigned network address, e.g., an Internet Protocol (IP) address. A "user" is a computer that does not have a fixed, assigned network address. To obtain connectivity to the Internet, for example, a user must commonly obtain a temporary IP address from a host with a pool of such addresses. Such a temporary IP address is retained by the user only for the duration of a single session of connectivity with the Internet.

Information flows in certain networks in packets. A "packet" is a quantum of information that that has a header containing a source and a destination address. An example of a packet is an IP packet. Packets such as IP packets have a network protocol identifier ("protocol") as a part of packet header. The protocol identifies the version number of the protocol used to route the packet. An example of a network protocol identifier is the IP protocol field in an IP packet header.

Packets on a network are directed to and from ports. A "port" is a logical address within a computer through which a process executing on the computer communicates with other executing processes. These other processes may reside on the same computer, or on other networked computers.

Information systems security is implemented by means of a security policy, which comprises rules directed towards regulating the flow of information in an AIS. The rules of a security policy are embodied in a "rule base," a set of rules that specify whether a packet should be passed to the intended recipient or dropped based upon the packet's identifier. A packet identifier is data generally carried in the packet header that serves to identify the packet. An example of a packet identifier is a circuit number, which occurs in the headers of packets flowing in connection-oriented (i.e., circuit-switched) packet switched networks. Another example of a packet identifier is a packet 5-tuple, which is the packet's source and destination address, source and destination port, and protocol. Packets with 5-tuples flow in connectionless packet switched networks.

A rule base may be global or local. A global rule base is a uniform set of rules ("global rules") that apply to a group of users, hosts, or both. A local rule base is a set of rules ("local rules") that apply to a single user with a temporary network address or a host. A single user with a temporary network address or a host that has its own rule base is called a "peer."

Another means for implementing security policy is to restrict access to a network to a predetermined set of users and hosts. When a user or host requests access, its identity must be established and verified before access is granted. This process implicates two steps: identification and authentication.

FIG 1 shows one method of identification and authentication in the form of a flow chart with each step designated by a reference numeral. A first step requires a source of information to identify itself by name by supplying a string of data called a user id 10. To prevent an imposter from obtaining the privileges associated with a given user id, the user behind the user id is verified by requiring it to provide a password 11 that is normally kept confidential. Such verification is called "authentication." The AIS checks the combination of source id and password against a list of valid users, 12. When the AIS recognizes a valid user id and corresponding password, a user or host is said to have been identified and authenticated 14. Otherwise, the request for access is denied 13. Hereinafter, a source that has been identified and authenticated will be said to have been "authenticated" for purposes of brevity.

A security policy rule base is implemented on a network using a device called a filter comprising hardware and software. The rule base is loaded into the filter, which receives packets en route (between their source and destination) and checks the identifier of each packet against the identifier contained in each rule of the rule base for a match, i.e., if the packet corresponds to the rule. A packet corresponds to a rule if the rule applies to the packet. Hence, a rule that is meant to apply to packets with a circuit number of 3254, for example, "corresponds" to all packets with a packet identifier that indicates circuit number 3254. If the network packet identifier corresponds to a rule identifier, the filter carries out the PASS or DROP action prescribed by the rule on the packet. If the PASS action is carried out, the packet is allowed to pass through the filter. If the DROP action is carried out, the packet is eliminated.

A filter is often combined with other hardware and software that helps manage the flow of information through the filter. The combination of hardware and software that carries out and supports packet filtering is called a firewall. A firewall is often positioned between a first network that "owns" the firewall and a second network. The purpose of the firewall is to regulate the flow of information into and out of the first network from the second network by implementing the rule base belonging to the first network for all such information.

A typical application of a firewall is shown in FIG 2. A corporate network 20 may wish to provide access to Internet hosts 21 to its subscribers, but may wish to limit the access that the Internet hosts 21 have to the corporate network 20, which may contain trade secrets and proprietary information. The corporate network 20 would develop a security policy implemented by a firewall 22 placed at the interface between the corporate network 20 and the Internet hosts 21. The firewall 22 comprises a filter 23 that would PASS or DROP packets from Internet hosts 21 to corporate network subscribers 20 and vice versa based upon the packets' source and destination addresses. The firewall is said to belong to the corporate network, and enforces rules that "protect" hosts within the corporate network that have IP addresses. Such hosts are said to be "behind" the corporate network firewall.

An example of a rule base for corporate network 20 having hosts A 24, B 25 and C 26, connected through a firewall 22 to the Internet having hosts G 27, H 28 and I 29 is as follows:

SOURCE	DESTINATION	VERSION	ACTION
Address, Port	Address, Port		
A,21	G,32	4	PASS
A,22	H,19	3	DROP
G,11	A,64	4	DROP
C,9	I,23	4	PASS

Every rule base must also have a default action for transactions that are not explicitly specified in the rule base, which is usually the DROP action. Thus, packets from system A,21 to system G,33 will be dropped because the above rule base does not expressly include a rule for such a transfer.

A typical architecture for providing users access to the Internet is shown in FIG 3. Users 31 and 32 do not have fixed IP addresses. Rather, a user is assigned temporary IP addresses by an Internet Service Provider (ISP) Point of Presence (POP) 33 from a pool of such addresses kept by the POP 33 for this purpose. A POP comprises at least one host (not shown). When a user 31 terminates his session of access to the Internet 35, the IP address is returned to the POP 33. Thus, over successive access sessions, a user 31 is likely to have several different IP addresses.

Known filters are not well suited to providing appropriate access control for networks such as a POP. This is because a known filter is only able to load and store rules through the intervention of a system administrator, a slow and cumbersome process. Indeed, the system administrator generally must hand-code rules in a format specific to the filter platform. With known filters, it is impractical to implement the access rules of a specific user (known as the user's "local rules") who is accessing and leaving the network with changing network addresses.

This problem is illustrated in FIGs 5a and 5b. FIG 5a shows a first session where a first user 51 has requested Internet access and been authenticated by a POP and been assigned IP address B from the POP IP address pool 52. Likewise, a second user 53 has been authenticated and been assigned IP address E from the pool 52. A rule base 53 is loaded into a filter to regulate the flow of information between users 51 and 53 and the hosts P, U, V and W on the Internet. The rule base shown in FIGs 5a and 5b show only the source and destination addresses for each rule, and omit source and destination ports and protocol for simplicity.

Both users stop accessing the Internet and then later request access again and are authenticated for a second session, shown in FIG 5b. This time, the first user 51 is assigned IP address E from the pool 52, and the second user is assigned IP address A. With the newly assigned network addresses, the rule base in the filter is now out of date, containing no rules for the second user, and the wrong rules for the first user, which has been assigned the IP address assigned to the second user during the first session. Even if both users had fortuitously been reassigned the same IP addresses for their second sessions, if either user's security needs had changed between sessions, a new rule base would have had to be loaded into the filter. As discussed above, loading rules into known filters is tedious. Loading and dropping such rules with the frequency that users access and leave a POP is impractical for known filters.

The inflexibility of known filters often necessitates the implementation of rule bases that are too broad for a given application. Without the possibility of easy updates, it is simpler to mandate global rules that apply to all AIS behind a filter rather than to load rules that apply to specific hosts. In such a case, all AIS behind the filter must conform to the most restrictive security requirements of any such AIS, resulting in overly restrictive filtering.

The shortcomings of known filters are illustrated by some of the architectures presently used to provide information systems security for a POP. The architecture shown in FIG 3 provides a minimal level of security through an authentication system 34 which limits access to a predetermined list of authenticated users. But the list of users must generally be entered by hand by the system administrator, and so cannot be easily changed. Further, once access is granted, the access is unlimited. Information may flow to and from users 31 and 32 from the Internet 35 without regulation, providing no security past the initial authentication process. This exposes users 31 and 32 to the risk of hacker attacks from users and hosts on the Internet, possibly resulting in the theft or unauthorized manipulation of user data.

The architecture illustrated in FIG 4 shows another known solution to providing information systems security on a POP. The known filter 46 implements a security policy for packets flowing between the Internet 45 and hosts 41 and 42. However, the rule base in the filter 46 must still be formulated and loaded by the system administrator. Further, the network addresses of the users 31 and 32 are likely to change on a session by session basis. This means that it is only practical to load general, "global" rules into the filter that are valid for all of the users. Thus, for example, if user A does not wish to receive packets from a particular host on the Internet, the filter rule base must drop all such packets, thus cutting off user B from receiving packets from that Internet host as well. In this way, the global rule base necessitated by the limited capabilities of known filtering systems is almost always too broad. Another disadvantage is that it is difficult to change the filter rule base to accommodate changing security needs of either user 41 or 42.

Another architecture that provides security on for each peer is shown in FIG. 6. Here, filters 66 and 67 are placed between users 61 and 62, respectively, and the POP. Requiring every user to have its own filter is an expensive solution that is impractical to implement.

What is needed is a filtering system and method that accurately and efficiently implements local rule bases on a network whose configuration and security needs are constantly changing. Such an invention would provide peer-level security flexibly and inexpensively, with little intervention required from a system administrator.

Summary of the Invention

In accordance with one aspect of the present invention, there is provided a filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises: a. means for accessing a peer's local rule base; b.

means for detecting when the peer is authenticated; c. means for loading a rule from the peer's local rule base at the filter when the authentication of the peer is detected; d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and e. a global pre-rule base having a global pre-rule, wherein upon receiving the packet, said filter first searches said global pre-rule base for a rule that corresponds to the packet and carries out the action of the corresponding global pre-rule on the packet, and wherein if no corresponding global pre-rule is identified, the filter searches the local rule base for a rule that corresponds to the packet and carries out the action of the corresponding local rule on the packet.

In accordance with another aspect of the present invention, there is provided a filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises: a. means for accessing a peer's local rule base; b. means for detecting when the peer is authenticated; c. means for loading a rule from the peer's local rule base at the filter when the authentication of the peer is detected; d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and e. a global post-rule base, wherein the global post-rule base is searched for a rule that corresponds to the packet, and the action of a global post-rule is carried out if it corresponds to the packet only if no corresponding rule in said global pre-rule base and no corresponding rule in said local rule base are identified.

In accordance with yet another aspect of the present invention, there is provided a filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises: a. means for accessing a peer's local rule base; b. means for detecting when the peer is authenticated; c. means for loading a rule from the peer’s local rule base at the filter when the authentication of the peer is detected; d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and e. a default rule, wherein if no corresponding pre-global rule and no corresponding local rule and no corresponding post-global rule are identified, said filter carries out the action of said default rule if said default rule corresponds to the packet, and generates an error condition if said default rule does not correspond to the packet.

In accordance with still yet another aspect of the present invention, there is provided a method for providing peer-level access control on a network with a peer, said method comprising: a. receiving a packet having a packet identifier; b. searching a global pre-rule base and identifying a global pre-rule that corresponds to the packet; c. carrying out the action of a global pre-rule if the global pre-rule correspond to the packet; d. loading a local rule base of a peer when the peer is authenticated; e. if no corresponding global pre-rule is found in the global pre-rule base, searching the local rule base, identifying a local rule that corresponds to the packet, and carrying out the action of a local rule if the local rule corresponds to the packet; f. ejecting the local rule base from the filter; g. if no corresponding global pre-rule is found in said global pre-rule base and no corresponding local rule is found in said local rule base, searching a global post-rule base for a global post-rule that corresponds to the packet; and h. carrying out the action of a global post-rule if the global post-rule corresponds to the packet.

The present invention comprises a filter that efficiently stores, implements and maintains access rules specific to an individual computer on a network with rapidly changing configurations and security needs. This advantageously allows an individual computer (a peer) to implement its security policy on a filter shared by many such computers on a network.

When a local rule base is no longer valid because the peer is no longer authenticated to the filter in accordance with the present invention, the peer's local rule base is "ejected," i.e., a logical operation is carried out at the filter whereby the local rule base is deleted from the filter. This logical operation of stored data in a computer is well known in the art. This effectively regulates the flow of information on session-by-session basis, which is especially advantageous in AIS where individual users and hosts have different security needs that change from time to time. For example, the present invention is useful for implementing a parental control system wherein a parent is able to regulate the access to certain types of licentious material on the Internet for household Internet access accounts.

The present invention allows a single device to flexibly and efficiently regulate the flow of information in accordance with security policies that are specifically tailored to the individual user or host. Advantageously, no intervention on the part of the system administrator is ordinarily required in the ordinary functioning of the present invention. Unlike known filters, the present invention is able to accommodate users with temporary network addresses as easily as hosts with fixed network addresses.

In accordance with the present invention, each individual peer is authenticated upon requesting network access. The peer's local rule base is then loaded into the filter of the present invention, either from the peer itself, or from another user, host or peer. When the peer is no longer authenticated to the POP (e.g., the peer loses connectivity or logs off from the POP), the peer's local rule base is ejected (deleted)from the filter.

Brief Description of the Drawings

FIG 1 shows the process of identification and authentication.

FIG 2 shows a firewall interposed between a corporate network and the Internet.

FIG 3 shows users connected to the Internet through a Point of Presence (POP) having an authentication system.

FIG 4 shows a POP with an authentication system and a filter.

FIG 5a shows a first Internet access session for two users through a POP having a filter.

FIG 5b shows a second Internet access session for two users through a POP having a filter.

FIG 6 shows a known method of providing user level access control to the Internet.

FIG 7a shows a rule base architecture in accordance with an embodiment of the present invention.

FIG 7b shows an implementation of the rule base architecture shown in FIG 7a.

FIG 8a shows a POP with a filter and an authentication system that provides access to the Internet to three peers.

FIG 8b shows a simplified depiction of the rule bases belonging to the peers shown in FIG 8a.

FIG 8c shows a hash function applied to the network addresses of the three peers shown in FIG 8a, and the local-in and local-out rule bases.

FIG 8d shows a detailed representation of the box "Check Local Rule Base" shown in FIG 7b.

FIG 9 shows an implementation of the present invention.

Detailed Description

In accordance with the present invention, FIG 7a shows an embodiment of a rule architecture that incorporates the functionality of known filters by including a global pre-rule base 701, a local rule base 702 and a global post-rule base 703.

The global pre-rule base 701 usually comprises general rules that apply to all hosts behind the firewall, and are most efficiently applied before any local rules. An example of a global pre-rule is that no telnet (remote login) requests are allowed past the firewall.

The local rule base 702 comprises the set of peer rule bases loaded into the filter for authenticated peers. These rule pertain to specific hosts. An example of a local rule is that host A may not receive e-mail from beyond of the firewall.

The global post-rule base 703 comprises general rules that are most efficiently applied after the global pre-rule base and local rule base is searched. A rule applied in the global post-rule base need not have the same effect as if it were applied in the global pre-rule base. Consider the above example prohibiting the reception of certain telnet requests. If this rule is placed in the global post-rule base, the local rule base is searched first, and may contain a rule allowing a telnet request through for a particular peer. If such a rule is found in the local rule base, the global post-rule base is not subsequently searched, and the telnet request is allowed to pass. Consider the different effect of the same rule when it occurs in the global pre-rule base, which is to block all telnet requests for all hosts behind the firewall. The importance of the order of applying rules is evident from a more thorough consideration of the method of the present invention.

FIG 7b illustrates a flow chart of packet processing or filtering in accordance with the present invention. As shown therein, a packet entering the filter is first checked against a global pre-rule base 711 containing rules for all hosts and users having network addresses behind the firewall.

If a corresponding rule is found and the prescribed action is DROP, the packet is dropped 712. If a corresponding rule is found and the action is PASS, the packet is passed 720. If no corresponding rule is found, then the local rule base is checked 713.

The local rule base 702 is the set of all per user rule bases that are dynamically loaded upon authentication and ejected upon loss of authentication in accordance with the present invention.

If a corresponding rule is found in the local rule base and the action is DROP, the packet is dropped 714. If a corresponding rule is found and the action is PASS, the packet is passed 721. If no corresponding rule is found, then the global post-rule base is checked 715.

If a corresponding rule is found in the global post-rule base and the action is DROP, the packet is dropped 716. If the action is PASS, the packet is passed 722. If no corresponding rule was found in any of the rule bases, then the packet is checked against the default rule 717, whose action is generally to DROP the packet. If the packet corresponds to the default rule, then the default action is carried out 723. If the packet does not match the default rule, then an error condition occurs 724.

This rule base architecture advantageously retains the functionality of known filters. For example, if there are rules in the global pre- or post-rule base only, the filter behaves the same as known filters. If there are only rules in the local rule base, the filter has all of the new and innovative features of the present invention without having global rules.

It is advantageous to implement the present invention with a system for efficiently searching the local rule base for corresponding rules for a given packet. A system that provides such efficiencies uses a hash function to generate an index for the rules. A hash function maps a string of characters to an integer. As is known in the art, a character string is represented as binary numbers inside a computer. An example of a hash function would be to take the third, fourth and fifth bytes of a character string as it is stored in a computer as the first, second and third digits of an integer to be associated with the string. A string on which a hash function has been carried out is said to be "hashed," and the resulting integer is referred to as the "hash" of the string.

This is carried out by logically dividing the local rules into local-in rules and local-out rules. A local-in rule is any rule that applies to a packet whose destination address corresponds to a network address behind the firewall. For example, suppose a host with network address A is behind the firewall, and hosts B, C and D are outside the firewall. The following are examples of local-in rules for host A, following the format SOURCE ADDRESS, SOURCE PORT--> DESTINATION

ADDRESS, DESTINATION PORT: Protocol: ACTION:

B,31-->A,33:4:DROP

C,64-->A,45:4:PASS

D,11-->A,17:4:PASS

A local-out rule is any rule that applies to a packet whose source corresponds to a network address behind the firewall. Local out-rules for the above example are:

A,44-->B,70:4:PASS

A,13-->C,64:4:DROP

A,12-->D,17:4:DROP

In accordance with the present invention, a hash function h is carried out on the network address of the owner of a local rule base. A hash function associates an integer with a string. For the above example in which a host with network address A ("host A") has a local rule base, a hash function would be carried out on A:

h(A)=N, where N is an integer

An example of such a hash function is to take the last decimal digit in each octet of an IP address and compose an integer for the hash number. Thus, for example, the IP address 123.4.46.135 would have a hash value of 3465.

After the hash function is carried out, a local-in and a local-out hash table is generated. These tables are essentially indexes searchable on hash numbers derived from network addresses of peers, where each hashed peer network address points to that peer's local-in and local-out rules. Thus, if A is the network address of peer A, and if h(A)=32, then 32 would point to peer A's local-in and local-out rules in the local rule base.

The advantages of this indexing system in accordance with the present invention may be demonstrated with the aid of FIGs 8a, 8b, 8c and 8d. FIG 8a shows an example architecture where peers A 801, B 802, and C 803 are behind a firewall 804 having a filter 805 connected to a network 806 having hosts G 807, H 808 and I 809. These letters represent network addresses. FIG 8b shows the local rule base associated with each host. For simplicity, each rule in the rule bases is shown only as a network source and destination address; the source and destination ports and protocol numbers are not shown. The asterisk represents a wildcard indicating any host. For example, this feature may be advantageously implemented in accordance with the present invention by including wildcards in one or more of the four octets that constitute an IP address. The following IP address specifications are all valid for use in rule bases in accordance with the present invention:

123.*.233.2

34.*.*.155

..*.32

..*.*

The wildcard feature may also be used in accordance with the present invention in a similar fashion in any other component in the 5-tuple, i.e., the source and destination ports and the protocol.

FIG 8c shows the peer-in hash table 821 and peer-out hash table 822 derived from the local rules shown in FIG 8b and hash function h carried out on network addresses A, B and C 823. When a packet is received by the filter 805, the filter carries out the same hash function h on the packet's source and destination address 824.

FIG 8d shows the method by which the hash tables are searched in accordance with the present invention. FIG 8d represents a detailed view of the box "Check Local Rule Base" 713 in FIG 7b.

In accordance with the present invention, if there was no corresponding rule found in the global pre-rule base 711 (FIG 7b), then the local-in hash table is efficiently searched for a rule that corresponds to the packet 841. If a corresponding rule is found and the action is DROP, the packet is dropped 842. If the action is PASS or there is no corresponding rule, the peer-out hash table is checked 843. If a corresponding rule in the hash-out table is found and the action is DROP, the packet is dropped 844. If the action is PASS or there is no corresponding rule, and if at least one of the hash tables contained a corresponding rule, the packet is passed 845. If there were no corresponding rules in either hash table 846, then the post-rule base is checked 715 as shown in FIG 7b.

Were it not for the peer-in and peer-out hash tables, the rules would have to be searched far less efficiently by searching the entire rule base for rule identifiers (e.g., 5-tuples) that match the packet identifier (e.g., 5-tuple.) The part of the rule that identifies the packet to which the rule applies (the rule identifier) is also called the rule "key." Using hash tables eliminates the need to search the keys of all rules, pointing instead to the relevant subset of possibly applicable rules through a speedier search. Thus, the scope and computational time needed to carry out the search is substantially and advantageously reduced, reducing the delay in packet transit time caused by the interposition of a filter between the packet source and destination.

As shown in FIG 9, a peer is first authenticated 91 in accordance with the present invention. Upon authentication, the peer's local rule base is loaded into the filter 92. A hash function is carried out on the peer's network address 93, and the filter's peer-in and peer-out hash tables are updated 94 with pointers to the peer's peer-in and peer-out rules. When the peer is no longer authenticated 95, the peer's local rules are ejected from the filter local rule base 96, and the pointers to the peer's peer-in and peer-out rules are ejected from filter's peer-in and peer-out hash tables 97.

The present invention provides new security functionality on a per user basis to filters and firewalls, while maintaining the functionality of known filters. The present invention allows for the dynamic adjustment of local rule bases that can be dynamically tailored to meet the changing needs of the individual user.

Claims:

1. A filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises:

a. means for accessing a peer's local rule base;

b. means for detecting when the peer is authenticated;

c. means for loading a rule from the peer's local rule base at the filter when the authentication of the peer is detected;

d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and

e. a global pre-rule base having a global pre-rule, wherein upon receiving the packet, said filter first searches said global pre-rule base for a rule that corresponds to the packet and carries out the action of the corresponding global pre-rule on the packet, and wherein if no corresponding global pre-rule is identified, the filter searches the local rule base for a rule that corresponds to the packet and carries out the action of the corresponding local rule on the packet.

2. The filter of claim 1, further comprising:

f. means for detecting when the peer logs off; and

g. means for ejecting said local rule base from said filter upon detecting that the peer has logged off.

3. The filter of claim 1, wherein the packet identifier comprises a source and destination address, a source and destination port, and a protocol identifier.

4. The filter of claim 1, wherein said means for accessing the local rule base comprises receiving and storing the local rule base.

5. The filter of claim 1, further comprising means for authenticating the peer.

6. A filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises:

a. means for accessing a peer's local rule base;

b. means for detecting when the peer is authenticated;

c. means for loading a rule from the peer's local rule base at the filter when the authentication of the peer is detected;

d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and

e. a global post-rule base, wherein the global post-rule base is searched for a rule that corresponds to the packet, and the action of a global post-rule is carried out if it corresponds to the packet only if no corresponding rule in said global pre-rule base and no corresponding rule in said local rule base are identified.

7. The filter of claim 6, further comprising:

f. means for detecting when the peer logs off; and

g. means for ejecting said local rule base from said filter upon detecting that the peer has logged off.

8. The filter of claim 6, wherein the packet identifier comprises a source and destination address, a source and destination port, and a protocol identifier.

9. The filter of claim 6, wherein said means for accessing the local rule base comprises receiving and storing the local rule base.

10. The filter of claim 6, further comprising means for authenticating the peer.

11. A filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises:

a. means for accessing a peer's local rule base;

b. means for detecting when the peer is authenticated;

c. means for loading a rule from the peer's local rule base at the filter when the authentication of the peer is detected;

d. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer; and

e. a default rule, wherein if no corresponding pre-global rule and no corresponding local rule and no corresponding post-global rule are identified, said filter carries out the action of said default rule if said default rule corresponds to the packet, and generates an error condition if said default rule does not correspond to the packet.

12. The filter of claim 11, further comprising:

f. means for detecting when the peer logs off; and

g. means for ejecting said local rule base from said filter upon detecting that the peer has logged off.

13. The filter of claim 11, wherein the packet identifier comprises a source and destination address, a source and destination port, and a protocol identifier.

14. The filter of claim 11, wherein said means for accessing the local rule base comprises receiving and storing the local rule base.

15. The filter of claim 11, further comprising means for authenticating the peer.

16. A method for providing peer-level access control on a network with a peer, said method comprising:

a. receiving a packet having a packet identifier;

b. searching a global pre-rule base and identifying a global pre-rule that corresponds to the packet;

c. carrying out the action of a global pre-rule if the global pre-rule corresponds to the packet;

d. loading a local rule base of a peer when the peer is authenticated;

e. if no corresponding global pre-rule is found in the global pre-rule base, searching the local rule base, identifying a local rule that corresponds to the packet, and carrying out the action of a local rule if the local rule corresponds to the packet;

f. ejecting the local rule base from the filter;

g. if no corresponding global pre-rule is found in said global pre-rule base and no corresponding local rule is found in said local rule base, searching a global post-rule base for a global post-rule that corresponds to the packet; and

h. carrying out the action of a global post-rule if the global post-rule corresponds to the packet.

17. The method of claim 16, further comprising the steps of:

i. if no corresponding rule is found in the global pre-rule base and no corresponding rule is found in the local rule base, and no corresponding rule is found in the global post-rule base, determining if the packet corresponds to a default rule; and

j. carrying out the action of the default rule if the default rule corresponds to the packet, and generating an error condition if the default rule does not correspond to the packet.

FIG. 1
(PRIOR ART)

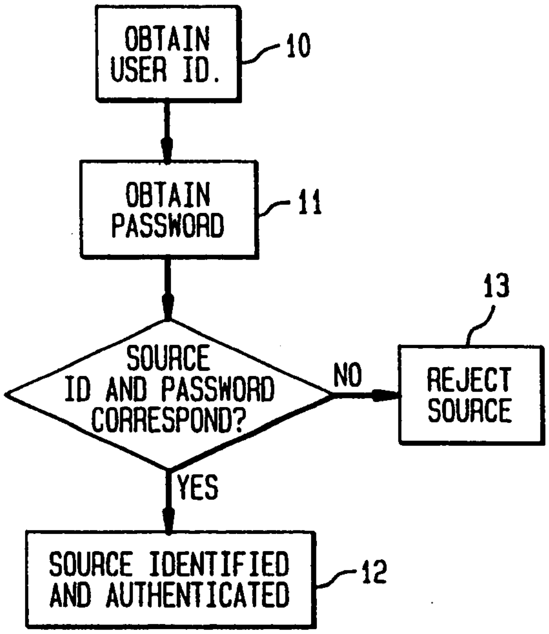

OBTAIN USER ID.
10
OBTAIN PASSWORD
11
SOURCE ID AND PASSWORD CORRESPOND?
NO
13
REJECT SOURCE
YES
SOURCE IDENTIFIED AND AUTHENTICATED
12

FIG. 2
(PRIOR ART)

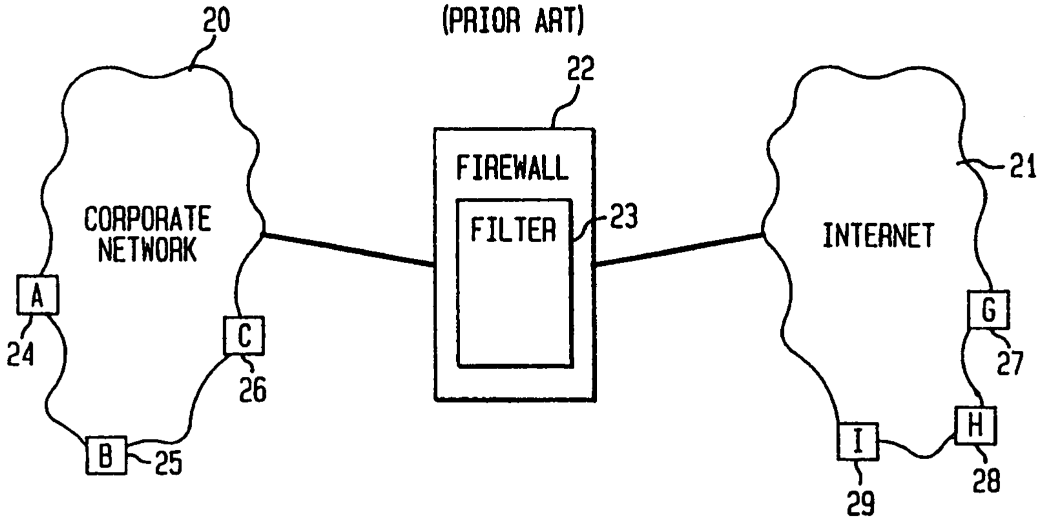


FIG. 3
(PRIOR ART)

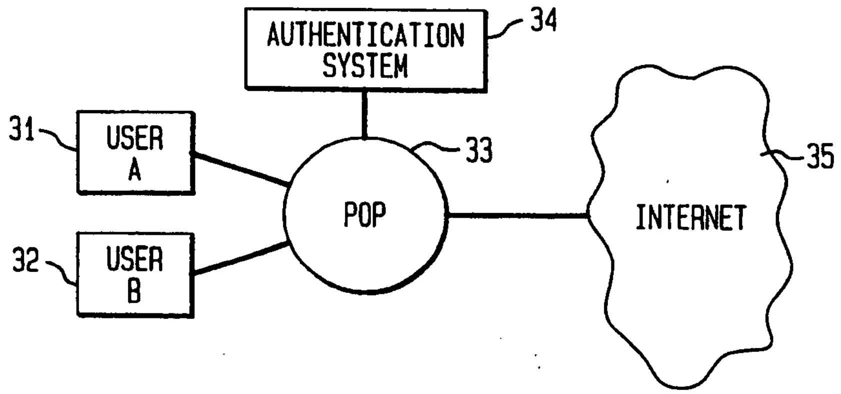


FIG. 4
(PRIOR ART)

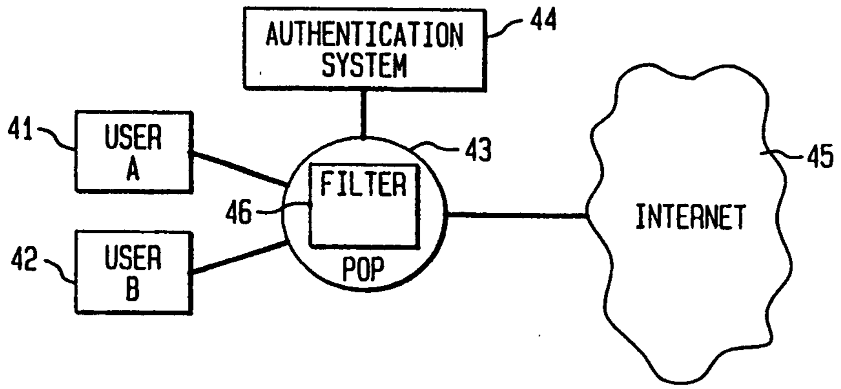


FIG. 5A

(PRIOR ART)

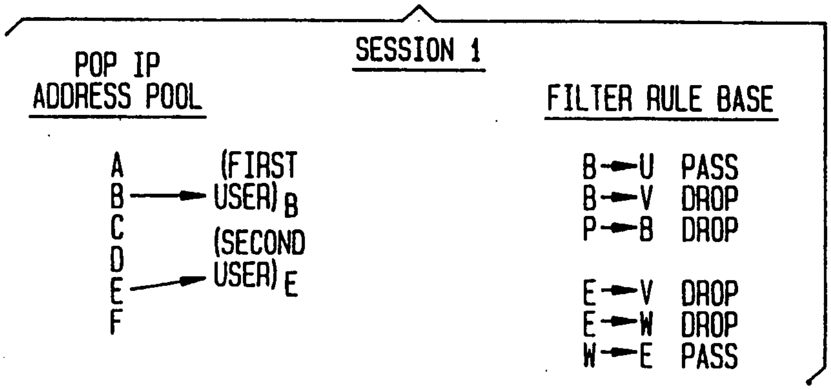


FIG. 5B

(PRIOR ART)

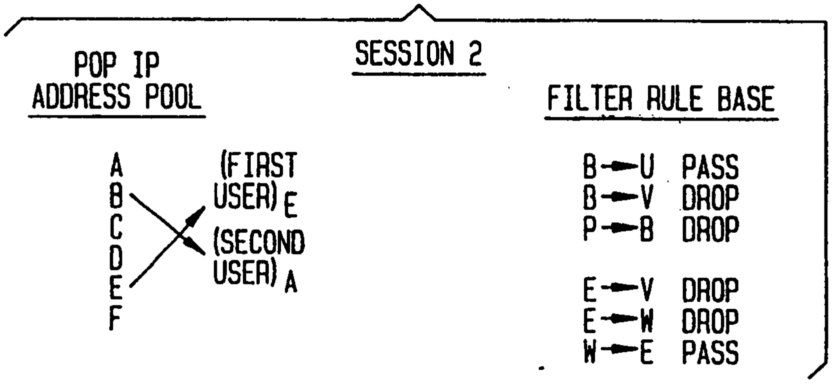


FIG. 6

(PRIOR ART)

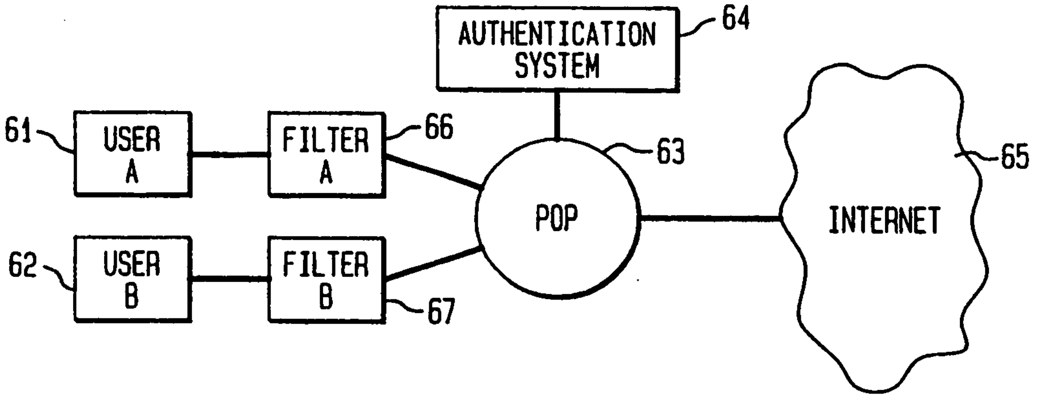


FIG. 7A

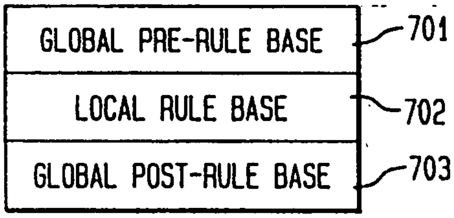

GLOBAL PRE-RULE BASE
701
LOCAL RULE BASE
702
GLOBAL POST-RULE BASE
703

FIG. 7B

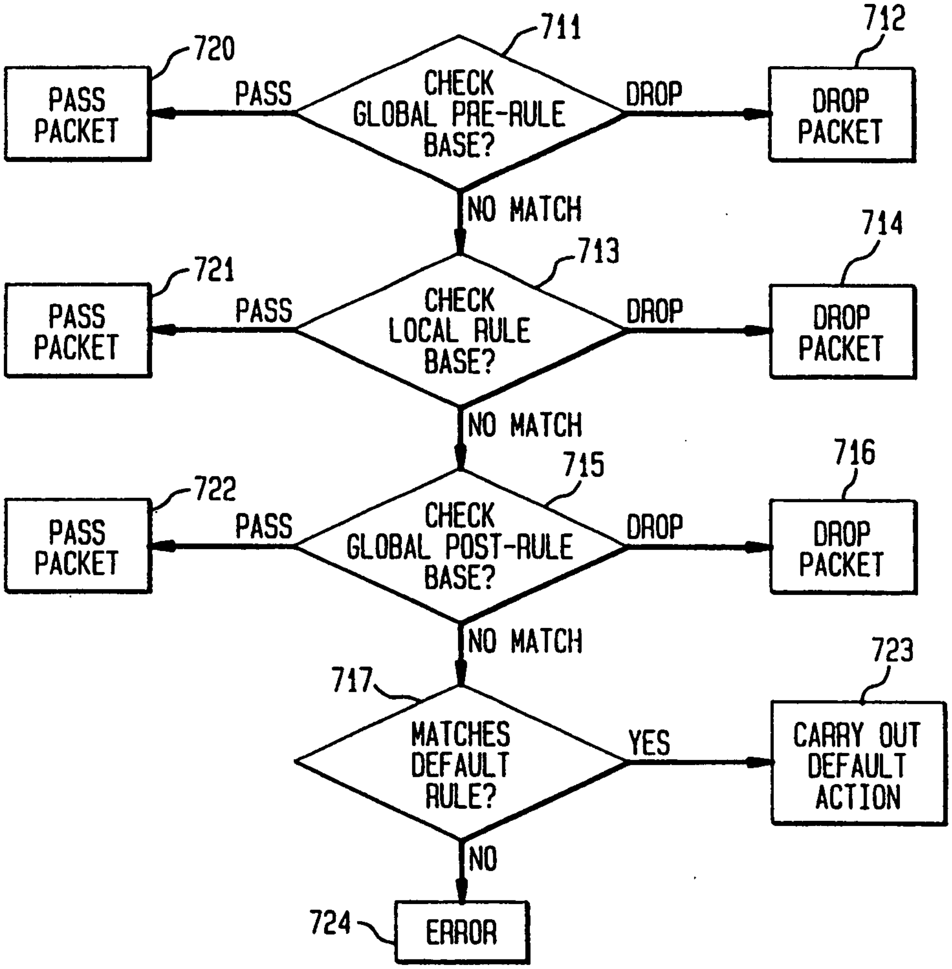

711
CHECK GLOBAL PRE-RULE BASE?
PASS
720
PASS PACKET
DROP
712
DROP PACKET
NO MATCH
713
CHECK LOCAL RULE BASE?
PASS
721
PASS PACKET
DROP
714
DROP PACKET
NO MATCH
715
CHECK GLOBAL POST-RULE BASE?
PASS
722
PASS PACKET
DROP
716
DROP PACKET
NO MATCH
717
MATCHES DEFAULT RULE?
YES
723
CARRY OUT DEFAULT ACTION
NO
724
ERROR

FIG. 8A

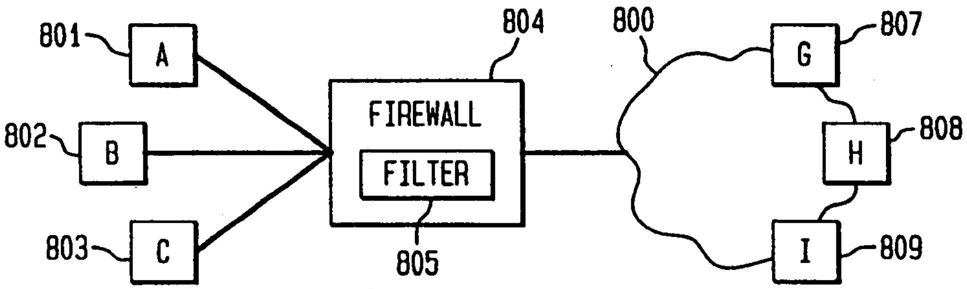
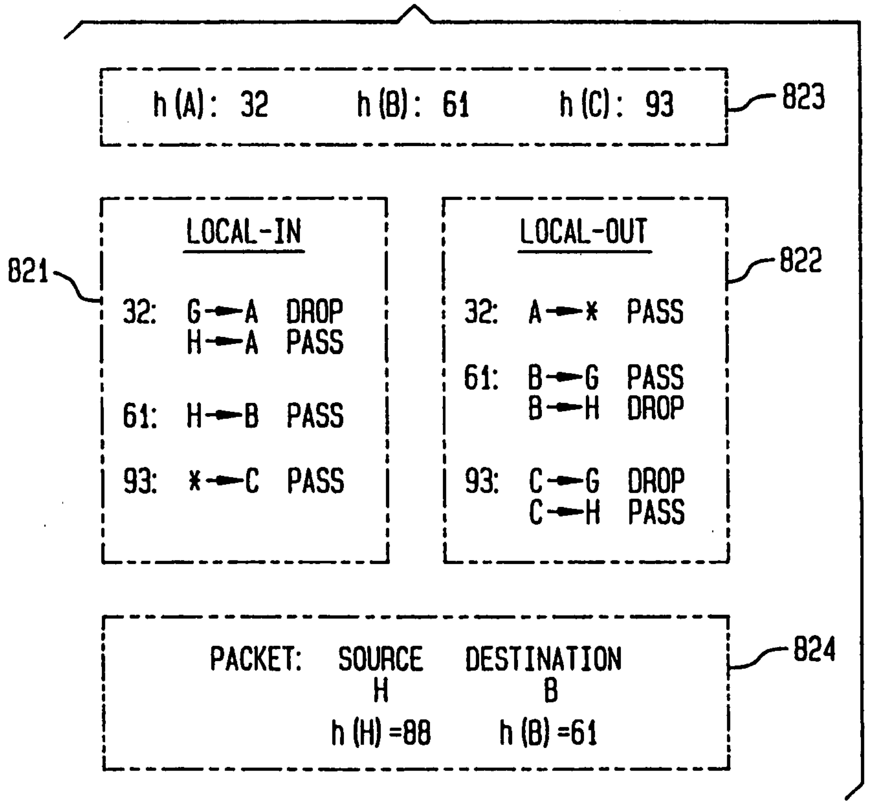


FIG. 8B

A: A ↔ * PASS	B: B ↔ G PASS	C: * ↔ C PASS
G ↔ A DROP	B ↔ H DROP	C ↔ G DROP
H ↔ A PASS	H ↔ B PASS	C ↔ H PASS

FIG. 8C



h (A): 32 h (B): 61 h (C): 93

LOCAL-IN			LOCAL-OUT		
32:	G ↔ A	DROP	32:	A ↔ *	PASS
	H ↔ A	PASS	61:	B ↔ G	PASS
61:	H ↔ B	PASS		B ↔ H	DROP
93:	* ↔ C	PASS	93:	C ↔ G	DROP
				C ↔ H	PASS

PACKET:	SOURCE	DESTINATION
	H	B
	h (H) =88	h (B) =61

FIG. 8D

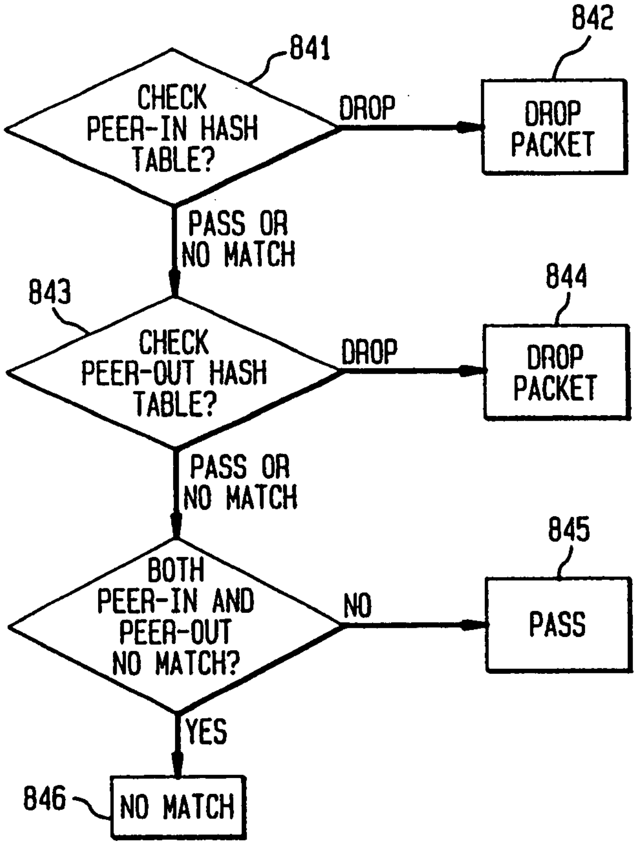
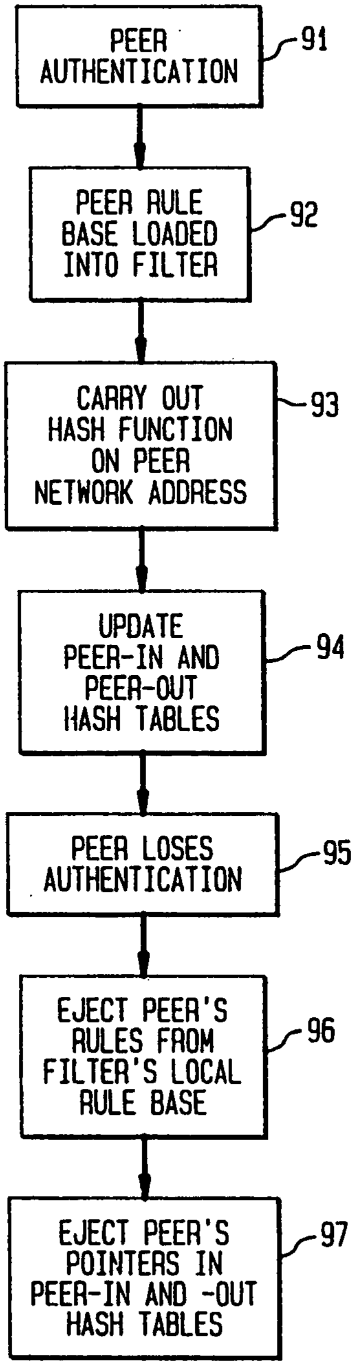

841
CHECK PEER-IN HASH TABLE?
DROP
842
DROP PACKET
PASS OR NO MATCH
843
CHECK PEER-OUT HASH TABLE?
DROP
844
DROP PACKET
PASS OR NO MATCH
BOTH PEER-IN AND PEER-OUT NO MATCH?
NO
845
PASS
YES
846
NO MATCH

FIG. 9


PEER AUTHENTICATION
91
PEER RULE BASE LOADED INTO FILTER
92
CARRY OUT HASH FUNCTION ON PEER NETWORK ADDRESS
93
UPDATE PEER-IN AND PEER-OUT HASH TABLES
94
PEER LOSES AUTHENTICATION
95
EJECT PEER'S RULES FROM FILTER'S LOCAL RULE BASE
96
EJECT PEER'S POINTERS IN PEER-IN AND -OUT HASH TABLES
97

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
G06F 17/30

A2

(11) International Publication Number: WO 98/03927

(43) International Publication Date: 29 January 1998 (29.01.98)

(21) International Application Number: PCT/US97/13309

(22) International Filing Date: 22 July 1997 (22.07.97)

(30) Priority Data:
60/022,035 22 July 1996 (22.07.96) US

(71) Applicant: CYVA RESEARCH CORPORATION [US/US]; Suite 219, 437 South Highway 101, Solana Beach, CA 92075 (US).

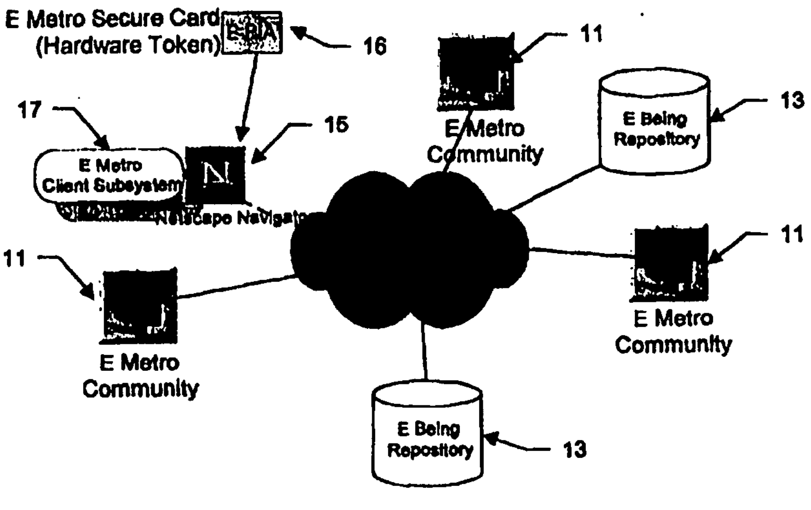
(72) Inventors: O'NEIL, Kevin; 3540 Seahom Circle, San Diego, CA 92031 (US). SEIDMAN, Glenn, R.; 830 West California Way, Woodside, CA 94062 (US).

(74) Agents: TEKANIC, Jeffrey, D. et al.; Lyon & Lyon, First Interstate World Center, Suite 4700, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

(81) Designated States: DE, IL, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: PERSONAL INFORMATION SECURITY AND EXCHANGE TOOL



(57) Abstract

Utilization of the E-Metro Community and Personal Information Agents assure an effective and comprehensive agent-rule based command and control of informational assets in a networked computer environment. The concerns of informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to author, secure, search, process, and exchange personal and/or confidential information in a networked computer environment. The formation of trusted electronic communities wherein members command and control their digital persona, exchanging or brokering for value the trusted utility of their informational assets is made possible by the invention. The present invention provides for the trusted utilization of personal data in electronic markets, providing both communities and individuals aggregate and individual rule-based control of the processing of their personal data.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

PERSONAL INFORMATION SECURITY AND EXCHANGE TOOL

FIELD OF INVENTION

The present invention relates to the software management of information within a network computing environment. More specifically, the present invention relates to a software system operating on the Internet that creates a virtual private network where a user may author, secure, search, exchange and process personal information in a trusted and controlled manner. This software system encapsulates trusted communities and their members, where a trusted authority certifies the identity and the informational-self of community members. Once a user is registered with a trusted community, the user can author and secure at will the hypermedia content, command and control the rule-based presentation and processing of their personal information.

BACKGROUND OF THE INVENTION

The introduction and accelerating use of the Internet has resulted in an explosion of both the quantity and availability of personal information. Unfortunately, since the Internet is largely unregulated, there is no assurance that all this information is accurate or reliable, and often the source of the data is not even ascertainable. Additionally, unless particular precautions are taken, anything sent via the Internet is subject to interception and misuse. These joint concerns for data reliability and data protection can be combined into a multifaceted concept of a trusted information utility. Data reliability or trustworthiness is present if the data is accurate and can be authenticated and/or corroborated. Trusted utilization is when data is available for access or processing only by those approved by the owner of the data, and assurance of continued command and control according to rules established by the owner is present. Trusted utilization or trusted processing is especially critical when dealing with personal data. Personal information, such as an individual's credit worthiness, medical history, employment background, or lifestyle is now finding its way on to the Internet. It is likely that law enforcement agencies, credit bureaus, landlords, and others will be using this information to assist in making decisions. Since all these groups make decisions that dramatically impact an individual's life, using incorrect data, or information that they shouldn't even have, can be devastating.

Thus, people realize that something must be done to protect a person's personal information and as more individuals join the Internet, there will be more pressure to collect, use, and market the available personal information, and the individual will want to participate in, command, and control this activity. Collectively, these ideas cannot be properly implemented with the Internet tools presently available, and no tool can efficiently incorporate these ideas. Thus, there is a need to provide an Internet utility or tool for the security and exchange of personal information.

It is therefore an object of the present invention to assist in the trusted utilization of personal information on the Internet by 1) providing a mechanism for individuals or entities securely author and encapsulate personal data and processing rules governing the presentation and processing of personal information, while 2) empowering the individual or entity, at will, command and control of their personal information within network computing environments.

SUMMARY OF THE INVENTION

The present invention is a software system for operating on network servers, with supporting applications operating on an individual user's personal computer system, inclusive of wire-line and wireless tele-computing devices. This invention is directed to a system for allowing an individual or entity to protect, command, control, and process personal information on a computer network, including the Internet. Specifically, this invention facilitates the formation and use of networked Trusted Electronic Communities, hereafter referred to as E-Metro Communities, where each E-Metro Community comprises several members meeting common admission requirements.

Preferably, it is the E-Metro Community that sets registration rules and verifies member identity itself or facilitates the use of other trusted Certificate Authorities. The informational identity of each member is encapsulated within the E-Metro Community as electronic personal information agents, hereafter referred to as E-PIAs, with each E-PIA representing a member's information and behavior, with some of the information supplied by each member and some of the information coming from trusted sources external to the member's E-Metro Community. By establishing and enforcing registration rules and performing accountable and audited verifications of member identity, and if so chosen, personal information certification, the E-Metro Community builds a community wherein each of its members can belong and participate in a electronic domain where the rights and responsibilities of privacy and informational self-determination are realized. Thus, it is through the association and certification by a trusted E-Metro Community that a member becomes trusted and reliable in other transactions, but more importantly gains control of their data.

Once a user is a member of an E-Metro Community, the member can assign access rules to each piece of personal information. These access rules set the requirements that must be met before an individual piece of information can be processed. Additionally, the E-Metro Community may get minimum standards for all transactions which must be met. When a request for a particular piece of information is received, E-Metro Community standards and the rule attached to that piece of information is checked by a processes specific to the E-Metro Community, hereafter referred to as the E-Metro Community's E-Broker. The E-Broker is the actual process that checks to see if the requester and the situation meet the requirement of the rule. If so, the E-Broker allows the requested information to be processed; if not, the E-Broker does not allow the information to be processed. Additionally, the information may be transport packaged with transitive privilege rules attached, that is, rules that define the requirements for processing by anyone other than the original member. Using these transitive privilege rules, a member can maintain command and control on third party dissemination and processing of their personal information.

A member may also create an agent, hereafter referred to as an E-AutoPIA, to interact with other members in any E-Metro Community, or even with data external to any E-Metro Community. This agent contains a subset of the personal information on the member, plus contains an itinerary that directs the activity of the agent. Thus, the agent is able to interact with the personal information of other members as directed in its itinerary.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features, and advantages of the invention will become more readily apparent upon reference to the following detailed description of a presently preferred embodiment, when taken in conjunction with the accompanying drawings in which:

Fig. 1 shows users connected to network servers accessing the Internet.

Fig. 2 shows how a user of the preferred embodiment views other E-Communities on the Internet.

Fig. 3 shows the components of a digital certificate, e.g., VeriSign's Digital ID.

Fig. 4 shows how RSA Public-key cryptography works and how a digital signature is created and attached to a document to assure authorship.

Fig. 5 shows an E-AutoPIA operating outside the E-Metro Community.

Fig. 6 shows an E-AutoPIA that has collected several informational E-PIAs from several E-Metro Communities.

Fig. 7 shows several network servers, a user's personal computer connected into the Internet plus a wireless communicator.

Fig. 8 shows several E-Metro Community systems along with other resources interconnected by the Internet.

Fig. 9 shows the architecture of the E-Metro Trusted Server.

Fig. 10 details the DORMS subsystem in the E-Metro Trusted Server, which is shown in Fig. 9.

Fig. 11a-d detail the storage mechanism for several objects used in the preferred embodiment.

Fig. 12 details the messaging subsystem used in the DORMS subsystem, which is shown in Fig. 10.

Fig. 13 is a Booch diagram of the E-Metro Community object.

Fig. 14 is a Booch diagram of the E-Broker object.

Fig. 15a is a Booch diagram of the E-PIA object.

Fig. 15b is a Booch diagram of the informational E-PIA object.

Fig. 16 is a Booch diagram of the E-AutoPIA object.

Fig. 17 is a Booch diagram of the itinerary object.

Fig. 18 is a Booch diagram of the Interact Instruction object.

Fig. 19 is a Booch diagram of the Interact Protocol object.

Fig. 20 is a Booch diagram of the rule object.

Fig. 21 is a Booch diagram of the parameter object.

Fig. 22 describes the relationship of the various classes of objects used within the preferred embodiment.

Fig. 23 shows the basic Booch symbols employed in the object model descriptions within the preferred embodiment.

Fig. 24 shows that the communication external to an E-Metro Community are all done with RSA-type security and encryption.

Fig. 101 is the user interface to the preferred embodiment showing the initial screen.

Fig. 102 is the user interface to the preferred embodiment showing the log-in screen.

Fig. 103 is the user interface to the preferred embodiment showing the community listings screen.

Fig. 104 is the user interface to the preferred embodiment showing how E-Metro Community members construct and execute searches displaying search results.

Fig. 106 is the user interface to the preferred embodiment showing the initial page of an E-Metro Community registration object being authored.

Fig. 107 is the user interface to the preferred embodiment showing the selected E-Being performing a trusted presentation of their personal information, with certain components and their attributes indicating secured or locked status because the requesting viewer does not meet the requirements set by the E-Metro Community and E-Metro Community member.

Fig. 108 is the user interface to the preferred embodiment presenting additional personal information indicating attributes with disclosed and undisclosed access-processing rules.

Fig. 109 is the user interface to the preferred embodiment presenting rule authoring and assignment of rules to both particular personal information attributes and particular groups or sub-communities of a community.

Fig. 110 is the user interface to the preferred embodiment presenting rule authoring governing what criteria a processor of information must meet to access-process the user's information.

Fig. 201 details the E-Bazaar E-Broker subsystem.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment of the invention primarily operates on a network server, with supporting applications operating on the individual's personal computer system. To a user, the preferred embodiment appears as a Web site, so it may be accessed simply by knowing its Web site address, but it is a Web site with comprehensive security safeguards: firewalls, proxy servers, SSL enabled Web servers and clients, digital certificates, hardware tokens, security policies and procedures. Not only will the Web site typically require certificate-based identification for access, but all communications between E-Metro Communities and members and other E-Metro Communities will be encrypted. For additional assurance of user identification, an optional hardware token or secure card security system may be implemented. This security system will be discussed in a later section.

As discussed earlier, trusted processing of information has two components: reliability of content and controlled processing, and each is addressed by the preferred embodiment of the invention. It is easiest and most clear to discuss the preferred embodiment using a metropolis analogy. Just as in a city, the Internet provides an individual a place to meet others, share information, seek entertainment, do work, and shop. Likewise, every individual on the Internet has an address where correspondence may be sent. In the city, caution must be used when meeting someone for the first time as it may be unwise to give too much information to someone who is untrustworthy. Also, business transactions with a new person must be done carefully as the quality of goods, standard of support, or origin of the product is not known. These same concerns appear with new encounters and transactions on the Internet.

In the city, people use an unfamiliar person's associations to lower the risk of these new encounters and transactions. For example, if someone is wearing a police uniform, we will typically be more likely to give them our drivers license number, home address, and other personal information. If someone is seated in an attorney's office and hands us a business card with the title of "Attorney," we are more likely to expose confidential information. Also, if someone lives in our same community, maybe even our neighbor, we too will be more likely to share information and feel safe conducting a transaction. On the Internet, if a person has an address that ends in .gov, we may feel safer doing business with them, as some government agency has allowed them access to the Internet from a government network server, thus giving that user an air of trustworthiness. If that user conducts a bad transaction, the agency that allowed their access to the Internet can be contacted, and the agency is likely to sanction that user. However, the vast majority of users on the Internet will be from network servers that provide no hint as to their trustworthiness. Therefore, the preferred embodiment of the present invention provides a method to reduce the risk in new interactions, and increase the probability that the other user is who they say they are: the preferred embodiment creates agent-rule based trusted electronic communities.

In the city, citizens belong to several communities. Some communities are defined by geography, ethnic background, religion, alma mater, employment, or hobbies. Commonly, people get a great deal of self-identification and satisfaction from choosing the communities to which they belong. It is quite common for someone to refer to themselves as an employee of a company, as a member of a religion, or as an expert at a hobby. Belonging to a community is not only personally satisfying to the member, but allows the reputation of the E-Metro Community to lower the risk of dealing with any one of its members.

In the preferred embodiment, a user may join one or more E-Metro Communities. Each of these E-Metro Communities is independently operated by an administrator that sets admission requirements, authenticates membership, issues digital certificates, and sets the services available to members. The E-Metro Communities are actually implemented as Web sites on the Internet, but are special Web sites as they have a great deal of intelligence and utility. Fig. 2 diagrams a user's view of the Internet using the preferred embodiment. The user will be a member of one or more E-Metro Communities 11 and be aware there are several other E-Metro Communities 11 on the Internet. The user will use a Web Browser such as Netscape Navigator 15 running on their personal computer to access the Internet and attempt to become a member of one or more E-Metro Communities. When desiring to become a member of an E-Metro Community, it is possible to retrieve an unregistered or empty

E-Being object from the E-Metro Community or from a public E-Being repository 13 that will need to be initialized with identity information and certified in order to become a member. An unregistered E-Being may be retrieved prior to visiting the E-Metro Community desired to be joined. Once a user is authorized to join an E-Metro Community, the user becomes a member of that E-Metro Community and can use the services the E-Metro Community administrator has provided. Services may include links to other E-Metro Communities, shopping, or access to information. Besides the standard Netscape Navigator 15, the member will also need some additional support programs at their local computer, the client subsystem 17. These client subsystem 17 support programs are processes that allow the Netscape Navigator to have specific functionality in support of specific E-Metro Communities. These programs will be provided as part of the preferred embodiment, but will be configurable by the E-Metro Community administrator or even the user to provide specific functionality. These programs could be created in any language, but Java is presently preferred. It should be a goal of each E-Metro Community, however, to not require additional software besides standards based browsers, as this maintains a much easier to support client software subsystem. Additionally, the member may desire to gain privilege or access to specific E-Metro Community services to which it does not have rights. The E-Metro Community may require further information to be filled out in forms that must be submitted for approval. These forms are stored in an E-Being repository 13, and can be set up as an independent Web site, an FTP site, or any other storage mechanism allowed on the Internet.

Remembering that trusted processing comprises reliability and controlled processing, in the preferred embodiment, trusted processing of personal data is improved by two means. First, the personal information that is processed is authored and monitored by the individual. The information can also be verified by third parties who issue digital certificates which corroborate the facts claimed by the individual. The information stored is transparent to the individual. Additionally, the users themselves can request trusted certificate authorities to verify and assert the reliability of the personal information. The Certificate Authorities issue digital certificates asserting the reliability of the data. An example would be a credit union, which will certify personal financial or loan data. As an E-Metro Community's reputation for reliability and user-centric control of personal information processing increases, the informational value and mutual trust of its users will also increase.

The other aspect of trusted processing, protection of data, is improved in two ways by the preferred embodiment of the present invention. First, the preferred embodiment uses state-of-the-art techniques, such as public-key cryptography, to securely store and transmit information. Public-key cryptography is discussed in more detail in a later section. These techniques assure that the data can not be deciphered if intercepted during transmission, and only the intended reader can decrypt and understand the information. The second security feature of the preferred embodiment is designed to place controls on the amount of information processed and to limit the utilization of data to recipients meeting criteria established by the user. This security feature allows the user to set rules that govern the processing and utilization of personal information. For example, one rule may state that it is acceptable to release legal history information to a user that is from the American Bar Association E-Metro Community. Another rule may state it is acceptable to utilize a home phone number by a user that is single, from a particular geographic area, and also agrees to have their home number utilized in a controlled manor. By setting sufficient rules, an individual can control the utilization of personal information by only trusted users. Additionally, the user may set transitive rules that attach to information that control electronic distributed processing of the information. Thus, when a user authorizes trusted remote processing of personal information, the information is utilized in a manner that allows the user to maintain command and control of how the information is subsequently utilized.

The preferred embodiment additionally allows an individual to set rules for processing personal information for money or other value. An individual's preferences, physical characteristics, and buying habits have value to those selling products. Traditionally, marketing firms would collect and organize such information and sell those mailing lists to businesses that had a product that may appeal to those on the list. Using the preferred embodiment, an individual can "license" their own personal information to a business directly or to a marketing firm, thus sharing in the value created by the trusted processing of reliable personal information.

Referring now to Fig. 101, an example of what a user may see when accessing an E-Metro Community Web site is shown. Here, the computer user is running Netscape Navigator on their personal computer, and the standard Netscape Navigator menu items 501 can be seen. To get to this point, the user had to tell the Netscape Navigator the address of the E-Metro Community Web site, and the Netscape Navigator, through the user's network server, connected to the remote network server where this E-Metro Community Web site is located. Once accessed, the E-Metro Community Web site sends this introductory screen 511 to the user, which contains a graphical logo 505 and title 503 specific to this E-Metro Community. The user can select one of three option buttons 507: get more information on this E-Metro Community, go to the services available in this E-Metro Community (will require a security check-in), or, if a new user, register for admission to this E-Metro Community. If the user selects to register, the registration objects will be supplied by the E-Metro Community or retrieved from a E-Being repository and the user will author their E-Being, similar to filling out a standardized form.

If the user selects the services option, the user will be asked for security information and/or hardware tokens. In

Fig. 102, the E-Metro Community only asks for a certificate-based identification 523 and a security code or challenge response 515. Once the user selects "OK" 517, and the user is allowed into the E-Metro Community, the user can utilize the available services. In this example, the member is presented with the communities available screen 521 shown in Fig. 103, which is made of the graphical logo 505 and the community links 523. Services available in this E-Metro Community include search and selection, registration updates, advertising, shopping, customer support and other services selected by the E-Metro Community administrator. Search services provided in this E-Metro Community is the availability to perform parametric queries. Fig. 104 shows a partial view of the members who met a specific search request in this E-Metro Community, allowing the searching member to select particular E-PIAs by selecting a picture-link 527. Provided the requesting member has the proper qualifications as set by the interrogated member, the interrogated member's information can be seen by the requester.

The preferred embodiment is premised on a user's membership in at least one E-Metro Community, with the E-Metro Community defining the member's duties and rights. In the preferred embodiment, the E-Metro Community has three primary responsibilities. First, the E-Metro Community sets admission requirements that produces a high probability that the applicant for admission is who they say they are. Second, the E-Metro Community has security measures in place to reasonably assure that a member's identity can't be appropriated by someone else. Third, the E-Metro Community sets standards that place a high probability that the member is transacting business and disclosing accurately and in good faith.

The first responsibility for assuring the applicant is who they say they are is met in the preferred embodiment in a two step process. In the first step, an applicant, using the Netscape Navigator 15 accesses the Web site for the E-Metro Community 11 they wish to join. This user selects the registration object from an E-Being repository 13, fills it out and submits it to the E-Metro Community administrator. The E-Metro Community administrator reviews the application to assure that the applicant meets the E-Metro Community qualifications. If the applicant meets the qualifications, the application process moves to step two. In step two, the applicant/user appears in-person to the E-Metro Community administrator or another trusted authority or entity, such as a Certificate Authority or notary, to verify the user's identification. The applicant can present one or more pieces of identification, such as birth certificates, drivers' licenses, passport, social security card or other reliable means of identification. Once the applicant is personally identified and a key pair generated, they are issued a digital certificate binding the public key and both member and E-Metro Community information. A security code or challenge response access method is chosen and hardware token if requested. At a minimum the member will have a digital certificate and access method to fully use the selected and approved E-Metro Community services. The E-Metro Community is now reasonably assured that the person is who they say they are and has accounted for the processing of the registrant's application.

The second responsibility of the E-Metro Community is to assure that only the original applicant can use that member's identity. The digital certificate and security code or challenge response described above will assist in assuring the security of an individual's identity, but new technology allows for even greater security. For this advanced security, the E-Metro Community may issue the user a hardware token or secure-card, such as those sold commercially by Gemplus, Schlumberger, and Spyrus corporation. Although the LYNKS secure card from Spyrus has several options as to what information it can hold, three particularly useful items are 1) the basic information about the user, 2) a digital certificate, and 3) E-Metro Community digital certificate digitally signed by the certifying E-Metro Community. The first item may contain several pieces of information, including passwords, security codes, and particular challenges or code phases that can be used by the preferred embodiment to verify the identity of the user. For this challenge security, the user loads the security card with challenge response pairs that only the user will know. When the user wants to access an E-Metro Community, the security card "challenges" the user by presenting a challenge phrase that must be answered precisely. The second item, the digital signature, is an advanced security mechanism that allows the sender to attach a digital signature to a document that gives an assurance that a specific document was actually originated by that sender. The digital signature will be discussed in more detail in a later section. Those skilled in the art will recognize other alternatives to assure on-going security of a user's identity such as biometrics. The third item possibly held in the card stores information on the authority that certified this particular member. This authority could be the government, an E-Metro Community administrator or surrogate, or a commercial business. The more accountable, diligent and exhaustive the security policy and procedures are of the certifying agency, the higher the assurance that the member is also trustworthy.

The third responsibility for the E-Metro Community is to assure that the member properly transacts business and discloses personal information accurately and in good faith. This is mostly a policing process for the E-Metro Community, where those who violate the interaction policies for ethical interaction are removed from the E-Metro Community. Stricter enforcement of the rules will lead to a better E-Metro Community reputation for trustworthiness and accuracy.

Once there is assurance of the member's identity, the next level of security is to assure that the member can communicate with the E-Metro Community without messages and information being intercepted and interpreted by unauthorized individuals. This security level has two main components. First, the preferred embodiment uses security protocols approved by Netscape for commerce transactions, including purchases made on the Internet with a credit card. Second, the Netscape Navigator web browser has built in cryptography techniques, called public-key cryptography, that can assure the communication from the member to the E-Metro Community is secure from outside interception and interpretation. The preferred embodiment uses the public-key cryptography techniques supplied by RSA Data Security, Inc, but those skilled in the art will recognize alternatives.

Public-key cryptography is one method currently known for secure transfer of information. A diagram on the operation of public-key cryptography is shown in Fig. 3. In this method, each user has a code pair, where one code is public and one is private. These codes are commonly called keys, so each user has a public key and a private key. The public key list 25 is widely distributed to anyone that may need to send the user information. However, the private key is kept secret by the user. For example, if "A" wants to securely send a file to a "B," A will encrypt the file using the Bs public key 19. This key is publicized and available to anyone who wants it. After encryption, the file 21 can be deciphered only by using Bs private key 23, which is known only to B. Thus, if B has properly secured the private key, only B will be able to receive and interpret the encrypted file. It doesn't matter if the file is sent via an unsecured transmission method such as the mail, Internet, or phone lines, since no one that intercepts the message can interpret it, unless they have somehow appropriated Bs private key 23.

A second security mechanism is the previously introduced digital signature, and assures the receiver that the message was actually sent by the stated sender. As briefly discussed above, a member can use a digital signature to "sign" files so to give a high degree of assurance that it was the owner of the signature that sent the message. Fig. 4 will assist in explaining the use of the digital signature. To add a digital signature to a file, the member passes the file 27 through a mathematical formula 31 that produces a digital pattern, or message digest 33, that is unique to that file. This message digest 33 is then encrypted using the members private key 23 as discussed above, creating the digital signature 29. This digital signature, then, can tie a particular file to a particular owner of a private key. The member then attaches the digital signature 29 to the file 27 and sends both to the receiver. In this example, the file 27 is sent unencrypted, but if the file must be securely sent, the member can use the method describe in the previous paragraph to encrypt the file with the receivers public key. When the file and signature are received, the receiver deciphers the digital signature 29 using the senders public key 19, revealing the digital pattern 33 unique to the file 27. The public key, as before, is available from a published public key list 25. If the digital signature 29 was made using any other user's private key, the resulting pattern will not match the file, and the receiver will know the file was not sent by the named sender. Using this digital signature technique, the preferred embodiment can place a high assurance that a particular file was sent by a specific member.

Using the techniques described above, there is a high level of assurance that information and business transactions will be made securely and accurately. However, security is only one part of a successful Internet interaction. Presently, interaction on the Internet is an impersonal and often random experience. A common critique of using the Internet is that interacting on-line doesn't allow us to locate, understand and know with assurance the person behind the e-mail ID or message -- to hear the voice, to see the face, to know a little about the senders personality, characteristics, and trustworthiness. Without these, the interaction is not only personally unsatisfying, but frustrating and useless.

Virtual communities are forming but people have little assertive control over their digital persona or interactions and much of the rationale behind these virtual communities is data gathering. This data gathering is performed by commercial entities seeking to track consumers, performing continuous and subtle surveillance of community members. Overwhelmingly consumers want control of their personal information and are demanding change as a backlash is mounting seeking legislation to circumvent this unbridled gathering, trafficking and processing of personal information. The present invention creates a trusted virtual community enforcing informational privacy and informational self-determination, wherein people can individually and corporately demand value in exchange for accessing and processing personal information controlling the many attributes which make up their informational existence.

A digital persona or Internet personality is determined by the personal information available for an individual. The more complete and reliable the information, the more accurately the Internet personality will reflect the real-life personality. This personal information is valuable not only to accurately define an on-line presence, but, as discussed earlier, has commercial value to others. Personal information may take many forms, including health, financial and legal records, school transcripts, employment history, or buying preferences. Each of these pieces of information, if accurate, is an asset that can make interacting on the Internet more effectual and enjoyable. In the preferred embodiment, these information assets are compiled and made available to others according to the desires of the individual E-Metro member. All the personal information, taken as a whole, makes up the electronic presence or digital persona of an individual. For purposes of clarity and ease of explanation, it is useful to think of this electronic presence in a Web site E-Metro Community as an electronic personal information agent or E-PIA, as introduced earlier.

Some of the informational assets of an E-PIA are created and held by others, but can be dispatched or processed in accordance with the rules embedded in the E-PIA, such as medical records and school transcripts. Other assets are those that can be authored by E-Metro Community members. The preferred embodiment allows a member to self-assure or collaboratively assure the information encapsulated within the E-PIA is accurate and reliable.

In Figure 106 a user has accessed an E-Metro Community Web site using Netscape Navigator and is displaying the initial registration application 21. The standard Netscape interface 25 is near the top of the figure. Specifically, the user interface includes a menu bar 25, control buttons 27, quick access tree structure 37, and a communication activity indicator 31. Additionally, the key graphic 33 near the bottom of Fig. 106 tells us that security is in operation, so all communications with the E-Metro Community Web site are encrypted.

The registrant can navigate to other data subject areas (professional, financial, medical) within the notebook shown in the left most scrollable window. If the user selects the professional data area 37, the user will see the professional profile and begin data entry or update the information.

Fig. 107 is a dispatched E-PIA, which is displaying a portion of the personal profile. In Fig. 108 which is the continuation of Dieter's E-PIA the Home Address is not displayed and a closed lock icon accompanies the data attribute to the right. This indicates the person requesting to access this information did not meet his rules for access-processing and Dieter is unwilling to disclose what the rule is governing access-processing. When Dieter completed this personal profile, he authored rules Fig. 109 that determine who gets access to each item of information. The user accessing this personal profile does not satisfy these rules, so Home Address and other information is not available. In the preferred embodiment, if access to information is denied, there may be opportunity to see what the rule is and respond as indicated by the open key icon to the right of Home Phone, Fig. 108.

In this example Dieter has several options for rule processing depending upon Dieter's anticipation of rule interactions and the level of hands-on control he'd like to maintain or entrust to the E-PIA. Dieter may simply wish this requesting user to provide, in exchange, their Home Phone number and so a simple rule interaction will begin. Either processing of this rule will be done at the requesting client site confirming rule satisfaction or the messaging system will be activated with a message sent back to Dieter's Home E-PIA requesting his Home Phone be provided or a signal to his dispatched E-PIA be sent authorizing decryption and display of the encapsulated Home Phone data.

An automated rule-based response can be executed on the client-side given rule interactions are pre-defined and can continue the user-agent dialog or delayed interactions supported by the messaging system will continue the rule interactions. Dieter's Home E-PIA may already have a response established by a rule which says if your show me yours I'll show you mine and so the message response is semi-automatic.

In the case where Dieter has already defined a rule for processing his Home Phone data at the requesting client site the interaction is carried out and triggers a client-side message to Dieter's E-PIA. So, within the requesting user's E-Metro client-side application Dieter's dispatched E-PIA receives a signal to decrypt his Home Phone number for controlled access. The rule interaction Broker within the E-Metro client-side application checks to see if the Home Phone has been properly provided.

In the above case the E-Metro Community E-Broker has dispatched an already loaded E-PIA with encrypted data encapsulated which will save the messaging sending, rule-processing, and hands-on response some overhead by processing the rule right at the client-side. Dieter will decide how trusting he wishes to be in that he can rely upon the system to fetch data in return prior to releasing his data over E-Metro's virtual private network or have the data and rules dispatched within this E-PIA for processing right at the client station.

Rule response dialog boxes display rules and give the requesting person the option to respond. The rule may specify a financial transaction to occur. In this case the user authorizes a debit from their E-Metro wallet for the amount required by the rule.

Rule specifications are authored in Fig. 109. The figure depicts a dialog screen wherein Dieter navigates on the left his PIA's data attributes 545, specifying what kind of rules will govern that attribute or group of attributes. Access groups are a means to group rules by particular communities or sub-communities 540. Initial Contacts is a group Dieter has specified as a sub-community in which his Age attribute rule is not disclosed and this attribute in locked 550 i.e. not revealed in an initial contact scenario.

His other attributes: City, Date of Birth etc. are open and will be displayed upon processing. With this screen Dieter can create a "Need To Know" Prompting where in the requesting user is prompted for a need to know. Dieter will have to process this response himself via E-Metro's messaging system. Some message interactions will be automated by pre-built rule responses such as "I'll Show You Mine If You Show Me Yours rules." So Dieter's Home E-PIA can react to rule messages automatically.

Some data attributes will have Time Requirements in that the E-PIA will only allow so much time to pass for viewing or processing the E-PIA's data. A case in point is that Dieter will only allow 24 hours to pass and then his E-PIA locks itself up (encrypts) in order to prevent further processing.

As shown in Fig. 110 the sub-community Initial Contacts 555 must meet the above rules 565 and 560 in order to process Dieter's E-PIA. So Dieter is specifying the criteria other persons must meet prior to processing his E-PIA.

So community members will send queries to the E-Metro for processing and although a query may have several matches the decision to dispatch the E-PIA which meets the query requirements may not be sent due to the fact the requesting person may not meet the person's rule requirements. In the prior case Dieter's E-PIA was dispatched as the person requesting his E-PIA met the above criteria.

As shown in Fig. 2, the E-Being repository 13 may be anywhere on the Internet, that is, it may be on the same server where the E-Metro Community resides, or the E-Metro

Community may use a E-Being repository residing somewhere else on the Internet. When a member joins an E-Metro Community, one of the first tasks will be to author, according to the users discretion, the personal profiles. These profiles, plus any information from outside sources, comprise the E-PIA representing an individual on the Internet.

A user can belong to several E-Metro Communities in the preferred embodiment. The user must, however, select one of the E-Metro Communities to be the home E-Metro Community. The selected E-Metro Community houses an E-PIA designated to be the "Home E-PIA" which keeps track of all the other E-Communities where the member resides. In this way, a change in the home E-PIA can be used to update the information in all the other E-Communities, if necessary. Once a member has joined an E-Metro Community and designated the E-Metro Community as its home, the member can join another E-Metro Community by simply meeting the admission requirements for the next E-Metro Community and then copying the E-PIA to the new E-Metro Community. As will be discussed in a later section, when a member desires to create a special E-PIA, called an E-AutoPIA, that is capable of moving to other E-Metro Communities and perform requested tasks, the E-AutoPIA can only be spawned from the home E-PIA. The E-AutoPIA, then, has a subset of the information contained in the parent home being, thus assuring anyone encountering the E-AutoPIA that the information it carries is related to a home E-PIA.

A member defines rules for the access-processing of their personal information to assure the information is processed appropriately. When a user tries to access the personal information of a member, the preferred embodiment checks to see if the user meets the requirements for trusted processing of the information. The preferred embodiment only dispatches an E-PIA to the requesting user containing information, which the user is authorized and qualified to process. These rules define the limitations on information processing and form the basis for interaction between E-PIAs in the E-Metro Communities. That is, when a member, represented by an E-PIA, contacts another member's E-PIA, the two E-PIAs can determine what, if any, information can be exchanged without any concurrent input from the represented humans. The specifics of this rule checking is described in a later section.

To this point the E-PIA in the E-Metro Community has been described as simply a storage repository for personal information with the ability to selectively release information according to rules, and acting only within one E-Metro Community. In the preferred embodiment, however, the E-PIA may also take the form of a more active entity, called an E-AutoPIA, capable of substantial unsupervised activity with other E-Metro Communities and E-PIAs in other E-Metro Communities on the Internet in general. The E-AutoPIA contains a subset of the personal information and rules of the full E-PIA, plus an itinerary that directs its activities. The itinerary tells the E-AutoPIA what E-Metro Communities to visit, what information to collect, and, in conjunction with the rules, what information may be processed. Using an itinerary, then, an E-AutoPIA will "move" about the Internet, visiting other E-Metro Communities where it can interact with the E-PIAs in each E-Metro Community.

In the preferred embodiment, the E-AutoPIA does not directly interact with other E-PIAs. Instead, each E-Metro Community has at least one process that acts as a brokering agent between an E-AutoPIA and the E-PIA members of the E-Metro Community. This brokering agent is the E-Broker presented earlier. When two E-PIAs or an E-PIA and an E-AutoPIA desire to interact, both present the E-Broker with their respective rules, and the E-Broker determines what, if any, information may be exchanged. Additionally, the E-Metro Community administrator may set minimum rules that apply to all the E-Broker mediated transactions to occur in that E-Metro Community, assuring that only transactions that meet minimum E-Metro Community standards will occur.

As alluded to, there are two modes of E-PIA Interaction. A user, electronically represented by his member E-PIA within an E-Metro Community, may invoke a single Interaction for an

E-Metro Community via his Netscape Browser and the appropriate HTML document. This is known as *Online Interaction Mode*. When an E-AutoPIA invokes Interactions within an E-Metro Community, this is called *Batch Interaction Mode*.

Fig. 5 conceptually shows a Web site E-Metro Community 35 containing several E-PIAs (members) 37. For any interaction, the members 37 must use the services of an E-Broker 39. The E-AutoPIA 41 can operate external to the E-Metro Community, and as shown in Fig. 6, the E-AutoPIA 41 can have an itinerary that directs it to interact with the E-Brokers 39 in several other Web site E-Communities 35.

The E-Broker has three main functions within the E-Metro Community. First, the E-Broker has been defined by the E-Metro Community administrator to check the credentials of any E-PIA that wants to enter an E-Metro Community. In this policing role, the E-Broker checks certification, verifies identity, and inquires into the purpose of any approaching E-PIA. After applying the rules set by the E-Metro Community administrator, the E-Broker will either deny access to the E-PIA or allow it into the E-Metro Community. Second, the E-Broker acts to search for members that meet the criteria designated by an E-PIA during its request for interaction. For example, if an E-PIA enters an E-Metro Community to find members who are interested in purchasing a car, the request is given to the E-Broker. The E-Broker, using several subsystems available in the preferred embodiment, then searches all the members to find those that have expressed an interest in purchasing a car and creates a list of all members meeting the necessary criteria. Third, the E-Broker acts as an intermediary between the E-AutoPIA and the E-Metro Community E-PIAs. In the above example, even after the E-Broker has created the list of members that express an interest in purchasing a new car, the E-Broker still acts as a mediator. The E-AutoPIA presents its rules for collecting information, and each member E-PIA presents its rules for disclosure, and the E-Broker determines what information, if any, will be exchanged. Of course, even if the two beings agree to exchange information, the E-Metro Community administrator may have set a more stringent rule that will not allow the E-Broker to finish the transaction.

One of the possible tasks that an E-Broker may negotiate is the controlled processing of a member's personal information. Provided both the E-Metro Community administrator and the user want to process personal information, the E-Broker can be instructed to collect money from a visiting E-PIA that wants personal information. In the preferred embodiment, the money collected may go to the E-Metro Community, the member, or split between them. An E-Metro Community with a substantial membership may find this an attractive way to finance other E-Metro Community services.

The E-Metro Community may provide several services to its members. Services may include intra-community functions such as collaboration groups, consensus building or voting systems, capital disbursement systems to manage the community revenues generated from services, on-line customer satisfaction databases to protect consumers promoting accountability and just resolution of customer complaints, or community subsidized provision of advanced wireless communicators to promote 'equal access' policy objectives. The E-Metro Community may also provide extra-community services, such as access to cross-community mobilization efforts for philanthropic or political purposes, joint electronic commerce services, sharing of communication infrastructure costs to facilitate cross-community advanced or newly introduced wireless networks and technology for all community members.

A typical physical arrangement for the preferred embodiment is shown in Fig. 7 where a user 43 accesses the Internet 1 by using a personal computer 45 to connect to a network server 11, and the network server 11 makes the connection to the Internet 1. Both wire-line and wireless connections will be supported with where more than one E-Metro Community can reside on one network server 11, and E-Metro Communities may even form a hierarchical relationship. That is, an E-Metro Community may contain not only members, but may contain other sub-communities as well. Fig. 7 shows network servers 11 with one, two, or three E-Metro Communities on each server. Additionally, E-Being objects for authoring member information for the particular E-Metro Communities may be requested from the E-Metro Community E-Broker or, if made available publicly, in the E-Being repositories 13. The preferred embodiment allows any public storage subsystem for E-Being objects. Two possible storage subsystems are an FTP site or a Mail server which is simply a file storage and communication system holding assorted file types and is available off the shelf from Netscape or other vendors. These E-Being repositories may be on any server 11 or 13, or the E-Being objects may even be held by user at their personal computer 45 or a wireless Communicator device 42.

We now turn to the specific software implementation for the preferred embodiment. The preferred embodiment is a modularized application, that is, the application is divided into several parts, with each part, or module, assigned specific functions. Some of these modules are designed to operate on one or more network servers, while other modules are designed to operate on a user's local computer system. The user and server processes necessary to the preferred embodiment are shown in Fig. 8, and are associated with the physical devices shown in Fig. 7. Referring to both diagrams, the user 43, from their personal computer 45, runs the Netscape Navigator Web Browser 49, a commercially available application. The Netscape Navigator 49 allows the user to conveniently access any E-Metro Community Web site. Also, the Netscape Navigator provides compatibility with other Netscape products that bring specific tools to the preferred embodiment. Besides the Netscape Navigator, the user locally runs several utilities 55 in support of E-Metro Community activities. These specific applications may be DLLs (Dynamic Link Libraries), Java applications, applets and scripts, or some other code of a similar nature that supports specific E-Metro Community activities. As mentioned earlier, however, in almost all cases, additional subsystems and DLLs should not be necessary.

The heart of the preferred embodiment is the Web site E-Metro Community system 47, which operates on the network servers 11. A top level view of the Web site E-Metro Community system 47 architecture is shown in Fig. 9. The system comprises the Distributed Object Resource Management System (DORMS) 57, which is shown in more detail in Fig. 10, a Netscape Enterprise Server 59, the Netscape Application Programming Interface 67, a LivePayment payment card transaction processor 61, an FTP server 65, and an FTP client 63. Each of these system components will be individually discussed below, and then their interaction explained, but first the important consideration of security will be addressed.

Strict security is necessary in order to ensure that only intended communications and information dissemination occurs. Security can be divided generally into two categories: 1) security mechanisms to assure that eavesdroppers or accidental recipients cannot access information, and 2) security measures to assure that information is only released to a trusted entity. The first type of security is accomplished by using cryptographic techniques to transfer data between entities. Referring to Fig. 24, several Web site E-Metro Community systems 47 and a user accessing the preferred embodiment with the Netscape Browser are shown. Each Web site E-Metro Community system 47 is operating on a network server as a secure process. It is expected that anyone skilled in the art of process security can create a local secure process for each Web site E-Metro Community system 47. For inter-community communications, each Web site E-Metro Community system 47 maintains its own private key and public key for encryption use.

When a source E-Metro Community wants to communicate with another target E-Metro Community, such as when an E-PIA is transferred, a double encryption technique is employed. The source E-Metro Community encrypts the message using the public key of the target E-Metro Community. The source E-Metro Community then encrypts the now encrypted message again, but this time with its own private key. Each E-Metro Community is aware of all other E-Communities and their public keys. When the target E-Metro Community receives a message, it first decrypts the message with the public key of the source E-Metro Community and then it decrypts the message with its own private key. This "double" encryption assures the target E-Metro Community that the source E-Metro Community was indeed the source E-Metro Community mentioned in the message and also assures the source E-Metro Community that only the target E-Metro Community will be able to decrypt the message intended for it. Similar security measures are used for communications from an E-Metro Community 47 to a user.

Another important security aspect concerns assuring the source of an E-PIA or E-AutoPIA. This assurance of origin is shown through the use of a Certificate 150 and TrustedToken 159. Certificates are held by all E-PIAs and E-AutoPIAs, and contain the name of the person or entity represented and their associated public key. Since the personal information held by an E-PIA or E-AutoPIA has been encrypted by the private key of the person or entity represented, if the public key in the certificate matches the published public key, and the personal information correctly deciphers, then there is certainty that the E-PIA or E-AutoPIA originated from the stated source. The Certificate, then, is to assure that a being represents who they say they represent and the information was originally encrypted by that representative. The TrustedToken represents a necessary privilege to perform an Interaction, given by an E-Broker at E-PIA or E-AutoPIA authoring time. Each Interaction that needs to be secured will require that a TrustedToken be issued. Before an E-Broker will act on a requested Interaction, it will check to see that the requesting E-PIA has the necessary to assure that the E-Broker had granted privilege to perform the Interaction previously. Each TrustedToken will be associated with a specific Interaction and will be encrypted by the requesting E-PIA's private key. By using the requesting E-PIA's known public key, the TrustedToken can be decrypted and compared to the expected value, thus giving assurance that the ability to request the Interaction was actually granted specifically to the requesting E-PIA.

The second security mechanism assures that information is only released to trusted entities. When an E-PIA gives some of its personal information to another, the personal information given is still secured and owned by the original E-PIA, so subsequent dissemination can be controlled. The mechanisms concern initial release of information and subsequent dissemination by others. The initial release of information is controlled by having both the Web site E-Metro Community administrator and the individual set rules which must be met before information can be released. The E-Metro Community administrator can set rules that generally apply to all potential exchanges in the Web site E-Metro Community, allowing the E-Metro Community to maintain control on the types of acceptable transactions. Also, the individual can assign a rule to each piece of personal information in their E-PIA. By setting these rules, the E-PIA will only share information in a trusted environment with a trusted being. A more difficult issue relates to control over subsequent dissemination of information. In fact, if the receiver of the information, in turn, passes the information on to a third E-PIA, the preferred embodiment still retains knowledge of the original owner of the personal information and continues to police access to the information. This subsequent security is set by Transitive Privilege Rules declared by the original E-PIA. The transitive privilege rules create a transitive trust such that: If A trusts B with information X, and B trusts C with information X, then A trusts C with information X. This important concept assures to A that its information is never passed on to an entity which it does not trust according to the Transitive Privilege Rules it has declared for the data it has submitted. Information is always passed as a version of the E-PIA which submitted its information. For example, suppose an E-PIA contains a rich set of information which includes birth date, address, phone number, etc. Further, suppose it wishes to release only its phone number to another during an interaction. The receiving entity will actually receive an E-PIA object informational E-PIA, which contains only the phone number. More specifically, the E-PIA object received is a version of the original E-PIA which represents how the submitting E-PIA wishes to be perceived by the receiving entity. Figure 6 depicts the collection of versions 40 of E-PIAs by a traveling E-AutoPIA. The versions of E-PIA objects is the only manner in which information is exchanged in the preferred embodiment.

The Distributed Object Resource Management System (DORMS) is central to the operation of the Web site E-Metro Community system 47. As shown in Fig. 9, the DORMS 57 handles several core activities for the system, including storing of E-Metro Communities, E-Brokers, and members, E-PIAs maintaining a directory of all E-Metro Communities on the Internet, holding auto beings, and handling the interaction between E-PIA and between E-PIAs and E-AutoPIAs. Each of these activities will be discussed below.

The activities of the DORMS 57 are implemented with a series of interrelated subsystems, as diagrammed in Fig. 10. The interaction processor 73 is the key subsystem for the DORMS 57, and is responsible for all external communication and most internal decisions. Once the interaction processor 73 decides on a particular course of action, the action is implemented by the use of an E-Broker process. There are several E-Brokers available to do specific, reoccurring tasks. The operation of the interaction processor is discussed in detail in a later section, but first the other DORMS functions and individual subsystems will be addressed.

The DORMS is responsible for the storage of the E-Metro Communities, E-Brokers, and E-PIAs. Although each of these items is quite different, they are all stored in a common structure within the Object Repository 75. The Object Repository 75 employs a simple object oriented interface over a relational database. The relational database can be any that operates on the network server, such as the popular Oracle Database system.

E-Metro Communities, E-Brokers, and E-PIAs are all objects in the preferred embodiment, with each instance of an E-Metro Community, E-Broker, or E-PIA assigned a unique Object Identifier, or OID 91. The characteristics are then stored with the OID 91 in the form shown in Fig. 11a. This figure shows the structure of each row of a table within a relational database. Referring to the figure, the OID 91 is in the first field. The next field, the CollectionOID 93 identifies if this object is included in any other object, allowing for the creation of relationships between objects. Using a common CollectionOID 93, for example, several E-Brokers, E-PIAs, or even other E-Communities can be associated with a single E-Metro Community. The CollectionOID 93, then, is the preferred embodiment's method for tracking the hierarchical relationships between E-Communities, and the method for tracking E-Broker and E-PIA assignment within a particular E-Metro Community. Following the CollectionOID 93 are several key fields 95 that contain selected information about the object. These fields are "keys" that may be used for search and selection criteria by the database program. In the preferred embodiment, six key fields 95 are allowed for each row in the database table. Of course, more or fewer keys could be used, or alternate search techniques are clear to those skilled in the art. The specific identity of the keys is left to the E-Metro Community administrator to assign, thus allowing E-Metro Community needs to direct the most effective fields for efficient searching. The last item in the row is the object itself, which is stored in BLOb (Binary Large Object) format. BLOb format is a standard database storage structure that allows a single field in a database to hold multiple pieces of discrete information and is unaffected by the content of each piece of information. Thus, the DORMS can search the key fields 95 in the object repository 75 to quickly select appropriate objects, then extract and view the objects themselves from the BLOb format, a much slower operation.

As stated above, E-Metro Communities, E-Brokers, and E-PIAs use this common row structure. Each, however, uses a slightly different naming convention. The convention used by the E-Metro Community is shown in Fig. 11b. Notice the CollectionOID 93 references a parent E-Metro Community by the ParentOID 99, if any. In this manner the preferred embodiment maintains the hierarchical structure for the E-Metro Communities. The only additional difference is that the first key field 95 is assigned to hold the name of the E-Metro Community. Since the database engine often will use the name of the E-Metro Community for searching, it is appropriate that the name be a dedicated key for all E-Metro Community objects.

The row structure for an E-Broker is shown in Fig 11c. Just as with the E-Metro Community, the first key field 95 is a name, in this case it is the name of a specific E-Broker. However, the CollectionOID 93 field contains the OID of the E-Metro Community that "owns" this E-Broker, thus associating a particular E-Broker with a specific E-Metro Community using a CommunityOID 101. This association method allows an efficient method to know which E-Brokers are allowed to operate in an E-Metro Community. Additionally, this same association method is carried through with the row structure for the E-PIA, which is shown in Fig. 11d. In the E-PIA, the CollectionOID field contains the Metro CommunityOID 101, thus associating a particular E-PIA with a specific E-Metro Community. As can be seen in Fig. 11d, all six keys are undefined in the E-PIA row structure, allowing the E-Metro Community administrator the flexibility to define each field to meet specific E-Metro Community needs.

Referring again to Fig. 10, the DORMS 57 also maintains a current directory of all E-Communities on the Internet. This directory is maintained by a special E-Broker in the E-Metro Community called the Directory Broker 77, with every E-Metro Community having a Directory Broker 77. The Directory Broker 77 tracks all E-Communities on the Internet and their address.

Additionally, the Directory Broker 77 holds information on all other E-Brokers in all other Internet E-Communities. Information held includes the E-Broker's name, rules, and other information the E-Metro Community administrator desires to keep about other Internet E-Brokers. To keep the directory information current, an E-Metro Community's Directory Broker 77 will periodically inquire to see if its E-Metro Community has added, deleted, or changed any E-Brokers or E-Communities, and if so, the directory E-Broker 77 will launch an E-AutoPIA. This E-AutoPIA will be sent to all other E-Communities to interact with their Directory Broker, updating each E-Metro Community with the changes. The frequency of this update will vary, but most likely a schedule of once-per-day updating will be sufficient to support accurate E-Metro Community interaction.

The DORMS 57 also contains a Messaging system 71 that allows the E-Metro Community to send an E-AutoPIA to another E-Metro Community. As can be seen from this figure, the DORMS 57 communicates with other remote E-Communities through the FTP client 63 and the FTP server 65. Although the FTP processes are shown connected directly with the Messaging subsystem 71, all actual communication is controlled by the interaction processor. A more detailed diagram of the Messaging Subsystem is shown in Fig. 12. As discussed earlier, the Messaging subsystem 71 uses the FTP protocol to conveniently send and receive messages from or to the Web site-based E-Communities. This Messaging subsystem is employed exclusively for transporting E-AutoPIAs from one E-Metro Community to another. When an E-AutoPIA is sent to another remote E-Metro Community, the interaction processor 73 first retrieves the address of the remote E-Metro Community using the directory E-Broker 77. The interaction processor 73 then bundles the E-AutoPIA with the remote address and forwards the bundle to the sender dispatcher 105. The sender dispatcher 105 places the message in the message queue 109 and notifies the FTP client 65 that a message (an auto-being bundled with an E-Metro Community address) is ready to be sent. At a convenient time, the FTP client 65 sends the message (the auto being bundled with the address) to the FTP server of the receiver E-Metro Community and subsequently erases the outgoing message for the message queue 109. For an in-coming E-AutoPIA, FTP server 63 accepts the message and places the message in the message queue 109. The receiver dispatcher 107 monitors the message queue 109, and when a new message is seen, it unbundles the message, revealing an E-AutoPIA. The receiver dispatcher 107 then notifies the interaction processor 73 that a new E-AutoPIA has arrived, and the interaction processor 73 determines what next to do with the E-AutoPIA. The incoming message in the message queue 109 is not deleted until the E-AutoPIA in that message has completed its tasks within the E-Metro Community and has left the E-Metro Community. Saving the incoming messages assures that the E-AutoPIA's assigned tasks will be completed, even if the DORMS server should shut down in error and lose the E-AutoPIA currently active in the network server. When the network server is restarted, the E-AutoPIA can be restarted from the original message and its tasks completed. The message queue 109 itself is a standard FTP file system which may comprising an incoming message file and an outgoing message file. It will be clear to those skilled in the art that other transfer methods .may be substituted for the FTP process described above.

The Virtual interpreter 81 is a software subsystem that provides the ability to execute the script language and rules language of the preferred embodiment. The Virtual Interpreter 81 plays a major part in the use of the rules processor 79 and the Itinerary processor, both which are discussed in a following section.

The DORMS 57 contains a Rules processor 79, which is an important subsystem for ensuring that information is securely distributed. A member or the E-Metro Community administrator uses rules to set the limitations and controls on the distribution of personal information. The rules are actually a series of strings, written in the programming language chosen for the preferred embodiment, that defines the requirements under which information will be released. It is possible to make the rules as simple or as complex as needed. The E-Metro Community administrator may provide minimum rules that will apply to all transactions, and allow the member to adjust rules for their particular needs. Although the preferred embodiment uses an application to set rules, those skilled in the art will recognize several alternative methods for a user or administrator to input rules.

As discussed earlier, requests for a member's personal information may come from either of two sources: another E-PIA member or an E-AutoPIA via Online Interaction mode or Batch Interaction Mode, respectively. If an E-AutoPIA enters an E-Metro Community and requests a member's information, the interaction processor 73 will start an E-Broker process to handle the request. The process to handle such a request is detailed in a later section after all subsystems have been describe, but generally, the E-Broker takes the rules that define the E-AutoPIA's request criteria and sends them through the virtual interpreter 81 and into the rules processor 79. The rules processor 79 converts the request into a standard database query request, such as a standard SQL SELECT command, and runs the query to select E-PIAs from the object repository 75. The E-Broker then accesses each selected E-PIA's rules, sends then through the virtual interpreter 81, to the rules processor 79, and the rules processor 79 compares the requirements set by the member E-PIA to the characteristics of the E-AutoPIA, and if the requirements are met, the E-Broker sends the requested information from the E-PIA to the E-AutoPIA.

If another member of the same E-Metro Community requests information on another member, the process is similar, although much simpler. In this case the interaction processor 73 again starts an E-Broker process, and the E-Broker sends each E-PIAs' rules through the virtual interpreter and finally to the rules processor 79. The rules processor compares the rules for each member and determines what, if any, information may be disseminated.

As previewed earlier, an E-AutoPIA is instantiated from a user's E-PIA and includes an itinerary. The itinerary is a set of instructions that direct the activity of the E-AutoPIA. Thus, the E-AutoPIA acts as an agent for the user. The itinerary, like the rules, can be a program written in Java, or other convenient language chosen for the preferred embodiment. As with the rules, those skilled in the art will recognize several alternative methods to creating an itinerary to direct an E-AutoPIA.

The Virtual Image 85 is used to improve the performance of the preferred embodiment by placing selected information in local RAM (Random Access Memory) for quick access. Since the system can access information in RAM much faster than it can retrieve information from a data base located on a hard drive, such as the Object Repository 75, the system runs more efficiently. Once an E-Metro Community, E-Broker or E-PIA is needed by the preferred embodiment, an E-Broker selects the needed entity from the object repository 75 and places a copy of the entity in the virtual image 85. From then on, the system uses the copy in the virtual image 85 rather than the original in the object repository 75.

As can be understood from a previous discussion, E-Brokers are processes that execute on the network server and are used within an E-Metro Community to assist in the orderly and efficient functioning of that E-Metro Community. Each E-Metro Community has at least one E-Broker, but may have more. Two special E-Brokers exist in the preferred embodiment, but there may be more. The first one is the mandatory directory E-Broker 77 and was discussed earlier. The second one must be present in E-Communities that require secure modification access to the E-PIAs and is called the Home E-Broker 87. The home E-Broker is responsible for assuring that only the owner of an E-PIA has edit access to his home E-PIA. The home E-Broker may be set to require very strict security access, such as having the member use a secure card, passwords, and challenge system, or may be set up with weak security, such as just having the member supply a proper member identification name.

Each E-Broker is a custom built executable that runs in the Web site. Each E-Broker executable 76 implements a specific set of E-PIA interaction choices provided by the E-Metro Community it resides in. When an E-PIA requests a specific interaction, the Interaction Processor 73 invokes the E-Metro Community's E-Broker and tells it to attempt the requested interaction. In order for the Interaction Processor 73 to communicate with each E-Broker executable with a unified communication protocol, E-Broker Adaptors 74 are employed. Thus, the Interaction Processor 73 actually communicates with an E-Broker Adaptor 74 specially built for the E-Broker executable which, in turn, communicates with the E-Broker executable 76. Thus, the E-Broker Adaptor 74 acts as a "bridge" for communication between the Interaction Processor 73 and an E-Broker executable. This adaptor mechanism is necessary since E-Brokers constructed from C, C++, Java, Visual Basic, PowerBuilder, or other development environment may require different means for invocation and information transfer.

As a means to assist the construction of all necessary activities that an E-Broker executable may need to perform, the E-Broker Service API DLL is provided as part of the DORMS server subsystem. E-Brokers must be capable of calling APIs in a DLL to employ these helpful services. Some services that have been identified are: 1) input a set of rules and output a list of E-PIAs in the current E-Metro Community that satisfy the rules; 2) interact with the Transaction Server to perform credit card processing; 3) bill a credit card; 4) validate a Security Card that is entered on-line. It should be clear to those skilled in the art that other APIs may be added as needed.

Referring to Figure 9 again, so far the DORMS 57, FTP client 63, and FTP server 65 portions of the Web site E-Metro Community System 47 have been discussed, with the LivePayment

Server 61, Netscape Enterprise Server 59, and Netscape API 67 yet to be detailed.

The LivePayment Server 61 is a commercially available application from Netscape that handles payment card transaction processing, event logging, and settlement. The LivePayment Server 61 will be customized to handle E-Metro payment card transactions. Anytime a transaction by an E-Broker involves the transfer of money or value, the E-Broker sends the information to the Interaction Processor 73, and the Interaction Processor 73 forwards the data to the customized LivePayment Server 61. Additionally, when the customized LivePayment Server 61 needs to send information to an E-Broker, as for credit card approval notification, the customized LivePayment Server 61 sends the data to the Interaction Processor 73, and the customized LivePayment Server 61 forwards the information to the proper E-Broker. Individual E-Brokers and E-PIAs can define their own billing policies, allowing a member or the E-Metro Community administrator to collect fees for the release of information. As an example, the E-Metro Community administrator could set a charge of $1.00 per name and telephone number released, but an individual could add a requirement that they receive $0.25, too. This raises the cost to $1.25 if an E-AutoPIA wants to utilize that user's name and phone number. Since the customized LivePayment Server 61 is aware of all financial transactions in the E-Metro Community, it can easily create accurate billing and financial summaries.

The Netscape Enterprise Server 59 is also a part of the Web site E-Metro Community system 47. This server is a standard commercial offering from Netscape, and when run on a network server allows that network server to be a Web site, communicate over the Internet, and efficiently interact with the Netscape Navigator. The Netscape Navigator, as discussed earlier, operates on a user's personal computer and is a client to the Netscape Enterprise Server 59.

The standard Netscape Enterprise Server 59, while providing the basic tools for allowing a network server to be a Web site and gain access to the Internet, must be enhanced to provide the services and tools necessary to support the E-Communities of the preferred embodiment. The Netscape Enterprise Server 59 can be modified using the Netscape API 67 (Application Programming Interface). The Netscape API 67 is a set of commands that can be accessed from any program to perform modified Enterprise Server 59 functions. In the preferred embodiment, the Netscape API 67 is used to modify the standard security measures and method for responding to requests, for example.

Now that all the systems and subsystems have been described, a specific example will be used to demonstrate system interaction. For this example, assume that a remote user has created an E-AutoPIA to enter the example E-Metro Community to retrieve information on selected members of the E-Metro Community. Refer to Figures 7, 8, 9, 10, and 12 for the following procedure sequence. For convenience, the steps are organized into preliminary steps that will only be done once to initialize the E-Metro Community, and request handling steps that are repeated each time an E-AutoPIA requests E-Metro Community information.

Preliminary steps:

1. An E-Metro Community administrator loads the preferred embodiment on a network server 11. This administrator employs an E-Metro Community administration tool to install the E-Metro Community. The administrator also creates several E-Brokers for handling tasks such as requests from E-AutoPIAs or transacting financial business. The E-Brokers may be constructed by modifying an existing E-Broker or by writing a new E-Broker process in any programming environment that can be "adapted" with the E-Broker Adaptor mechanism. The administrator additionally defines what services (interactions) to make available to members and creates the screens to present the information to the members. The latter is done with the standard Netscape Enterprise Server 59 or any other tool that can create Web site pages. The administrator either creates or modifies existing admission forms and places

the forms in a forms-object repository 13. The forms repository 13 can be on the same network server 11 as the E-Metro Community, or may be placed on any available remote network server 11. Finally, the E-Metro Community administrator brings the E-Metro Community on-line and begins announcing the presence of a new E-Metro Community. The E-Metro Community is now ready for members.

2. Internet users or members of other E-Communities become aware of the new E-Metro Community and access the E-Metro Community's Web site address to get more information. Using the Netscape Navigator 49 Browser on their personal computer 45 they join an E-Metro Community. They can access admission forms and submit the requested information. At this point, the administrator may manually check the admission forms for completeness and minimum E-Metro Community requirements, or more likely, the administrator will have an E-Broker automatically check the form for the minimum requirements and set an in-person appointment with the user if the forms are acceptable. Depending on other requirements set by the E-Metro Community Administrator, the user may then be notified to come down to the E-Metro Community administrator's office or some other trusted authority and present sufficient identification and records to convince the administrator that the user is who they say they are. If E-Metro Community requirements dictate that security measures be maintained, then the user may be issued passwords, a secure-card, or other security mechanism. If all is in order, the user will become a member of the E-Metro Community. If the member has chosen the E-Metro Community to be his/her Home E-Metro Community, they must input a complete personal and professional profile, including compiling records held by others, such as medical and legal records. When the E-Metro Community is not the member's Home E-Metro Community, only a subset of information needs to be submitted and should be directly derived from the new member's Home E-PIA wherever it may reside. Several other users may also become members of this E-Metro Community.

3. At this point there is a going-concern E-Metro Community with active members. Members can take advantage of E-Metro Community services, communicate with other members, or create an E-AutoPIA that can go out and browse other E-Communities. The member may also define the rules for releasing personal and professional information, including the ability to charge for such release, or even require that the other side release similar information. There is such flexibility because the member creates the rules by writing a program in a language compatible with the E-Metro Community. Forms are available in the forms repository 13 to assist in the creation of rules, and the E-Metro Community administrator may even provide a default set of rules that simply need to be modified. Also, the E-Metro Community administrator is likely to create a set of minimum rules that will apply to all transactions to assure that an E-AutoPIA meets certain minimum standards and all transactions within the E-Metro Community are conducted in a proper manner. These minimum rules that apply to everyone can be called the E-Metro Community rules.

Request Handling:

4. Suppose that at this point an E-AutoPIA arrives at the FTP server 65 from another E-Metro Community. The server places the message in the Message Queue 109 and subsequently the Receiver dispatcher 107 recognizes that a message was received. The receiver dispatcher 107 notifies the interaction processor 73 that an E-AutoPIA message is waiting in the message queue 109 and retrieves the message containing the E-AutoPIA, but does not erase the original copy from the message queue 109. The Interaction Processor will retrieve the message from the receiver dispatcher and unbundle the E-AutoPIA from the message. The interaction processor 73 then starts an E-Broker process to handle the interaction requested by the E-AutoPIA. Since the E-AutoPIA is encrypted, the E-AutoPIA must be decrypted using the public key of the source DORMS server and private key for the local DORMS server. If the E-AutoPIA was intended for this E-Metro Community, it will properly decipher. Each E-AutoPIA also contains a Certificate

to assure that the owner of the E-AutoPIA actually initiated the sending of the E-AutoPIA, which was discussed in an earlier section.

While the E-AutoPIA is present in the E-Metro Community, the E-Broker places it in the virtual image 85 for easy access. The E-Broker then collects the rules from the E-AutoPIA, and using the virtual interpreter 81 and the rules processor 79 checks the rules against the E-Metro Community rules to see if this E-AutoPIA should be allowed to interact with members. If not, the E-Broker will send the E-AutoPIA to the sender dispatcher 105, and the sender dispatcher 105 will send the E-AutoPIA back to its Home E-Metro Community. However, if the E-AutoPIA satisfies the E-Metro Community rules, the E-AutoPIA will be allowed to interact with member E-PIAs. Additionally, the E-AutoPIA may be holding E-PIA data that is intended to be E Communicated or shared. If so, the transitive privilege rules of each E-PIA is checked in a similar manner, assuring that the E-PIA will only be shared if the transitive privilege rules taken from the original E-PIA are met.

5. If the transaction has progressed to this point, the E-AutoPIA has a high probability of originating from where it says it does, and the E-AutoPIA meets the general rules for further engagement. Now, the preferred embodiment begins to analyze each requested interaction. The E-AutoPIA sends its first request and a TrustedToken to the E-Broker, where the E-Broker verifies that the E-AutoPIA holds the TrustedToken for the specific requested interaction. If the TrustedToken passes this test, the request is retained and moves on to step six; if not, the request is discarded.

6. The E-Broker takes the request and again processes the rules for the E-AutoPIA with the rules processor 79, but this time to create a query into the object repository 75 to find E-PIAs that meet the criteria set by the E-AutoPIA. Once the rules processor 79 develops this search, a SQL query, the E-Broker process runs the query on the object repository 75 and places the selected E-PIAs in the virtual image 85.

7. The E-Broker now collects the rules from each E-PIA, sends the rules through the virtual interpreter 81 and to the rules processor 79. The rules processor 79 then compares the E-PIA's rules and characteristics, the E-AutoPIA's rules and characteristics, and the E-Metro Community's rules and reports to the E-Broker what, if any, information can be exchanged between the E-AutoPIA and the E-PIA. Once notified, the E-Broker then sequentially collects the necessary information, including any transitive privilege rules and billing information, from each E-PIA, and creates an informational-being. Each E-PIA contains the certificate from the original being, the selected personal information, and the transitive privilege rules. The informational beings are then passed to the collecting being. If any billing information is collected, or credit card authorization is needed, the E-Broker interacts with the LivePayment Server 61 to satisfy these needs. The above process is repeated for each selected E-PIA, or, if the E-AutoPIA has a rule that only allows a set number of interactions, until that number is met.

8. After collection of the information, the E-AutoPIA's tasks at this E-Metro Community are completed, so the E-Broker removes the selected E-PIAs from the virtual image 85. The E-Broker looks at the itinerary from the E-AutoPIA, and using the itinerary interpreter 83 and the virtual interpreter 81 determines the E-Metro Community where the E-AutoPIA should next be sent. The Interaction Processor contacts the directory E-Broker 77 to find the address associated with the next E-Metro Community, and the directory E-Broker 77 retrieves the address from the E-Metro Community directory in the object repository 75, and answers the address to the Interaction Processor. The Interaction Processor then bundles the E-AutoPIA and the address into a message. The Interaction Processor passes this message to the sender dispatcher 105, and the sender dispatcher 105 places the message in the message queue 109 and notifies the FTP client 65 that there is a message waiting to be sent. The FTP client 65 retrieves the message form the message queue 109 and sends the message.

Since the E-AutoPIA has been sent out of the E-Metro Community, the sender dispatcher 105 now removes the original incoming message from the message queue 109. With the E-AutoPIA successfully handled, the Interaction Processor's current session ends.

Now that the interactions of all processes and objects in the preferred embodiment are understood, it is important to describe a specific and important example of an implementation of a type of E-Metro Community known as the "E-Bazaar." The focus of the example is the E-Broker implementation because it is an E-Broker that contains all of the machinery and maintains the behavior of an E-Metro Community. This E-Bazaar E-Broker maintains unique properties that are original to the extent that they are included in the claims of the invention.

E-Broker Example: The E-Bazaar

The E-Bazaar is a type of E-Metro Community that offers three useful commercial scenarios or case studies. While serving as an example E-Broker, the E-Bazaar E-Broker is also very complex. The three case studies are general privacy enabled commerce, semi real-time auction, and large quantity sales. In all three cases, the salient objects are E-PIAs acting as sellers, E-PIAs acting as buyers, and an E-Broker. Note that an E-PIA may also be an E-AutoPIA in this context. The E-Broker handles various public services and Interactions directly on behalf of the E-Bazaar, as well as mediate the Interactions between E-PIAs. An important purpose of the E-Broker is to validate that commercially interacting parties satisfy each others privilege rules for interacting. In the context of this document, the term trade shall be used to refer to a generic notion of either "buy" or "sell." Additionally, the term advertiser shall be used to refer to someone who publicizes a desire to trade. The term shopper shall be used to refer to someone who browses advertisements and who may eventually place an order to trade.

The privacy enabled commerce case provides a means for both buyers and sellers to:

advertise a desire to trade

actively place an order for a trade
fulfill an order for a trade.

When the trading interaction occurs, it is guaranteed to be performed securely and in privacy between buyer and seller according to all the privilege rules configured by both parties. The actual trade activity is what is privacy enabled.

The semi real-time auction case is the same as the privacy enabled commerce case except that a seller or buyer has decided to advertise an electronic auction. In this case, the goods or services are typically advertised along with the current bid so other potential bidders know what to beat. However, auctions may be performed with secret bid.

The large quantity of sales case is also the same as the privacy enabled commerce case except that a seller or buyer has decided that it won't trade unless it can trade a certain quantity of goods or services. Therefore, a placed order may not be fulfilled immediately.

It will be shown that the E-Bazaar is able to perform each of these three case studies with the identical framework in the invention, the subject of a later discussion. It will be shown that the primary distinguishing feature between each scenario is the manner in which an order for buying or selling is fulfilled.

E Bazaar Activity Model

An overview of E-Bazaar activities is best described by presenting the activities lifecycle of an E-Bazaar when employed in E-PIA Online Interaction mode. An enumeration of the Online mode activities in the lifecycle are listed below. Refer to Fig. 201.

1. An Internet Client 303 (as E-PIA) interested in buying or selling a product interacts with the E-Bazaar E-Broker 301 by submitting all of the information about the product so that the E-Bazaar can make the information public to other buyers and sellers.

2. An Internet Client 303 (as E-PIA) browses the product and service offerings at the E-Bazaar.

3. ProductInfo 317 for a specific E-PIA advertiser's product can be obtained upon request.

4. An Internet Client 303 (as E-PIA) obtains the OrderForm 315 for a product it is interested in from the E-PIA advertising the product.

5. An Internet Client 303 (as E-PIA) fills out the OrderForm 315 and submits the filled out form to the E-PIA advertising the product.

6. The filled out form is processed by a process designated by the advertising E-PIA known as the OrderProcessor 319. The process may or may not complete the order immediately. The client E-PIA is either immediately notified of a fulfilled order or notified of an order which is in progress. Such an order is said to be fulfilled asynchronously at some later point in time.

7. For asynchronous order fulfillment, the client E-PIA is notified of a fulfilled order or otherwise when the client E-PIA requests order status later, or receives e-mail regarding status.

For E-AutoPIA Batch Interaction mode, the activities are identical except that the sequence of Interaction activities would be performed according to the E-AutoPIA's Itinerary. For an E-AutoPIA advertiser, the E-AutoPIA would submit product information to the E-Bazaar E-Broker as part of its Itinerary and typically proceed to another E-Metro Community. However, for an E-AutoPIA shopper, the Interaction sequence in the E-Bazaar would typically be quite different. Since E-AutoPIAs tend to automate Interactions, it would be most likely that it already has a copy of order forms it needs. It just needs to submit filled in order forms. Thus, the E-AutoPIA would avoid browsing and a request for an order form and simply place orders. For asynchronous fulfillment orders, the E-AutoPIA can check on status in its Itinerary later, or the person representing the E-AutoPIA can wait for Internet e-mail.

E-Bazaar E-Broker Administration Tool

The E-Bazaar Administration Tool primarily provides the following "birth" features:

1. The E-Bazaar Administration Tool is used to deploy an empty E-Metro Community representing the E-Bazaar in a WebServer containing the preferred embodiment.

2. The E-Bazaar Administration Tool is used to configure the empty E-Bazaar.

The E-Bazaar Administration Tool assists an Administrator in getting an E-Bazaar ready for commerce. The primary task is to decide on which attributes are the most important for all goods and services that will be traded in the E-Bazaar. Such attributes are known as the E-Bazaar's public attributes. For example, some attributes such as brand (advertiser E-PIA name) and price are always of interest. The E-Bazaar Administration Tool will suggest always including these attributes. Other attributes may only be interesting to a particular kind of E-Bazaar. For example, an E-Bazaar that deals exclusively with wine bottles would typically include year as a public attribute. However, if the E-Bazaar deals with many different products where year is not appropriate for all of the products, then a wine product in the same E-Bazaar would have to employ a private attribute assigned only to the wine product. Note that all attributes may be associated with any rule expression governing type restrictions or other general restrictions such as value ranges.

The E-Bazaar may also assist in configuring the product list before commerce commences. Products are organized by category and type. A category represents a group of products that have similarities. For example, in a "Milk" category one might find product types such as quarter gallons of milk, half gallons of milk, gallons of milk, as well as possibly cream or even cheeses. In this example, the milk, cream, and cheeses are product types within the product category. Finally, each product has its own productId, a number assigned by the E-Bazaar Administration Tool. An InteractProtocol exists on the E-Bazaar E-Broker so that products may be added at runtime.

E-Bazaar E-Broker Subsystem Architecture

As mentioned earlier, an E-Broker 301 executable may be any subsystem which can execute in the preferred embodiment. In the E-Bazaar E-Broker case, the executable is very complex consisting of databases, files, and dynamically changing subsystems depending on the E-PIA being interacted with. In the actual implementation, the subsystems may be an EXE which invokes several DLLs, a Java Application, or any other alternative which maintains the suggested subsystem architecture presented below.

Fig. 201 primarily depicts the subsystem architecture of the E-Bazaar executable. It also shows a simplified view of the Internet Client/E-Bazaar executable interaction. The Internet Client actually communicates with the DORMS Server via HTTP which, in turn, invokes a series of Rules processing and interpretation, as well as security verification. After such processing, the E-Broker executable is finally invoked.

As shown in Fig. 201, the architecture of the E-Bazaar executable is such that there is an E-Bazaar Community Info Encrypted File 309, a Commercial Activity Dispatcher 305, a TrustedToken Processor 307, a "Public Product Database" 311, and other "Runnables" (contained in the Advertiser Directory 313) for each Advertiser where each Advertiser has its own OrderProcessors 319, ProductInfos 317, and OrderForms 315 which it maintains to trade its products. Finally, each Advertiser will need to maintain its own "Private Activities Database" 321.

The E-Bazaar Community Info file 309 contains information to manage various aspects of the E-Bazaar. During actual development, this file may be found to be a convenient place to store additional information.

The Commercial Activity Dispatcher 305 is the main subsystem of the E-Bazaar. It handles all incoming Interaction requests, which involves processing and controlling the flow of information from and to all subsystems, files, and databases as necessary. More specifically, it processes many of the requested Interactions with the E-Bazaar E-Broker 301 proper, and it is also responsible for invoking the necessary E-Broker Service APIs 72 for specific E-PIA Interaction determination.

The TrustedToken Processor 307 remembers public keys of E-PIA visitors, issues TrustedTokens, and validates TrustedTokens presented by those E-PIAs attempting to do business.

The Public Product Database 311 primarily consists of one Table with one Record per product which has been submitted to be publicized. The columns of the table correspond to the public attributes that have been configured by the E-Bazaar Administration Tool for all products in the E-Bazaar. Meanwhile, there is a BLOb column in the table containing a Dictionary of each product's private attributes. The Table of Products is meant to be browsed and queried.

The three special Runnables are stored in a root file directory called the Advertiser Directory. The Advertiser Directory 313 then has one subdirectory for each Advertiser. When one of the three is needed, the Advertiser is known so that the Commercial Activity Dispatcher 305 knows which subdirectory to obtain the needed Runnable. The E-Broker 301 itself has its own subdirectory as well.

The Private Activities Database 321 provides the means for an Advertiser to store pending orders if it needs to, store its inventories, or whatever other information it needs to maintain in order to carry out commerce in the E-Bazaar. It should be possible to maintain such private activity databases wherever the Advertiser desires. This just means that the OrderProcessor 319 will need to access information external to the WebServer where the E-Bazaar is running. Such external information should be able to reside in an external Database Server or even a mainframe. In either case, it should be possible for the external database to reside locally or remotely as needed.

The E-Bazaar should be provided with a variety of simple OrderProcessors 319, as well as ProductInfo 317 and OrderForm 315 templates so that an Advertiser may quickly and easily become an advertising participant in an E-Bazaar. With the simple OrderProcessors, a simple database may also be configured to reside in the WebServer or even tables within the same database as the Public Product Database 311 (as long as the database provides per table security).

E-Bazaar E-Broker InteractProtocols

When the E-PIA Internet Client communicates with the DORMS Server via HTTP, the requests get converted into Interaction requests submitted to an E-Metro Community E-Broker. In this section, the available Interactions that can be requested are presented in detail. This complete list and description of E-Bazaar Interactions intends to provide a full understanding of all the possible and important activities that can take place in a fully functioning E-Bazaar E-Metro Community.

As is obvious from the discussion thus far, the E-Bazaar E-Broker is the heart of a running E-Bazaar E-Metro Community. The InteractProtocol names that the E-Bazaar E-Broker provides are listed in the table below. These InteractProtocols are available at runtime. The "Seller" column denotes who the Seller E-PIA interacts with when it initiates the Interaction while the "Buyer" column denotes who the Buyer E-PIA interacts with.

InteractProtocol	**Overview Description**	**Seller**	**Buyer**
getSummary()	Get runnable body of code that summarizes E-Bazaar.	w/E-Broker	w/E-Broker
	Get runnable body of code that summarizes advertiser's product offerings.	w/Buyer	w/Seller
getPublicProductAttribute Template()	Get Dictionary of public attribute names associated with their rules.	w/E-Broker	w/E-Broker
putProductToTradeInfo ()	Put a new product in the E-Bazaar to advertise publicly.	w/E-Broker	w/E-Broker
getProductToTradeInfo	Get all of the information about	w/E-Broker	w/E-Broker

()	an existing product in the E-Bazaar.		
getProducts()	Query the E-Bazaar's list of E-PIA advertisers for products matching the query conditions.	w/Buyer	w/Seller
getPrivateProductAttributes()	Given a productId, get Dictionary of private attribute names associated with their values.	w/Buyer	w/Seller
getProductTradeForm()	Given a productId, get a runnable body of code representing an order form that can be filled in.	w/Buyer	w/Seller
putProductTradeOrder()	Given a filled in order form to submit to the advertising E-PIA, obtain either an indicator of order acceptance or an OrderNumber for a "to be fulfilled" order.	w/Buyer	w/Seller
cancelProductTradeOrder()	Given an OrderNumber of a "to be fulfilled" order, cancel the order so that it will not be fulfilled.	w/Buyer	w/Seller
getProductTradeOrderStatus()	Given an OrderNumber, obtain current status information about the order.	w/Buyer	w/Seller
getOrderHistory()	Get a list of OrderRecords of all orders submitted to the E-PIA satisfying a Query given	w/E-Broker	w/E-Broker

The next table describes the precise subsystem activities that must be performed by each InteractProtocol implementation. This will assist the reader in understanding the relationship of the subsystems for various Interaction requests.

InteractProtocol	Design
getSummary()	Obtain "ProductInfo" Runnable from the E-Broker subdirectory to present Summary of E-Bazaar to Internet Client.
	The getSummary() request is submitted along with Rules that specify a single E-PIA Advertiser. When the Advertiser is determined, its subdirectory is searched for the "ProductInfo" Runnable to present the summary to the Internet Client.
getPublicProductAttribute Template()	The E-Bazaar E-Metro Community Info File is read to obtain the public attribute information.
putProductToTradeInfo ()	A new Record in the Public Product Database Table is INSERTED or UPDATED. The Runnables associated with the Record are stored in the corresponding Advertiser Directory. If the product is new and has a new Advertiser, a new subdirectory must be created. In this case, the Advertiser's name and its subdirectory name association must be stored in the E-Bazaar E-Metro Community Info File.
getProductToTradeInfo ()	The Record of the product specified is read -- its public attributes and private attributes BLOb is read, and its Runnables are retrieved from its Advertiser's subdirectory. The public attributes and Runnables are assembled into a single Dictionary. The Dictionaries may be presented to the Internet Client and the Runnables executed on an as needed basis.
getProducts()	A submitted Query is performed on the Public Product Database Table. The same two Dictionaries described above are returned FOR EACH product satisfying the Query.
getPrivateProductAttributes()	For the specified product, return the BLObbed private attribute Dictionary.
getProductTradeForm()	Return the OrderForm Runnable so that it can be presented to the Internet Client.
putProductTradeOrder( )	Submit a Dictionary of the OrderForm fields with their associated "filled in" values to the OrderProcessor Runnable so that the Order can be processed by the

	Advertiser's private order processing subsystem in any way he chooses. A Boolean and String regarding immediate order status are returned. The Boolean indicates whether or not the order was immediately fulfilled. The Boolean value and String contents may be presented to the Internet Client.
cancelProductTradeOrder()	The Commercial Activity Dispatcher must determine which Advertiser E-PIA to submit the cancellation to by Rules submitted with the request. When the Advertiser is determined, the OrderNumber is submitted to the Advertiser's private OrderProcessor. A String concerning cancellation status is returned which can be presented to the Internet Client.
getProductTradeOrdersStatus()	The Commercial Activity Dispatcher must determine which Advertiser E-PIA to submit the status request to by Rules submitted with the request. When the Advertiser is determined, the OrderNumber is submitted to the Advertiser's private OrderProcessor. A String concerning cancellation status is returned which can be presented to the Internet Client.
getOrderHistory()	The Commercial Activity Dispatcher knows that the requester is the Advertiser in question. The Query is submitted to the Advertiser's private OrderProcessor so that the OrderRecords containing Orders which satisfy the Query may be returned. These may then be presented to the Internet Client.

The InteractProtocol interfaces will now be described. Before describing the interfaces in detail, it is important to present the fundamental object framework employed by the InteractProtocols. These objects are presented below. After the fundamental object descriptions, the InteractProtocols are discussed in detail denoting which parameters are input, which are output, and their types based on the types described in the fundamental object framework. This should provide the reader a maximum amount of detail with regard to the flow of data into and out of the E-Bazaar, how data is employed to interact with advertisers and shoppers in the E-Bazaar, as well as when specific objects or data is presented to an Internet Client.

Runnable – A Dictionary of names associated with executable bodies of code which can themselves be instances of Runnable. The Dictionary comprises all of the executable "pieces" necessary to run a particular subsystem. Some useful subclasses are ExeApp, Dll, JavaAppelet, and Html. The Commercial Activity Dispatch knows how to download all of the executable bodies contained in a Runnable down to the Internet Client so it can execute them appropriately. A Runnable with a single Html Document is the simplest case.

ProductInfo – A Runnable whose purpose it is to present product information to a shopper.

Query – A String representing a SQL SELECT.

PublicAttributes – A Dictionary of names associated with values representing the values of the public attributes of a product. An example is shown below.

Name	**Rule**	**example**
activity	this.isKindOf(String) && (this=="buy" || this=="sell")	"sell"
advertiser	this.isKindOf(String)	"Dad's"
productCategoryName	this.isKindOf(String)	"sodas"
productTypeName	this.isKindOf(String)	"root beer"
productInstanceName	this.isKindOf(String)	"Dad's Root Beer"
productId	this.isKindOf(String)	"D-RB10014"
pricePerUnit	this.isKindOf(Money) && this>0	.79
unitSize	this.isKindOf(Integer) && this>0	48
productInfo	this.isKindOf(Runnable)	Html Document
orderForm	this.isKindOf(Runnable)	Html Document
orderProcessor	this.isKindOf(Runnable)	Java Application

PrivateAttributes – A Dictionary of names associated with values representing the values of the private attributes of a product.

OrderForm – A Runnable that presents an order form for a person to fill fields with values.

FilledOrderForm – a Dictionary of OrderForm fields names associated with values of the fields that are filled in.

OrderProcessor – A Runnable that processes OrderForms. Typically this Runnable must perform processing on a private database.

ProductId – a String that uniquely identifies a product.

OrderNumber – a String that uniquely identifies an Order that has been placed.

OrderRecord – a structure is with the format shown below. Note that it may be desirable to allow the structure of OrderRecords to be authorable on a per advertiser E-PIA basis.

Name	type
productId	String
numberOfUnits	Integer
when	Time
price	Money
fulFilled	Boolean
comment	String

The InteractProtocol interface descriptions below explain how to use the InteractProtocols and what data is expected to be input and output.

getSummary(out Runnable aSummary) – Obtain aSummary which can be executed to present a Summary of the E-Bazaar or the Summary of the Advertiser, depending on rules chosen.

getPublicProductAttributeTemplate(out Dictionary aListOfPublicAttributeRules) – Obtain aListOfPublicAttributeRules, a Dictionary of attribute names associated with their rules.

putProductToTradeInfo(in String aProductId, in Dictionary aListOfPublicAttributes, in Dictionary aListOfPrivateAttributes) – Enter a new product into the Public Product Database or modify an existing one. If attempting to enter a new product, then aProductId must be 0, otherwise it is its existing productId. aListOfPublicAttributes and aListOfPrivateAttributes comprise all of the attributes of the product to be newly entered or modified.

getProductToTradeInfo(in String aProductId, out Dictionary aListOfPublicAttributes, out Dictionary aListOfPrivateAttributes, out String aGeneralStatus) – Obtain all of the information about an existing product in the Public Product Database aProductId is a String representing the productId of the existing product. aListOfPublicAttributes and aListOfPrivateAttributes comprise all of the attributes of the product. aGeneralStatus is a String with some human readable status information.

getProducts(in String aQuery, out OrderedCollection aListOfProductIds, out OrderedCollection aListOfListOfPublicAttributes, out OrderedCollection aListOfListOfPrivateAttributes) – Obtain all of the information about more than one existing product. The products to obtain information on are the ones satisfying the Query aQuery. Three OrderedCollections are returned in the out parameters: aListOfProductIds, aListOfListOfPublicAttributes, and aListOfListOfPrivateAttributes.

getPrivateProductAttributes(in String aProductId, out Dictionary aListOfPrivateAttributes) – Obtain all of the private attribute values of the product with productId aProductId. The private attributes are returned in the Dictionary aListOfPrivateAttributes.

getProductTradeForm(in String aProductId, out Runnable anOrderForm) – Obtain a Runnable anOrderForm representing the OrderForm of the product with productId aProductId.

putProductTradeOrder(in Dictionary aFilledOrderForm, out String anOrderNumber, out Boolean fulfilled, out String aStatus) – Place an order with the Dictionary aFilledOrderForm. A String anOrderNumber is returned representing a unique order number for the order placed. The Boolean fulfilled is returned indicating whether or not the order was fulfilled immediately (TRUE) or if it will be fulfilled ȴater (FALSE). Also returned is a general status string indicating any other fulfillment information.

cancelProductTradeOrder(in String anOrderNumber, out String aStatus) – The order anOrderNumber which has currently not been fulfilled is canceled so that it will never be fulfilled. aStatus is returned indicating any other cancel information.

getProductTradeOrderStatus(in String anOrderNumber, out Boolean fulfilled, out String aStatus) – The order anOrderNumber is submitted to obtain current status information about the order. If fulfilled is TRUE, then the order has been fulfilled already, else it has not been fulfilled yet. aStatus is a String containing further status information.

getOrderHistory(in Query aQuery, out OrderedCollection aListOfOrderRecords) - Obtain all of the OrderRecords for Orders for products from an E-PIA which satisfy the SELECT in aQuery. The OrderRecords are returned in the OrderedCollection aListOfOrderRecords. A useful example using the Query is to employ the expression "fulfilled==TRUE" to obtain only those OrderRecords which correspond to actual trades performed.

Commercial Scenarios Using the E-Bazaar Framework

As presented, any E-PIA can participate as an advertiser in an E-Bazaar by providing its own implementations of OrderProcessor, ProductInfo, and OrderForm Runnables. This framework allows an advertising E-PIA to maintain a very general capability for performing its necessary commerce. Additionally, the framework provides the means for efficient trading scenarios not possible without an electronic commerce system and which is not possible without special attention to privacy, security, and privilege which the invention provides so well. Additionally, E-PIAs and E-AutoPIAs may also participate as shoppers using this unified framework and receive the same benefits of efficiency, privacy, security, and privilege. Efficiency in this context applies to the effort in connecting with trading partners as well as the efficiency in the cost to do business.

As mentioned at the start of the E-Bazaar discussions, the primary distinction between the three case studies is their implementation of the OrderProcessor. This single distinction was intentional so that a single E-Bazaar Framework could successfully implement all three cases. The three cases that the E-Bazaar can handle are now discussed below.

The "Privacy Enabled Commerce" scenario allows for any desired commerce to take place securely and privately. The model for ordering and fulfilling orders is meant to be general. Thus, there is really nothing to expound on since the framework itself is able to accomplish this case due to its intended generality. The Semi Real-time Auction and Large Quantity Sales cases are, therefore, members of the "Privacy Enabled Commerce" case due to this generality. Note that Internet E mail may be a useful tool for notifying shoppers of asynchronously fulfilled orders.

The "Semi Real-time Auction" case requires certain processing and functionality in the ProductInfo as well as the OrderProcessor Runnables. The ProductInfo Runnable should not only advertise product information as is done normally, but should also display the current bid and any other real-time parameters of the auction that are deemed necessary to present to a shopper.

The processing of Orders is interesting because most will be canceled eventually. However, totally adhoc order fulfillment is possible if the OrderProcessor is coded to allow it. For example, it could allow the auctioneer to examine the Order history. The auctioneer could decide at any time to extend the time of the auction, cut it short, fulfill the non-highest bid (order), fulfill multiple bids (order), or cancel all bids (orders). The behavior of the auction is governed by the OrderProcessor.

Internet E mail will be very useful in Semi Real-time Auctions. For example, orders may be placed with a request to be notified of important bid updates in the future may be requested. However, it should be possible to build a Semi Real-time auction system which allows Online E-PIA clients to realize periodic updates from the E-Bazaar periodically.

The "Large Quantity of Sales" case mostly requires certain processing in the OrderProcessor Runnable. All orders for a product will typically maintain a "pending" unfulfilled status. At some point in time, however, the aggregate order quantity for a certain product exceeds its predetermined threshold for invoking order fulfillment. However, a real OrderProcessor for the Large Quantity Sales case must allow premature fulfillment in the scenario where it is taking too long for a certain quantity of orders to come in. Premature cancellation of all or some orders should also be possible.

It may also be desirable to allow real-time price adjustments. In this case, an Advertiser may find it desirable to maintain a hybrid of an auction along with a large quantity of sales scenario. The Advertiser who finds that he can trade product for less because there are enough Orders and still make sufficient profit, should be able to go ahead and invoke order fulfillment rather than wait and possibly be left with a large unwanted expensive inventory.

Some Advertisers may desire to display real-time information in the ProductInfo Runnable such as the current quantity ordered and the total quantity desired.

E mail can be used for notification of sudden changes in order status, just as in the other commercial scenarios.

Specific Objects

Since the preferred embodiment is designed to be implemented with an object-oriented programming language, we now turn to the design of the individual objects.

Before continuing with each of the objects in the preferred embodiment, the fundamental object classes that make up the preferred embodiment objects that will be presented are listed below. Most of these object classes are commonplace in fundamental object oriented frameworks and should be familiar to those skilled in the art of object orientation. See Fig. 22.

Type	Description
Object	abstract Class for which is the superclass of all Classes such as the ones listed below.
Class	a Class whose instances represent each of the Classes defined in the system.
Integer	Number
String	Characters
Float	Number
boolean	Expression
Collection	an abstract Class which is the superclass of all Classes that represent collections of Objects
Ordered Collection	a Collection subclass that represents a list of Objects that are ordered in a set sequence.
Set	a Collection subclass that represents a list of Objects in no particular order
Dictionary	A list of keyed objects.
Folder	Can store objects using hierarchically arranged keys.
SQL Statement	Provide fast lookup for information.
Executable String	A piece of code that can be passed around as an object, interpreted when it needs to be, and executed.
Compiler	a Class whose instances each represent an executable body of code that translates a String into an OrderedCollection of Codes that are interpretable by a runtime interpreter.
Extended Classes	Other classes will need to be defined for individual E-Metro Community needs, such as for video, sound, etc.

The E-PIA object 135, shown in Fig. 15A. The E-PIA encapsulates the personal data and data processing rules or behavior of a real individual or an entity by storing information assets and releasing them under the rules established by the owner of the E-PIA. Fig. 15B shows an E-PIA that is created to pass informational assets. The asset folder will contain the approved subset of informational assets, and the rules will contain the transitive rules (from the interact protocol) of the original E-PIA, thus providing a limit on the subsequent dissemination of the informational assets in the folder. The certificate helps assure subsequent users of the information that the informational assets originated from the original E-PIA.

Items in the E-PIA	No.	Type	Description

Object			
auditTrail	153	Ordered Collection	An OrderedCollection of RecordEvents 154 that chronicle the history of an E-PIA.
assets	155	Folder	All the informational assets known about the E-PIA are stored in an unstructured folder. Information may be input into the folder using the forms retrieved from the forms repository.
interactProtocols	143	Set	An E-PIA may contain several interact protocols stored in a set.
trustedTokens	157	Set	The E-PIA will collect trusted-tokens to give to E-Brokers to assure the integrity of any transactions.
privilegeRules		Set	The E-PIA has a set of rules that must always be met for any interact protocol to be performed.
certificate	150	Certificate	The certificate contains the name and public key of the entity the E-PIA represents.

The InteractProtocol Object 141 is depicted in Fig. 19. The InteractProtocol defines the name, input parameters, output parameters, and the conditions that must be met in order for the interaction to occurs. An E-Broker actually implements the interaction. InteractInstructions cause InteractProtocol invocations. InteractInstructions are detailed in a later section.

Items in the Interact Protocol Object	**No.**	**Type**	**Description**
	141	Interact Protocol	Inherits
name	191	String	Each protocol must have a name.
PrivilegeRules	185	Set	Already described in a previous table.
MaxInstructions	193	Integer	See corresponding description in the interact instruction above
transitivePrivilegeRules	185	Set	See corresponding description in the

			interact instruction above
defaultMap	197	Dictionary	Since the interact instruction must be "filled in" before execution, the default map can provide defaults to assist in completing the interact instruction.
Inputs	197	Set	
outputs	198	Set	What informational assets will be stored in the information E-PIA if the subsequent interact instruction is successfully executed.
Enabled	192	boolean	

The Rule object 201 is shown in Fig. 20.

Items in the Rule Object	**No.**	**Type**	**Description**
a Rule object is actually just an ExecutableString object	201	Executable String	an ExecutableString representing a user defined Rule
compiler	187	String	name of compiler which is always "Rule"

The Parameter object 195 is shown in Fig. 21.

Items in the Parameter Object	**No.**	**Type**	**Description**
name	211	String	name of parameter
validationRule	187	Rule	an ExecutableString whose compiler is "Rule"

The E-AutoPIA 151 object is shown in Fig. 16. The E-AutoPIA is an intelligent agent that employs an Itinerary to perform specific tasks assigned by the owner. Itineraries are detailed in a later section. Only the original E-PIA may launch an E-AutoPIA, but the original E-PIA may launch several E-AutoPIAs and have them active at one time.

Items in the E-AutoPIA Object	**No.**	**Type**	**Description**
itineraries	161	Set	An E-AutoPIA may have several itineraries hierarchically callable Itinerary objects 163.

The Itinerary Object 163 is shown in Fig. 17.

Items in the Itinerary Object	**No.**	**Type**	**Description**
name	170	String	An itinerary must have a name.

instructions	171	Set	The itinerary may contain several interact instructions. If there are several instructions, and there is no script, the instructions are performed sequentially.
scripts	175	Dictionary	Scripts are stored in a dictionary object, which allows an executable string to be referenced by a name.
TransitivePrivilegeRules	178	Set	Already described in a previous table.
privilegeRules	172	Set	Already described in a previous table.

The Interact Instruction 173 object is shown in Fig. 18. InteractInstructions cause interactions between E-PIAs and E-AutoPIAs. Each InteractInstructions names the InteractProtocol that will be performed and the actual parameters for the interaction as well as the rules under which it can occur. The end result of a successful InteractInstructions is the creation of an informational E-PIA as shown in Fig. 15B. Each item of information held by the informational E-PIA is encrypted using the private key of the original E-PIA, thus providing subsequent users authenticity of the information when using the E-PIA's public key.

An InteractProtocol maintains essentially a template relationship to an InteractInstruction. An InteractProtocol is represented by a signature of parameters to be filled in, while the InteractInstruction counterpart is the same except with parameters filled in. InteractProtocols and Interact Instructions are both authoring time entities. The InteractProtocols represent the services provided by an E-Broker and are authored along with the E-Broker. InteractInstructions are authored during the construction of an Itinerary for an E-AutoPIA. Each InteractInstruction represents the call of a requested interaction or InteractProtocol. The inputs, outputs, and the default map are removed from the InteractOrotocol when constructing the corresponding InteractInstruction.

Items in the	**No.**	**Type**	**Description**

Interact Instruction Object			
interactProtocolNname	181	String	Each protocol has a name.
CommunityName	131	String	The name of the E-Metro Community where the E-AutoPIA's original E-PIA resides.
PrivilegeRules	185	Set	Already described in a previous table.
MaxInstructions	183	Integer	The maximum number of E-PIAs that will have this instruction used on. This number can be infinity.
ParameterAssignments	182	Dictionary	
transitivePrivilegeRules	185	Set	Already described in a previous table.

The E-Metro Community Object 130 is shown in Fig. 13. The E-Metro Community object provides a grouping concept for the E-PIAs and other E-Communities.

Items in the E-Metro Community Object	**No.**	**Type**	**Description**
	135	E-PIA	The E-Broker class inherits from the E-PIA class. Thus, an E-Broker is a subclass of E-PIA containing all of the items that an E-PIA contains, but additionally includes:
name	131	String	Each E-Metro Community must have a name.
Communities	132	Set	An E-Metro Community 137 may contain other E-Communities in a hierarchical relationship.
Brokers	133	Set	Each E-Metro Community will need at least one, and likely several E-Brokers 136 to perform specific tasks. The E-Brokers are organized into a set.
Beings	134	Set	All the E-PIAs 135 in an E-Metro Community are kept in a set.

The E-Broker object 136 is shown in Fig. 14. An E-Broker is required for all E-PIA and E-AutoPIA interactions. It is the E-Broker that assures that information is released only to trusted entities that meet the requirements set by the individual.

Items in the E-Broker Object	No.	Type	Description
	135	E-PIA	The E-Broker class inherits from the E-PIA class. Thus, an E-Broker is a subclass of E-PIA containing all of the items that an E-PIA contains, but additionally includes:
protocolDirectory	143	Set	The E-Broker may contain several InteractProtocols 141 stored in a Set.

Architecture and Design

This next section describes the architecture and design of a personal and private information protection and brokerage system called "E-Metro."

Introduction -- Users' E-Metro World

The E-Metro World is the collection of all hardware and software that is being employed to store E-Metro specific objects and/or perform E-Metro activities. The user view of the E-Metro World is achieved primarily through a Netscape Browser, and from that application, the view is that of many E-Communities all connected to each other via the Internet as shown in Figure 2. Ultimately, the user does not care where the E-Communities are physically located, only that they serve as a logical place for interaction with other E-PIA's with similar interests.

As a facility for building up one's information asset structures, E-Metro Forms Repositories are also available. Forms can be retrieved using the E-Metro Client authoring facility and incorporated into existing or new E-PIA's to add information according to a useful reusable structure. A user may then store his E-PIA into one or more E-Communities.

System Architecture Overview

E-Metro World Machine Configuration

In reality, each E-Community resides on an E-Metro Web site Server. As depicted in Figure 7, more than one E-Community may reside on one such Server. Furthermore, E-

Communities residing in a single Server may be configured to maintain a hierarchical relationship to one another.

Two E-Being - Forms Repositories 13 are depicted in Figure 7. As indicated by the text in Figure 7, one E-Being - Forms Repository is implemented by an FTP site, while another is implemented by a Mail Server System. It is even possible that no Forms Repository exists and that the Forms are simply managed as local files.

E-Metro World System Processes Architecture

The Client and Server Processes in an E-Metro World are shown in Figure 8. The client workstation consists of the Netscape browser and E-Metro specific DLLs, JAVA scripts, or some other client code of similar nature meant to facilitate various E-Metro client activities. FTP Servers are well known staples on the internet while the Netscape Server System is discussed in Netscape's Server documentation. The focus of this document is the shaded E-Metro Trusted Server Systems 47 in Figure 8. While using E-Metro, the Clients always communicate with an E-Metro Trusted Server. At authoring time, InteractProtocols and InteractInstructions may only be obtained from the correct E-Brokers (Actually, the Forms for InteractProtocols and InteractInstructions may be obtained from Form Repositories if set up to do so, but the required TrustedTokens for these activities may only be obtained from the E-Brokers). At runtime, E-Metro Clients query a user's Home E-PIA at the E-Community, and therefore E-Metro Server, where it resides to see the latest results or status of associated E-AutoPIA's. E-Metro Server Systems actually consist of many processes which will be discussed in the next section.

E-Metro Security Architecture

E-Metro emphasizes security of information assets and trusted interactions. E-Metro guarantees that all information put into the E-Metro World System will be secure and that only those who are trusted to have access to specific information will. The reader is referred to Figure 24 for a depiction of when and where encrypted transmissions occur in what is essentially the "public" interlinks of the E-Metro World System. All of the necessary cryptographic security is handled by Netscape's SSL communication layer. To maintain the level of security described, the following system attributes are maintained:

1) Each E-Metro Trusted Server Subsystem at a Web site consists of secure processes that nobody can get access to while they are running. It is assumed that an ordinary person skilled in the art of process security on a single machine can achieve this runtime integrity.

2) Each E-Metro Trusted Server Subsystem maintains its own private key and public key. The public key of a specific E-Metro Trusted Server Subsystem is known by all other E-Metro Trusted Server Subsystems via the DirectoryService E-Broker.

3) All E-PIAs and E-AutoPIAs are encrypted when transmitted between E-Metro Trusted Server System Web sites. Encryption is performed with both the public key of the E-Metro Trusted Server Subsystem that is the destination of the transmission as well as the private key of the source of the transmission. This double encryption accomplishes a double guarantee:

a) Only the E-Metro Trusted Server Subsystem (the destination) with the correct private key will be able to decrypt the transmission.

b) This same E-Metro Trusted Server Subsystem (the destination) will be guaranteed that the transmission came from the source E-Metro Server stated in the transmission and not a fraudulent source. See Figure 24.

4) All interactions between E-PIAs and E-AutoPIAs are performed in private on a single machine within an E-Metro Trusted Server System.

5) When a client requests information contained in its Home E-PIA, the E-Metro Trusted Server Subsystem maintaining the Home E-PIA encrypts the information for the transmission with the Home E-PIA client's public key so that only the receiving client will be able to decrypt the information. When writing information to the Home E-PIA, the information is encrypted

with the destination E-Metro Trusted Server Subsystem's public key so only that the correct destination will be able to decrypt the information. Writing information also includes E-AutoPIA and associated itinerary authoring. See Figure 24.

6) When a client is obtaining authoring information from an E-Broker, the authoring information is encrypted with the client's public key, again so that only the client knows how to decrypt the information. This encryption is important mostly for the transmission of TrustedTokens during authoring which must immediately be encrypted via the client's private key upon reception.

Metro Trusted Server System

Figure 9 pictures the top level subsystems of an E-Metro Server. The core subsystem that provides the primary services of E-Metro is the Distributed Object Resource Management System Server or DORMS. The five other subsystems are an FTP Server and FTP Client Process and three Netscape Web site Server subsystems that, together, perform the functionality necessary for a complete E-Metro Server.

DORMS Server

As mentioned, the DORMS Server is the heart of the E-Metro system architecture. It essentially governs the trusted storage and brokering of all E-Metro objects and resources with the assistance of the smaller grained objects, namely E-Communities and E-Brokers, that it internally manages. More specifically, the DORMS Server performs the following:

D1. Stores E-Communities

D2. Stores E-Brokers

D3. Maintains an entire E-Metro World Directory of where all Communities and E-Brokers are located and keeps the directory up to date.

D4. Stores or "banks" E-PIAs

D5. Maintains a Messaging Subsystem for E-AutoPIA transport between E-Communities

D6. Maintains visiting E-AutoPIAs

D7. Drives E-Broker mediation of E-AutoPIA with E-PIA interaction

InteractProtocol or InteractInstruction. E-PIA's may do the same, but realize that E-PIA's can only do so via an E-Broker implementation. Both credit card and billing APIs are available in the E-Broker Service API which E-Broker implementations may call. This will be discussed later.

Netscape Server API (NSAPI)

The NSAPI works closely with the Netscape Commerce Server in order to provide the means for a Web site to have control over the processing when a normal HTTP compatible request comes in to the Commerce Server. In order to do this, Netscape has identified the following steps in the normal response process:

NS1. Authorization translation
NS2. Name translation
NS3. Path checks
NS4. Object type
NS5. Respond to request
NS6. Log the transaction

The NSAPI provides the ability to override the processing that is performed in any or all of these steps. It is assumed that an ordinary person skilled in the art of computer programming can easily follow the necessary NSAPI manuals to enable the required overriding of these steps. In particular, steps 1, 2, 3, and 5 will need specific E-Metro replacements. An overview of the replacement implementations are enumerated below:

For NS1,

The E-Community privilegeRules necessary for the request can be checked; and

The TrustedToken necessary for the request can be checked.

For NS2,

Paths may refer to hierarchically located E-Brokers or E-Communities. The path submitted is munged by leaving only the relative path corresponding to the E-Broker or E-Community assuming the site portion of the path is correct.

D8. Maintains the Privilege Rules Processor that assists the DORMS' guarantee of secure and trusted interactions.

Netscape Commerce Server

The Netscape Commerce Server is the core subsystem enabling an E-Metro Server to be a Web site and interact over the Internet. Since it uses the open Secure Sockets Layer (SSL) protocol, it provides full Internet security. SSL provides encryption, server authentication, and message integrity using technology from RSA Data Security. When the client makes a request, it always communicates with the Netscape Commerce Server initially. In turn, the Netscape Commerce Server will cooperate with the DORMS Server via the Netscape Server API. This communication with an E-Metro Server via the Netscape Commerce Server is what allows the client subsystem to consist primarily of an HTTP/HTML compliant World Wide Web Browser such as Netscape Navigator. The details of this cooperation are described in the next section.

Netscape Transaction Server

As noted in Figure 9, the Netscape Transaction Server handles credit card processing, transaction logging, and billing management. The DORMS Server interacts with the credit card processing function when a person wishes to begin using E-Metro services for the first time, or add new capabilities to their E-PIA. The charges for initial or new capabilities are processed automatically by the credit card function of the Transaction Server. The DORMS Server also interacts with the transaction logging function to track what is going on at an E-Metro site and may employ the billing management function as well. It is assumed that an ordinary person skilled in the art of computer programming can easily follow the necessary Netscape manuals to configure the cooperation between the DORMS Server and Transaction Server.

An important E-Metro feature is that individual E-Brokers and E-PIA's can configure their own billing policies. E-Brokers can require the entry of credit card information in order that it submit a required TrustedToken for an

For NS3, the E-Broker or E-Community is checked to see if it exists. For NS5, the requested DORMS service is performed. There are several types of requests which are:

1) Client requests to browse the DORM Directory

2) Client requests authoring time information from an E-Broker.

3) Client requests retrieval of owned E-PIA information assets.

4) Client requests to store E-PIA information assets after assets were updated on Client.

5) Client requests to launch an E-AutoPIA.

Note that E-AutoPIA's do not utilize this entrypoint because E-AutoPIA activities are not a Client driven process.

FTP Server and FTP Client

As will be introduced later in the architecture, E-Metro requires a reliable Messaging Subsystem for transporting the E-AutoPIA's from E-Community to E-Community. Since Internet E Mail is not reliable, FTP Servers and FTP Clients are used to implement the transport. E-AutoPIA's are marshalled into a BLOb and transported to remote sites via a file. The file is then uploaded via initiation of an E-Metro Server's FTP Client to another E-Metro Server's FTP Server. The later section describes the details of the use of FTP for the Messaging Subsystem machinery.

Distributed Object Resource Management System (DORMS) Server

Figure 10 shows the complex arrangement of subsystems within the DORMS Server. The rest of this section devotes portions to discussing each of these component subsystems. Realize, however, that the Interaction Processor is the focal point because it is the driving subsystem that gets called due to a Client request via the Netscape Commerce Server or due to an E-AutoPIA arrival via the Messaging Subsystem. Another important point to make before continuing is that all service requests are somehow implemented as an interaction with an E-Broker.

Interaction Processor

As mentioned, the Interaction Processor is the focal point of the DORMS Server and it satisfies all requests via an E-Broker. When the Messaging Subsystem submits an E-AutoPIA to the DORMS, it is actually submitting it to the Interaction Processor which is the driving body of code for the whole DORMS Server. When the Messaging Subsystem does this, it assumed that it also has unmarshalled the E-AutoPIA BLOb so that the E-AutoPIA is in a suitable form for the rest of its processing. As enumerated in Tables 1 and 2 below, there is much processing to be done for a client request as well as for a visiting E-AutoPIA. The service requests that the Interaction Processor handles are all the Client requests listed below, as well as the InteractInstructions of incoming E-AutoPIA's. The complete list of requests serviced by the Interaction Processor and an overview of how they are handled is enumerated below.

IP1. Client requests to browse the DORMS Directory— The request is redirected to a special E-Broker known as the "DirectoryService" E-Broker.

IP2. Client requests authoring time information from an E-Broker -- The request is redirected to the E-Broker designated to call one of its special authoring time services (InteractProtocols) such as "interactProtocolDirectory" or "getRightsToInteractProtocol."

IP3. Client requests retrieval of owned E-PIA information assets— This request is redirected to a special E-Broker known as the "Home" E-Broker. The special service employed is called "retrieveAssets." This special E-Broker must be present in every E-Community that Home E-PIA's are to be allowed to reside in.

IP4. Client requests to store E-PIA information assets after assets were updated on Client -- This request employs the "Home" E-Broker by calling its "storeAssets" service.

IP5. E-AutoPIA requests interaction via current InteractInstruction in its Itinerary— The request is

		perform service
13	E-Broker Service API, read E-PIA's from Object Repository	Call **collectTrustedEPIAs()**
14	E-Broker executable	Perform the rest of executable code in E-Broker's service implementation
15	Virtual Image	Update E-AutoPIA with outputs for which transitive privileges are satisfied..
16	Itinerary Interpreter	Interpret current script and determine next InteractInstruction to perform.
17	DirectoryService E-Broker and Virtual Image	Look up FTP address for next E-Community of next InteractInstruction
18	Messaging Subsystem	Submit E-AutoPIA back to Messaging Subsystem to be transported to next E-Community. Messaging Subsystem must encrypt the information to be transmitted using the public key of the destination.

Table 2 A request from an E-AutoPIA -- the Interaction Processor's steps and use of intra-DORMS subsystems.

Rules Processor

The Rules Processor is a key security enforcement subsystem. It checks privilegeRules, and additionally, the Rule Processor also handles conversions to SQL statements to aid in E-PIA selection.

Validation of privilegeRules requires a fairly complex procedure. In the case of E-AutoPIA's, the privilegeRules can refer to "myself" and "yourself." Each privilegeRules is a Set of Rule objects. Each Rule object must initially be broken into subexpressions which include "myself" references only. These "myself only" subexpressions may be immediately be reduced to TRUE's or FALSE's by executing the Virtual Interpreter on the E-AutoPIA which is the current context.

The remaining "yourself" subexpressions are combined with the results to form a reduced expression. This remaining reduced expression is then parsed and transformed into a SQL SELECT statement which may have an ORDER BY clause if the Rules language provides this. This SELECT statement is used

This page is missing upon filing.

6	E-Broker Adaptor	Call execute()
7	E-Broker executable	Invoke executable code to perform service
8	E-Broker Service API	May need to call service API procedure
9	Netscape Commerce Server	Return information back. Encrypt the information sent back with requesting client's public key.

Table 1 A request from the Client application -- the Interaction Processor's steps and use of intra-DORMS subsystems.

	Subsystem Used	**Action**
1	Messaging Subsystem	Receives E-AutoPIA and decrypts it using the private key of the local E-Metro Trusted Server System.
2	Interaction Processor and Virtual Image	Request is submitted to DORMS with E-AutoPIA
3	Virtual Image with Virtual Interpreter	Look up E-Community named in E-AutoPIA's InteractInstruction
4	Rules Processor with Virtual Interpreter	Validate privilegeRules of E-Community
5	Rules Processor with Virtual Interpreter	Validate the privilegeRules of any transitively exchanged E-PIA versions that are going to be passed as an input or output Parameter.
6	E-Broker	Validate that E-AutoPIA has necessary TrustedToken by decrypting it with E-AutoPIA's public key obtained from its certificate.
7	E-Broker Adaptor	Call execute() with "getTrustedToken" service and name of InteractProtocol (which will be performed shortly) as parameter.
8	E-Broker executable	Invoke executable code to generate unique TrustedToken for InteractProtocol named.
9	Rules Processor with Virtual Interpreter	Construct reduced SQL Statement in preparation for E-PIA selection and collection (see next section)
10	E-Broker	Call E-Broker
11	E-Broker Adaptor	Call execute() but allow only those inputs that satisfied transitive privileges to be passed.
12	E-Broker executable	Invoke executable code to

later to collect the E-PIA's that satisfy all the rules so far evaluated up to this point.

Since each E-PIA has its own privilegeRules for the interaction with the E-AutoPIA which is the current context, the collected E-PIA's from the above SELECT must be further filtered. This is accomplished by taking each E-PIA one at a time from the collected set and executing their privilegeRules with the E-AutoPIA as "yourself" and the current E-PIA as "myself." This execution requires the Virtual Interpreter. Note that this portion of the privilege check may have poor performance since the database SELECT is not employed. It is therefore important to construct specific privilegeRules for E-AutoPIA's so that the collected E-PIA sets are as small as possible.

Virtual Interpreter

The Virtual Interpreter is simply the machinery that gives dynamics to the programming language of E-Metro. The programming language may be any language even a new one, but it is suggested that it have similar features to that of Smalltalk. This programming language is the one that must be used in the privilegeRules and the scripts of the Itineraries.

Virtual Image

The Virtual Image is the place where all E-Metro specific classes and objects which are being processed are kept in RAM. The Virtual Interpreter is what gives dynamics to these objects. As shown in Figure 10, all E-Communities and E-Brokers are kept in the Virtual Image as a performance technique, although each is persistently stored in the Object Repository.

When an E-AutoPIA or E-PIA is processed, they and all of the objects they own are brought into the Virtual Image. The privilegeRules then employ the Virtual Interpreter to process expressions. A special method on Class EPIA is able to check for the existence of a specific TrustedToken.

E-Broker Objects

Each E-Broker object may represent an executable which is essentially external to the delivered E-Metro software which implements their InteractProtocols in a variety of ways. However, if all that is desired is information sharing between an E-AutoPIA and an E-PIA then the E-Broker requires no external executable. Instead, the Interaction Processor will know only that an exchange of data is to occur if the privilegeRules are obeyed. An E-AutoPIA's InteractInstruction should be authored as though only one E-PIA will be involved in the interaction with the E-AutoPIA. The Interaction Processor will automatically construct Sets of size equal to maximumInteractions for the output parameters.

E-Broker Adaptor and E-Broker Executable

All E-Broker objects are accessed using a unified protocol with the Virtual Interpreter. However, the type of each E-Broker executable is possible different. An E-Broker can be a C or C++ EXE, a C or C++ DLL, a Visual Basic program, an OLE 2 object, a SOM, or other. The procedure required to invoke the implementation of an InteractProtocol or service in each case is possibly different. Therefore, each new type of executable requires an E-Broker Adaptor which transforms the unified protocol invocations into the mechanism required to communicate the necessary signals and information to and from the E-Broker executable.

The Adaptor is always a DLL which is dynamically loaded and which always supports the following APIs (with signatures undetermined):

start() -- called just after Adaptor DLL loads

stop() -- called just before Adaptor DLL is unloaded

execute() -- this is the main entrypoint to execute an InteractInstruction. The name of the InteractProtocol must be passed in along with a linked list of all the parameters. The implementation of execute() is important because it must contain the code that binds the InteractProtocol name somehow to the executable code body representing the InteractProtocol's implementation. Execute then invokes the executable code body.

E-Broker Service API

As mentioned the E-Broker executable may be any of the executable types mentioned above. In order to facilitate the writing of code to perform the service/InteractProtocol that the E-Broker developer is trying to achieve, APIs are supplied. The executable must be capable of calling C procedures from a C DLL to perform these procedures.

Some of the identified useful procedures (with signatures undetermined) are:

collectTrustedEPIAs() -- This API is the only one that must be called by each E-Broker executable. It is the only way for the executable to get a hold of the "privilege compliant" collection of E-PIA's. This API takes as input, additional Rules to be applied for the collecting of E-PIA's. The Rules Processor is employed to combine the input Rules with the SQL statement formed prior to entry into the E-Broker. This produces the final SQL SELECT statement to be employed. The SELECT statement is performed to obtain the collection of E-PIA's that satisfy the SELECT. The collection is not returned yet, however, until the individual privilegeRules of the E-PIA's in the collection are checked by executing the Rules Processor.

Once the entirely "privilege compliant" collection is returned, the E-Broker executable may do whatever it wants with them before returning from the interaction. Note that in the case of small maximumInteractions values for an InteractInstruction, "order by" rules may be very important.

processCreditCard() -- interacts with the Transaction Server after obtaining credit card information for a purchase of something.

billActivity() -- interacts with the Transaction Server to bill an E-AutoPIA based on an activity name.

validateWithSecureCard() -- requires a specific Electronic Secure Card to be entered into a card reader in order to return TRUE. The specific Secure Card is identified by information and Rules supplied as parameters to this API.

Meta E-Brokers

Since some of the E-Metro System proper is implemented by E-Brokers, these special E-Brokers are known as "Meta" E-Brokers. So far, only two have been identified. More may be needed.

Home E-Broker

This E-Broker primarily needs to validate that the user editing or browsing information assets of a specific Home E-PIA is in fact the person who owns it. While this special E-Broker needs to be present in perhaps many E-Communities, its implementation may be overridden. For example, a one "Home" E-Broker implementation may provide strict security such that a Secure Card is absolutely required. Other "Home" E-Brokers may only require a password. A very loose E-Community may have no security.

DirectoryService E-Broker

This E-Broker attempts to maintain up to date knowledge of the entire E-Metro World. Only one DirectoryService E-Broker is needed per E-Community which is the top level parent at a site. Specifically, it keeps track of the public key of each online E-Metro Trusted Server Subsystem, of all E-Communities and the Internet addresses they are located at, as well as which E-Brokers reside in them and the names of the InteractProtocols each E-Broker owns. The Directory information must persist so it is stored in the Object Repository.

To keep the Directory Information up to date, every DirectoryService E-Broker periodically checks to see if there were any E-Community or E-Broker assignment changes. If there was, the DirectoryService E-Broker launches an E-AutoPIA with an Itinerary to visit each and every other DirectoryService E-Broker to notify them of the changes. The frequency of the period may be something like once per day since such changes are probably fairly infrequent. Note that a new E-Metro Site must obtain a copy of the entire current E-Metro directory upon installation.

Itinerary Interpreter

The Itinerary Interpreter understands that an Itinerary comes in one of two forms. Either the Itinerary has scripts or has no scripts. In either case, the Itinerary must have at least one InteractInstruction in the instructions OrderedCollection. In the case of no scripts, the instructions OrderedCollection is simply executed sequentially. In the case of scripts present, the InteractInstructions don't have to actually have parameters filled in because the script performs the call with parameters. In this case, the OrderedCollection of InteractInstructions merely represents the InteractInstructions that can be called from the scripts. There is no reason to have duplicate InteractInstructions for the scripts present case.

For the no scripts case, the Itinerary Interpreter merely increments an instructionPointer in the E-AutoPIA to keep track of which InteractInstruction in the Itinerary is the current one. When scripts are present, the Itinerary Interpreter must be able to compile and execute scripts. It achieves this only by employing the Virtual Interpreter. Each script is like a Smalltalk method in which the programming language may be employed to perform any general processing. The variables referenced in the scripts bind to the named information within the E-AutoPIA. At any time within a script, an InteractInstruction or even an entire Itinerary may be called by referring to the special variable "Instructions." The syntax for calling an InteractInstruction would be "Instructions at: aProtocolName performWith: aDictionaryOfParameters." In this example, aProtocolName is the name of the InteractProtocol to perform, while aDictionaryOfParameters is a Dictionary keyed on parameter name and valued on the values of the parameters.

Object Repository

The Object Repository is primarily meant to be the place where E-PIA's are maintained persistently. However, E-Communities and E-Brokers are stored there as well.

The Object Repository employs a simple object oriented interface over a relational database implementation (e.g. Oracle). The features of the simple object to relational table row design are as follows:

OR1. Each object is stored in a row of a database table with the row schema depicted in Figure 11.

OR2. The Object Identifier or OID is an Internet-wide unique numerical identifier which can be used to dereference the object. A technique that guarantees enterprise-wide uniqueness of the OID can be found in the prior art.

OR3. Each Object is considered to be stored in a PersistentMultiKeyedCollection which is just a grouping of rows that each have the same CollectionOID.

OR4. The keys are actually "exposed" information of an Object. When an Object is stored in a row, the Object data that has been identified to be exposed is copied into the appropriate columns of the row. Only the keys so identified can be used for fast E-PIA selection and collection because the database engine can be employed.

OR5. The actual objects themselves are stored in the BLOb column of a row.

An Object Repository is installed for each top level E-Community residing in an E-Metro Server. The database schema includes only three tables, one for E-Communities, one for E-Brokers, and one for the E-PIA's. The PersistentMultKeyedCollection schemas for E-Communities, E-Brokers, and E-PIA's are shown in Figures 11b, 11c, and 11d, respectively.

In each of the three tables, the CollectionOID refers to a different grouping concept. In the E-Community table, the ParentOID is a CollectionOID which treats a parent E-Community as a Collection of its children E-Communities. In the E-Broker and E-PIA tables, the ECommunityOIDs is the CollectionOID. The keys have been intentionally unidentified. This is because these keys should be determined by the needs of the E-Community and should be configurable via the E-Community Administration Tool.

It is important to note how access with hierarchical E-Communities is achieved. Suppose a query needs to allow any E-PIA that is a member of an E-Community or any of its children E-Communities to be in a result. First, the OIDs refering to all of the hierarchically reachable E-Communities must be discovered before the query and collected. The SELECT query then can be constructed with a bunch of ORed "CollectionOID==X" expressions.

Remember that most of the E-Community and E-Broker only processing is intended to be done directly in RAM in the Virtual Image. Only E-PIA's will be accessed in the Object Repository regularly.

Messaging Subsystem

As far as the Interaction Processor is concerned, the Messaging Subsystem is solely a source and sink of E-AutoPIA's which will request brokered services. When the service for an E-AutoPIA is complete, the Interaction Processor submits the E-AutoPIA to the Itinerary Interpreter. The Itinerary Interpreter interprets the current script as far as can until it gets to the very next InteractInstruction invocation. This will be immediate if there are no scripts and only a linear Itinerary of InteractInstructions. When the Itinerary Interpreter is finished, the Interaction Processor gets the E-AutoPIA back. The DirectoryService E-Broker is then conferred to see which site the E-AutoPIA needs to go to next. The Interaction Processor then submits the E-AutoPIA back to the Messaging Subsystem so it can be transported to its next destination. The details of the Messaging Subsystem are presented in the next section.

Messaging Subsystem

The Messaging Subsystem is employed exclusively for transporting E-AutoPIA's from one remote E-Community to another reliably. The messaging machinery pictured in Figure 12 is fairly simple. The Messaging Subsystem primarily relies on E-AutoPIA's arriving and being sent out of the Message Queue with the assistance of the external FTP Client and FTP Server. The E-AutoPIA Dispatchers are the primary interfacers to the DORMS Server. Note, however, that FTP is not required as the Messaging Subsystem implementation. Rather, any reliable means for sending information can be employed. Each of these subsystems are described in detail below.

E-AutoPIA Sender Dispatcher

When an E-AutoPIA is being sent to a remote E-Community, its FTP Internet address will have already been looked up by the Interaction Processor. Note that there is one FTP Internet address per top level E-Community. The Interaction Processor calls the E-AutoPIA Sender Dispatcher by handing off the E-AutoPIA to be sent along with this address.

The E-AutoPIA Sender Dispatcher puts the E-AutoPIA into an outgoing MessageQueue and then invokes the FTP Client to send the E-AutoPIA to its destination. If for any reason the FTP Client cannot send the E-AutoPIA right away, the FTP Client will read the entries in the outgoing Message Queue later and attempt to send the outgoing E-AutoPIA's then.

Message Queue

The Message Queue is really just an FTP file system. There is a single outgoing Message Queue and one incoming MessageQueue which can be two distinct FTP file directories.

E-AutoPIA Receiver Dispatcher

When the E-AutoPIA Receiver Dispatcher observes an arrived E-AutoPIA in the incoming Message Queue, it unmarshals the E-AutoPIA from its file format and then immediately calls up a new Interaction Processor server process to handle it. The E-AutoPIA file in the incoming Message Queue is not deleted until the E-AutoPIA is submitted to the outgoing Message Queue. This is required for recovery in case the DORMS Server crashes. Since only so many such server processes may be running simultaneously, a backlog of E-AutoPIA can build up in the incoming Message Queue. If the incoming Message Queue becomes empty, the E-AutoPIA Receiver Dispatcher may go to sleep and wake up periodically to check if anything has arrived. If there is a way for the FTP Server process to signal the E-AutoPIA Receiver Dispatcher, then the sleeping process can be asynchronously awakened on an as needed basis.

FTP Client

The FTP Client process really needs to perform a few more tasks than what a vanilla FTP Client does. It must delete the E-AutoPIA file in an outgoing Message Queue once it has successfully transfered the E-AutoPIA file to its next destination. Again, FTP is employed for transport since it is reliable. If errors occur during transmission, the FTP Client will know about it because transmission is directly point to point. The FTP Client will know that it must keep the failed E-AutoPIA in the outgoing Message Queue and try the transmission again later.

FTP Server

The FTP Server does not need to do anything special. It just stores incoming E-AutoPIA file transfers to the requested FTP directory. As mentioned the FTP directory designated represents the incoming Message Queue for one of the top level E-Communities at the local E-Metro Site.

Object Model Overview

This section describes the object model of a cyber-community based personal and private information protection and brokerage system called "E-Metro." The object model focuses on the user's view of objects in E-Metro. This object model provides a detailed description of how objects behave and how they relate to each other at the user level. In some cases the objects and classes at the user level will not map to an object or class in the target programming language. However, the transition from OOA objects to OOD objects is, for the most part, very smooth. The object oriented Booch notation is employed in the diagrams of this document as a means to communicate relationships of objects visually. Figure 23 depicts the basic notational symbols used and their meaning. The "uses for implementation" symbol is largely used for instance variables to denote that a Class needs the object in its implementation.

Foundation Objects

At the highest level of description of the E-Metro object model, there are E-Beings, E-Communities, and E-Brokers. An E-Being is the cyber-being concept mentioned previously. This is like a virtual person since it is supposed to "be" the person it represents, but in cyberspace. E-Beings reside in E-Communities in order to keep their information assets secure. Meanwhile, E-Brokers are the actual mediators of all E-Being interactivity in order to maintain the security provided by the E-Community as well as any designated personal (E-Being specific) security measures.

An E-Community is a cyber-community which is secure and trusted. An E-Community guarantees security in that only E-Beings with the proper E-Community privileges may enter or reside there. Security is also maintained within an E-Community in that the information assets of the E-Beings residing in it are only shared with those that have the proper personal privileges. An E-Community is trusted in that it guarantees that its contained E-Beings and visiting E-Beings will interact according to the rules that each E-Being has established, thus maintaining "trusted only" interactivity.

There exists at least one E-Broker per E-Community whose purpose it is to actually mediate privileged information sharing and interaction. In fact, both E-Being information sharing and interaction may only occur via an E-Broker.

E-Beings as Personal Information Agents

There are two primary subclasses of E-Beings in E-Metro. They are E Personal Information Agents (E-PIA) and E Auto Personal Information Agents (E-AutoPIA). The term "Personal Information Agent" exemplifies the purpose of the E-Beings in that they manage the electronic information assets of a real person. An E Corporate Information Agent (E CIA) representing a real corporation is also a possible subclass of E-Being that may be useful.

It is the E-PIA that shares its owned information while residing in an E-Community. However, such "passive" sharing may only occur with a more "active" E-PIA known as an E-AutoPIA. Only an E-AutoPIA with the proper privileges established by the perused E-PIA may interact with the E-PIA and enjoy the information sharing. An E-Broker 39 assigned to the E-Community 35, where the E-PIA 37 resides, mediates the privileged information sharing as shown in Figure 5. Note that only an E-AutoPIA 41 may initiate an activity.

If an E-AutoPIA desires to initiate interactions such as engaging in secured information sharing with other E-PIA's, requesting secured services from other E-PIA's, or performing secured transactions with other PIA's, the E-AutoPIA must visit the proper E-Broker for each specific activity. The list of interactions to be carried out by an E-AutoPIA is known as its *Itinerary*. As with E-PIA's residing at E-Communities, E-AutoPIA's are secured by an E-Broker and may only interact with other E-PIA's or E-AutoPIA's via an E-Broker. All information sharing and other general forms of interaction always occur via *InteractProtocols*. While the E-AutoPIA in Figure 6 is shown visiting several E-Brokers each located at a distinct E-Community, it is possible that multiple E-Brokers are present at a single E-Community and that they are each visited by a single E-AutoPIA depending on its desired activities.

Security and Transitivity of Trust

The reader should note the continual use of the qualifier "secured." Security is key in E-Metro as the chief means for maintaining the integrity of intended interactions between persons represented by E-PIA's. Strict security is necessary in order to ensure the intended E-PIA Interrelationships and to maintain the confidence of E-Metro users that only those who are meant to see specific information, can.

When an E-PIA gives some of its personal information to another E-PIA, the personal information given is still secured and owned by the original E-PIA. In fact, if the receiving E-PIA, in turn, passes another E-PIA's information on to a third E-PIA, E-Metro still knows the original owner of the personal information and continues to police access to the information according to *Transitive Privilege Rules* declared by the original E-PIA. This security paradigm pioneered by E-Metro is known as Transitivity of Trust. Transitivity of Trust means that:

If A trusts B with information A',
and B trusts C with information A',
then A trusts C with information A'.

This important concept guarantees to A that its information is never passed on to an entity which it does not trust according to the Transitive Privilege Rules it has declared for the data it has submitted.

It is easy for E-Metro to tell which E-PIA owns the information, because information is always passed as a version of the E-PIA which submitted its information. For example, suppose an E-PIA contains a rich set of information which includes birth date, address, phone number, etc. Further, suppose it wishes to submit only its phone number to another E-PIA during an interaction. The receiving E-PIA will actually receive an E-PIA object which contains only the phone number. More specifically, the E-PIA object received is a version of the original E-PIA which represents how the submitting E-PIA wishes to be perceived by the receiving E-PIA. Figure 6 depicts the "collection" of versions of E-PIAs 40 by a traveling E-PIA 41. The versions of E-PIA objects is the only manner in which information is maintained by E-PIAs in E-Metro. Figure 6 also depicts a version of the traveling E-AutoPIA that has been given to a non-traveling E-PIA 39 in one of the E-Communities.

<u>Subsystem Model</u>

Before presenting the details of object behavior and relationships, it is important to understand the subsystems that various users are aware of while using E-Metro. This section describes the activities of the major client and server subsystems.

<u>Modes of Use</u>

<u>Authoring Time</u>

<u>E-PIA</u>

E-PIA's have only two authorable items: their information <u>assets</u> and their <u>interactProtocols</u>. The assets need to be authored by employing some sort of hierarchical GUI. This GUI must allow for any data to be entered in a field and the field given a name. The GUI must also provide a means to create hierarchical structures by adding a sub-Folder concept. Hopefully, this hierarchical presentation is possible with some aspect of the HTML Form protocol.

InteractProtocols are strictly secured and may only be obtained from one of the E-Brokers residing in the same E-Community of the E-PIA being authored. A person may browse an E-Broker in an E-Community to obtain its protocolDirectory in HTML format. The returned HTML text includes an HTML Form representing the means to request obtaining one or more of the InteractProtocols listed. Actually obtaining a specific protocol may require some validation and/or paying a fee. When the InteractProtocol is actually obtained, it is stored in the E-PIA. However, the InteractProtocol has privilegeRules and a defaultMap which may be used as is or modified via HTML Forms.

E-AutoPIA

E-AutoPIA's have only to author their itineraries. This is because an E-AutoPIA is always instantiated from an E-PIA. To author an Itinerary, browsing an E-Broker for InteractProtocols is performed in the same manner as with E-PIA's. However, instead of retrieving an InteractProtocol, an InteractInstruction with parameters to fill in is obtained.

Forms Repository

Since the structure of E-PIA information is likely to be reused again and again, the HTML Forms necessary for filling out the information of various E-PIA structures can be stored in shared locations known as Forms or E-Being Repositories. These repositories can be simple FTP sites or possibly even Netscape Server Systems. It is also possible to store the HTML Forms associated with InteractProtocols, InteractInstructions, and Itineraries. However, as will be described later, E-PIA's employing these objects during runtime must have specific TrustedTokens associated with each of these objects in order to actually perform their intended activity.

Runtime

At runtime, a person who owns an E-PIA or E-AutoPIA does not see anything happening because all interactions are processed by E-Metro servers. However, to see progress or the latest results of interactions, an owner may retrieve his information assets and audit trail contained in his E-PIA(s) or E-AutoPIA(s). Note that a person may have multiple E-PIA's but that one is designated to be the *Home* E-PIA (more will be said about the home E-PIA later). As always, the presentation employs HTML text. In some cases, the state of an E-PIA may indicate that someone is waiting for further action on the owner's part to take place before the waiter can continue.

E-Community Administration Time

The E-Community Administrator needs to maintain, fix, and upgrade E-Brokers in an E-Community. The E-Community Administrator also needs to be able to have privilege to everything within an E-Community's boundaries (i.e. contained E-Communities) in order to make sure everything is running smoothly or find out where problems are. Backup and recovery functions must also be performed.

E-Metro Administration Time

An E-Metro Administrator employed by E-Metro who simply has access to everything does not exist. Each E-Community maintains and administrates its own assets autonomously according to the rules set up by the E-Community. This is a key ownership concept in E-Metro.

Client and Server Subsystems

User Perspective

The user's world consists only of E-Communities and the E-Brokers that belong to them, Forms Repositories, and the Netscape World Wide Web Browser. The user is aware that all of the E-Communities are attached to each other via the Internet and that they can be connected to via an "http://www." address. In the previous section it was mentioned how all of the data in E-Metro is transformed into an HTML format before being presented to the user. This transformation occurs on the server so that only the Netscape Client and an existing HTML conversant Client programming systems (e.g. C++ and NCAPI, or JAVA) are needed on the client workstation. Note that separate E-Communities may or may not actually be located at the same site in reality, but that this physical location consideration is irrelevant to the user.

Users may also want to use an Electronic E-Metro Secure Card to store E-PIA information assets. This may be needed for user validation while using some services, but may also be another way a person wishes to store his assets. It may be the only place a person wants to keep his assets at certain time -- it is totally a decision of the person owning the E-PIA where, when, and how their information assets are to be stored and/or shared.

Community Administrator Perspective

An E-Community Administrator employs the E-Community Administration Tool to manage one or more E-Communities on a single E-Metro World Wide Web Server. While each E-Community Administrator is aware of his E-Communities and their corresponding E-Brokers created by the E-Communities' development team, one E-Community Administrator designated the "E-Community Site Administrator" is also aware of the E-Metro and Netscape server processes which may need to be monitored and/or configured. Due to strict security measures required in E-Metro, the Administration Tool client application requires a direct log in directly to the E-Metro server rather than via any Internet protocols. Note that this restriction does not exclude remote login. An E-Community Administrator may also install a Forms Repository on the server if this is desired.

Detailed Object Model

A major feature of the E-Metro Object Model is that the first-class objects, namely E-PIA's, are not instances of Classes (at the user level), but rather just instances. Instead, they are dynamically assigned behavior at any time via protocol assignments. This provides a facility which adds behavior incrementally or subtracts behavior decrementally.

It is believed that this facility is necessary for the everyday changing needs and desires of a person desiring to do or explore different activities.

E-Being

B1. Purpose of E-Being-- An E-Being represents a "life" in the cyberworld of E-Metro. This life, or E-Being, must have at least one desire or one goal to interact with other E-Beings in order to exist on-line in E-Metro.

B2. An E-Being may represent the life of anything-- Note that "life" in cyberspace can be given to objects that normally would not be considered to have "life." For example, dead persons can be represented. While the primary goal of E-Metro is to have E-Beings represent real living people, they can also represent real animals, real corporations, real organizations, real inanimate objects, or even real objects that are stored or kept alive in electronic forms outside of E-Metro. Dead as well as totally fictitious (non-real) analogies of all of the above may also be represented.

B3. An E-Being is essentially an abstract root class, there are no direct instances of E-Beings.

Fundamental Information Objects

I1. Purpose of Fundamental Information Objects -- Information Objects hold data in E-Metro and are instances of Classes. It is important to mention fundamental data since the user interacts with various fundamental data types frequently.

I2. The base Classes are:

Class
Integer
String
Float
Boolean
OrderedCollection
Set
Dictionary
SQLStatement
Folder

ExecutableString
Compiler

I3. The base Classes have default protocol -- the default protocol corresponds to the methods of the Classes. For example, methods that obtain the size of an OrderedCollection, Set, and Dictionary are needed as well as specific indexes of OrderedCollections and specific keys of Dictionaries.

I4. An ExecutableString represents a piece of code that can be passed around as an object, interpreted when it needs to be, and processed -- ExecutableStrings require input arguments. Zero, one, and two argument ExecutableStrings should be supported. Each ExecutableString identifies the name of its Compiler/Interpreter. This allows the names referenced in the ExecutableSring to bind to information in different contexts controlled by the Compiler.

I5. SQLStatements are intended to provide a vehicle for fast look up of information while being able to reference E-PIA information -- since a reference to E-PIA information is hierarchical and, thus, not SQL compliant, SQLStatement Objects do not support SQL exactly. The references get fixed up by a special compiler provided by E-Metro.

I6. A Folder is able to store Objects using hierarchically arranged keys.

I7. An extended set of Classes will have to be provided to support the various standard object protocols -- some examples are OLEObject, OpenDocObject, and SOMObject. This is needed since some information asset data will be desired to be stored in such formats by persons.

I8. An extended set of Classes will have to be provided to support various multimedia -- some examples are Audio, Video, Picture.

I9. The very important Dictionary object appears as simply a list of keyed objects to the client of a Dictionary-- The keyed objects are frequently referred to as the "values" of the Dictionary. A key is used to look up a value or object in the Dictionary. Keys are typically Strings or Symbols (as in Smalltalk) and are used as names for the objects so keyed. But keys can be any object the programmer sees as useful as a key. The values can be any object as well. An example Dictionary is shown below.

keys	Values
"FirstName"	a String object
"Height"	a Float object
"Street"	a String object

E Personal Information Agent (E-PIA)

PIA1. Purpose of E-PIA -- An E-Being which represents a real person and maintains the real person's information assets that are intended to be shared in a secured fashion.

PIA2. An E-PIA may exist on an Electronic E-Metro Secure Card.

PIA3. Each E-PIA consists of an unstructured Folder that is created and edited at authoring time -- the editing is to be accomplished with HTML forms which is facilitated by the E-Metro client subsystem.

PIA4. Each E-PIA may be assigned a Set of InteractProtocols by the E-PIA's owner at authoring time -- E-PIA's share information at runtime only via an InteractProtocol and only one protocol at a time.

PIA5. An E-PIA contains a Set of Privilege Rules which must be checked and satisfied on all InteractProtocol executions.

PIA6. An E-PIA contains a Set of TrustedTokens which it obtains from E-Brokers at authoring time -- some or all of these may be used anytime the E-PIA interacts.

PIA7. An E-PIA contains an audit trail of all interactions that occur with it -- each RecordedEvent stores the information about an interaction that is interesting (e.g. time started, time completed, any access violations, etc.)

For an E-PIA, everytime an InteractProtocol is performed on it, a RecordEvent object is added to its auditTrail. For an E-AutoPIA, everytime an InteractInstruction is performed in its Itinerary, a RecordEvent object is added to its auditTrail. The contents of the RecordEvent objects needs to be determined based on audit trail needs during E-Metro development. Additionally, filtering of certain RecordEvents may not wish to be recorded for performance or disk space reasons. Finally, the point of the audit trail is to allow the owner of the E-PIA or E-AutoPIA to look back on what has been done.

PIA8. An E-PIA may exist in multiple E-Communities simultaneously.

PIA9. A Home E-PIA must be designated if there are more than one E-PIA's for a given person -- The Home E-PIA contains the E-Community names where the other E-PIA's are located.

PIA10. Only the Home E-PIA may be modified at authoring time.

PIA11. Each E-PIA contains a Certificate with its the name of the person it represents and that person's public key-- it is assumed that at any time a process can validate the (name, public key) pair by querying the appropriate certificate authority.

PIA12. A Version of an E-PIA is constructed at runtime when information from an E-PIA is supplied in an information interaction -- an E-PIA version contains only:

certificate
assets
privilegeRules.

The possibility of including an auditTrail should be considered. Note that versions of E-PIAs typically represent a subset of information actually contained in a source E-PIA, so that assets may be a copy of only a small part of the original assets folder. The certificate assists in validating that the information actually originated from the E-PIA whose name is stated in the certificate. This is important as the information can be passed on in "transitively trusted" third party information sharing. Additionally, each individual piece of information in the original E-PIA assets Folder is encrypted with the E-PIA's private key when assembled at the E-PIA owners personal workstation. By using the public key in the certificate in a version of an E-PIA, another E-PIA may have the data decrypted and know for sure that the version of the E-PIA is, in effect, "signed" by the owner.

TrustedToken

TT1. Purpose of TrustedToken -- A TrustedToken is obtained at authoring time from an E-Broker along with some other object in order to secure use of the object, typically an interaction or service, that the E-Broker brokers. The TrustedToken grants the new owner a primary and necessary privilege (but not necessarily sufficient privilege) to performing the secured interaction.

TT2. When a TrustedToken is given to an E-PIA author, it is encrypted with the E-PIA author's private key at his local machine -- the E-Broker then remembers the E-PIA author's public key.

TT3. When a secured interaction is requested, the E-Broker must be given the E-PIA's name and the encrypted TrustedToken. From this pair, the TrustedToken can be decrypted with the public key obtained from a previous authoring session -- the E-Broker knows that the E-PIA requesting interaction is trusted only if the TrustedToken can be decrypted successfully.

InteractProtocol

SP1. Purpose of InteractProtocol-- An InteractProtocol object designates specific named information and the conditions which must be true in order for the specific information to be shared. The shared information is packaged in the form of a version of an E-PIA. The version of the E-PIA is specifically defined by the outputs of the InteractProtocol.

SP2. An InteractProtocol must have a name.

SP3. An InteractProtocol consists of a 5-tuple of

1) Set of input Parameters

2) Set of output Parameters defining which information to store in version of E-PIA that will be shared

3) Default parameter mapping

4) Set of Privilege Rules for immediate sharing to occur

5) Set of Transitive Privilege Rules for sharing of version of E-PIA to occur by third parties (transitive sharing). At runtime, these rules are copied and placed in the privilegeRules of the version of E-PIA that will be shared.

6) Enable boolean -- an Interact may be disabled

SP4. Execution of an InteractProtocol creates a version of the E-PIA based on the runtime outpu parameter values. This version of the E-PIA is what is given and shared with the E-AutoPIA that is interacted with-- however, if ALL output parameter values are previously obtained E-PIA versions, then an E-PIA version is not created. Instead the information is passed along in the originally obtained E-PIA forms.

NOTE: Consideration to passing data as raw data in some situations, rather than always as a version of an E-PIA, should be investigated. Perhaps passing data as an E-PIA version or raw data can be a choice during InteractProtocol and InteractInstruction authoring.

SP5. The version of E-PIA that is shared, has each of its pieces of fundamental information encrypted with the E-PIA's private key-- this encryption occurs at the E-PIA's personal client workstation when the information for the Home E-PIA is assembled. Later, another E-PIA or process can decrypt the information by using the public key of the version of the E-PIA found in its certificate.

Note that since private keys are never located in servers, the input or output parameters used to pass data in an E-PIA version may need to be severely restricted in expression richness, since in general, an expression result would require re-encryption with the private key.

SP6. An InteractProtocol's Default parameter mapping is a Dictionary showing the name of zero or more Parameters and a hierarchical name that each listed parameter is associated with.

SP7. An InteractProtocol may inherit an existing InteractProtocol -- the subclassing InteractProtocol inherits the 4-tuple to which it may add more Parameters and Rules.

SP8. An E-PIA may overwrite privilegeRules in any or all of the InteractProtocols assigned to it.-- the authoring time E-PIA facility must provide this ability.

SP9. The default map is meant to act as an assistant to the construction of a corresponding InteractInstruction-- Since InteractInstructions must "fill in" the parameters of an InteractProtocol with ExpressionStrings, it might be nice to fill in some or all of the parameters with the commonly expected defaults. The table below shows an example default map.

Parameter name	default value
"FirstName"	FirstName
"Height"	profile.physicalAttributes.height
"Street"	address.street

The analogy in C/C++ would be the function prototype:

processSuperficialInfo(String* FirstName, Float* Height, String* Street)

that would be automatically filled with the default call:

processSuperficialInfo(firstName,
profile.physicalAttributes.height, address.street)

Realize that the default parameters reference variables that reference (and hence, bind to) the E-AutoPIA's Folder.

Parameter

P1. Purpose of Parameter-- A Parameter is a named "passageway" for an InformationObject to either be input to an interaction or be output from an interaction.

P2. Each Parameter is a 2-tuple of (name, validation Rule)-- the validation Rule may be used to verify type at runtime. For example, the expression "isKindOf: aClass" determines whether the runtime parameter value is an instance of aClass or one of its subclasses. A more complex example would be the combination of a type validation and a general expression such as:

(myself isMemberOf: Float) & (myself > 203500.00).

Rule

R1. Purpose of Rule-- A Rule is assigned to some activity and describes the conditions under which the activity will occur. Otherwise the activity does not occur. It is important to note that the Rule grammar needs to be multiple party centric.

R2. Rules are ExecutableStrings representing expressions that evaluate to TRUE or FALSE.

R3. The Rule expression grammar must recognize multiple contexts -- in the most interesting case, two E-PIA's can meet so we are interested in two contexts. The two contexts are the sharer and the sharee.

R4. To facilitate reference to two objects that meet, the keywords "myself" and "yourself" will be established in the grammar -- myself refers to the sharer (sharing E-PIA) while yourself refers to the sharee (E-PIA that meets with sharer).

R5. To facilitate reference to more than one object that meet, the keyword "yourselves" shall be established in the grammar -- yourselves refers to the Set of sharees (E-PIA's that meet with sharer). Indexes can be used to refer to specific sharees. Yourself is always the same as yourselves at index 0.

R6. References are used to refer to a hierarchically positioned piece of data in an object -- a Reference may use names separated by spaces to denote hierarchical access.

EXAMPLE: To restrict an activity to only those over 6 feet tall a sharer's rule might be yourself profile physicalAttributes height > 6

R7. Rules are meant to be interpreted at runtime -- therefore, only some errors are intended to be found at authoring time.

<u>E Auto Personal Information Agent (E-AutoPIA)</u>

APIA1. Purpose of E-AutoPIA -- E-AutoPIA's are intelligent agents that do work on behalf of a Home E-PIA. An E-AutoPIA is an E-PIA which initiates tasks intending to interact with other E-PIA's in local or remote E-Communities.

APIA2. An E-AutoPIA is an E-PIA which has at least one Itinerary assigned to it.

APIA3. An E-AutoPIA may only be launched, i.e. execute an Itinerary, from a Home E-PIA.

APIA4. A Home E-PIA may launch multiple E-AutoPIA's.

Itinerary

I1. Purpose of Itinerary-- An Itinerary consists of a list of InteractInstructions that are to be performed.

I2. An Itinerary must have a name.

I3. An Itinerary contains a Set of Privilege Rules -- these Rules must be satisfied for all InteractInstructions and are in addition to the Set of Privilege Rules defined for the E-AutoPIA.

I4. An Itinerary contains a Set of Transitive Privilege Rules -- these Rules govern transitive sharing of any E-PIA versions (or E-AutoPIA versions in this case) that are shared by InteractInstructions within the Itinerary. The Transitive Privilege Rules are in addition to any Transitive Privilege Rules defined for an individual InteractInstruction itself. At runtime, these Rules are copied and placed in the privilegeRules of the version of E-PIA that will be shared.

I5. An Itinerary contains a Set of zero or more Scripts -- a Script is just an ExecutableString written in some programming language. Scripts can control when and how InteractInstructions are to be performed. Thus, Scripts are just general programming code to do whatever processing a programmer wants to do. However, a Script can call an InteractInstruction by its name and pass it any variables as parameters that are within scope. Only the InteractInstructions of an Itinerary or superclassed Itinerary may be called from the Scripts that are attached to the same Itinerary object. The net affect is that the InteractInstructions can get called in any order. InteractInstructions are only called in sequence when no Scripts are present in the Itinerary.

I6. An Itinerary consists of one or more InteractInstructions -- if there are no Scripts, then the InteractInstructions are executed sequentially.

I7. An Itinerary may inherit an existing Itinerary -- the subclassing Itinerary inherits the Rules, Scripts, and Itinerary of the parent Itinerary.

InteractInstruction

II1. Purpose of InteractInstruction -- InteractInstructions are the single point in the whole system that cause interactions between E-PIA's (actually, E-AutoPIA and E-PIA) to take place. Each InteractInstruction describes the interaction that will occur and the rules under which it can occur. It is also important to note that is the execution of an InteractInstruction that is the only way to exchange information assets.

II2. Each InteractInstruction is a 5-tuple of

1) E-Community name

2) InteractProtocol name

3) Parameter assignments

4) Set of Privilege Rules for immediate sharing to occur

5) Set of Transitive Privilege Rules for sharing of version of E-AutoPIA to occur by third parties (transitive sharing).

6) Maximum number of interactions

II3. Execution of an InteractInstruction creates a version of the E-AutoPIA based on the runtime input parameter values. This version of the E-AutoPIA is what is given and shared with E-PIA that is interacted with-- however, if ALL input parameter values are previously obtained E-PIA versions, then an E-AutoPIA version is not created. Instead the information is passed along in the originally obtained E-PIA forms.

II4. The version of E-AutoPIA that is shared, has each of its pieces of fundamental information encrypted with the E-AutoPIA's private key-- this encryption occurs at the E-AutoPIA's personal client workstation when the information for the Home E-PIA is assembled. Later, another E-PIA or process can decrypt the information by using the public key of the version of the E-PIA found in its certificate.

Note that since private keys are never located in servers, the input or output parameters used to pass data in an E-AutoPIA version may need to be severely restricted in expression richness, since in general, an expression result would require re-encryption with the private key.

II5. The privilegeRules must be satisfied for the InteractInstruction to be performed -- they are in addition to the Set of Rules for the Itinerary as well as the Set of Rules for the executing E-AutoPIA.

II6. The transitivePrivilegeRules are copied and placed in the privilegeRules of the version of E-PIA that becomes shared due to the InteractInstruction's execution.

II7. Only maximumInteractions of E-PIA's will participate in the execution of an InteractInstruction -- this value may be infinity.

II8. An InteractProtocol must be able to generate an HTML Form representing an InteractInstruction with Parameters ready to be filled in.

II9. There is a special "Update Home" InteractInstruction which updates the latest information in the E-AutoPIA into its Home E-PIA -- an implicit "Update Home" InteractInstruction is executed at Itinerary termination. Note that this special InteractInstruction requires the E-AutoPIA to physically visit its Home E-PIA.

Clarifying the Relationship between InteractProtocols and InteractInstructions

An InteractProtocol maintains essentially a template relationship to an InteractInstruction. An InteractProtocol is represented by a signature of parameters to be "filled in," while the InteractInstruction counterpart is the same except with parameters "filled in."

InteractProtocols and InteractInstructions are both authoring time entities. The InteractProtocols represent the services provided by an E-Broker and are authored along with an E-Broker. InteractInstructions are authored during the construction of an Itinerary for an E-AutoPIA. Each

InteractInstruction represents the call of a "requested interaction" or InteractProtocol.

Also, shown in Figure 19 are privilegeRules that are part of InteractProtocols. Each privilegeRules is a Set of Rule objects. As described previously, each Rule is an ExpressionString which employs the Rule Compiler to process. In order for an InteractProtocol to execute all of the Rules in the privilegeRules must be true. As mentioned previously, the Rules can reference both myself (the provider of the InteractProtocol interaction) and yourself (the E-AutoPIA requesting interaction). It was also shown that Parameter objects have validation Rule objects. These Rules are applied only to the actual parameter being passed in.

Figure 18 also shows InteractInstructions as having privilegeRules. Such Sets of Rules may be added by an E-AutoPIA author as he is constructing an Itinerary and has decided that certain Rules should be maintained regardless of the InteractProtocol's privilegeRules that the InteractInstruction refers to.

E-Community

C1. Purpose of E-Community -- An E-Community provides a grouping concept for E-PIA's and other E-Communities. In this regard, an E-Community also provides security for the objects it groups.

C2. An E-Community is an E-Being -- an E-Community maintains a E-Metro notion of life concept in that it has goals to share information and interact with general E-Beings.

C3. An E-Community must have a name.

C4. E-Communities contain zero or more E-PIA's -- the E-PIA's reside together because they share the same goals as far as sharing information. Thus, E-AutoPIA's looking for specific E-PIA's will know which E-Communities to visit.

C5. E-Communities may contain other E-Communities such that they can be arranged hierarchically -- The contained E-Communities may, in turn, each contain one or more as well. The hierarchy must be strict, however, in that no E-Community is contained by more than one parent E-Community.

C6. Each E-Community consists of E-Brokers that the E-Community has decided to make available.

C7. Each E-Community contains no InteractProtocols because they may not interact.

E-Broker

BR1. Purpose of E-Broker-- An E-Broker is required for all inter-PIA Interactions. E-Brokers guarantee that the all E-PIA's involved in an interaction have the rights based on InteractProtocols to interact in the manner that the interaction is performed.

BR2. Each E-Broker owns one or more InteractProtocols.

BR3. An E-Broker contains the subsystems implementing all InteractProtocols it owns.

BR4. An E-AutoPIA may only interact with an E-PIA in an E-Community which has an E-Broker with the InteractProtocol identified by the E-AutoPIA's current InteractInstruction.

BR5. An E-Broker must generate a unique TrustedToken for each of its InteractProtocols.

BR6. InteractInstructions may only be authored by obtaining the corresponding InteractProtocol from an E-Broker.

BR7. An E-Broker mediates the interaction between an E-PIA and an E-AutoPIA as follows:

1) Validate that the E-AutoPIA satisfies the E-Community's privilegeRules.

2) Validate that E-AutoPIA has a decryptable TrustedToken corresponding to the InteractProtocol being executed.

3) Validate E-AutoPIA's privilegeRules.

4) Validate the E-AutoPIA's Itinerary privilegeRules.

5) Validate the E-AutoPIA's current InteractInstruction privilegeRules.

6) Validate the privilegeRules of any transitively exchanged E-PIA versions that are going to be passed as an input or output Parameter.

7) Call the entrypoint of the E-Broker which corresponds to the InteractProtocol's implementation -- only the Parameters that passed validation in (6) of the E-AutoPIA's InteractInstruction are passed in.

8) Determine the specific collection of E-PIA's involved in the interaction -- this is based on three items:

a) Validation Tasks 3 through 5 above.

b) An additional selection rule supplied via an E-Metro API call within the E-Broker executable.

c) The privilegeRules of the E-PIA's that are selected based on a) and b)

9) The E-Broker's implementation is executed -- if any failures occur, the InteractInstruction is not completed successfully.

10) Only the Parameters that passed validation of the E-PIA's InteractProtocol are passed out.

BR8. Each E-Broker offers an "interactProtocolDirectory" service -- this service answers a generated HTML document describing all of the InteractProtocols provided by the E-Broker.

BR9. Each E-Broker offers a "getRightsToInteractProtocol" service-- the service answers the InteractProtocol with the TrustedToken. It is important to note that this service can be implemented in any manner by the E-Broker. For example, this service may be where the person desiring rights to an InteractProtocol has to validate who he is and/or pay to obtain privileges. The E-Broker can refuse to answer a TrustedToken for any reason.

BR10. E-Brokers may be directly interacted with without regard to the E-Community privileges of the E-Community they belong to -- however, interaction with an E-Broker does require privileges to be obeyed of any parent E-Communities.

Having described and illustrated the principles of our invention with reference to a preferred embodiment, it will be apparent that the invention can be modified in arrangement and detail without departing from such principles. As such, it should be recognized that the detailed embodiment is illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as may fall within the scope and spirit of the following claims and equivalents thereto:

We claim

1. For implementation on at least one computer network server, a computer-networked system for providing secured exchange of an entity's information over a computer network, said computer-networked system comprising:

computer-implemented means for establishing at least one network community, each said network community being fixed in computer readable media in one of said computer network servers;

computer-implemented means for securely encapsulating an entity's personal information and rules governing said information of a plurality of community network members in the form of a plurality of community member profiles, each said community member profile being fixed in computer readable media in one of said computer network servers;

computer-implemented means for exchanging said entity's personal information according to at least one set of information exchange rules.

2. The computer-networked system of claim 1, wherein said network community is further comprised of:

a community network name;

a plurality of community network member profiles;

a set of community network member admissions rules; and

a set of community network information exchange rules.

3. The computer-networked system of claim 2 wherein said network community is further comprised of:

an electronic broker which securely processes said rules governing said personal information and to ensure that said rules governing said personal information are satisfied before said personal information is processed.

4. The computer networked system of claim 1 wherein said computer-implemented means for establishing at least one network community further comprises means for authoring and administrating said personal information and rules governing said information.

5. The computer networked system of claim 4 wherein said means for authoring and administrating said personal

information and rules governing said information is a distributed object resource management system (DORMS).

6. The computer-networked system of claim 1, wherein each said community network member profile is further comprised of:

a digital certificate containing the name of the community member;

at least one personal information object; and

at least one member information exchange rule corresponding to each said personal information object.

7. The computer networked system of claim 6 wherein said personal information object is selected from the group consisting of data, pictures, videos, sound clips and digital objects.

8. The computer networked system of claim 6 wherein said personal information object is selected from the group consisting of information objects defined by said network community.

9. The computer networked system of claim 6 wherein said personal information object is selected from the group consisting of personal data, financial data, medical data, and professional data.

10. The computer networked system of claim 6 wherein said digital certificate assures that said personal information originates from said entity.

11. The computer networked system of claim 6 wherein said digital certificate is issued by a third party which verifies and corroborates said personal information asserted by said entity.

12. The computer-networked system of claim 3, wherein said means for exchanging personal information is further comprised of:

computer-implemented means for creating a home electronic personal information agent (home EPIA) which contains all of said entity's personal information; and

computer-implemented means for creating an electronic personal information agent (EPIA) which contains all or some of said entity's personal information.

13. The computer-networked system of claim 12 wherein said home electronic personal information agent commands and controls said electronic personal information agent.

14. The computer-networked system of claim 12, wherein said means for exchanging personal information is further comprised of:

computer-implemented means for dispatching said electronic personal information agent to said destination community network.

computer-implemented means for causing said first destination community network to receive, verify, and process said electronic personal information agent.

computer-implemented means for utilizing said electronic broker upon verification that said electronic personal information agent satisfies destination community network interaction rules.

computer-implemented means for causing said electronic broker to search the community network member profiles according to a search criteria from said electronic personal information agent.

computer-implemented means for causing said electronic broker to extract a set of member information exchange rules from each said community network member profile matching said search criteria from said electronic personal information agent;

computer-implemented means to exchange value possessed by each electronic personal information agent according to:

a) said set of community network exchange rules;

b) said set of member information exchange rules from said electronic personal information agent; and

c) said set of member information exchange rules from each said community network member profile matching said search criteria from said electronic personal information agent;

computer-implemented means for dispatching said electronic personal information agent to said originating community network upon successful exchange of value;

computer-implemented means for dispatching said electronic personal information agent to said originating community network upon unsuccessful exchange of value.

15. The computer-networked system of claim 14 wherein said computer-implemented means for causing said electronic broker to search the community network member electronic personal information agents further comprises:

computer-implemented means for said electronic broker to take a request criteria from said electronic autonomous personal information agent; and

means for converting said request criteria to a standard database query request.

16. The computer-networked system of claim 14 wherein said computer-implemented means for causing said transacting agent to extract a set of member information exchange rules further comprises:

means for generating electronic personal information agents which satisfy said request criteria; and

means for comparing the information processing requirements of each of said electronic personal information agents.

17. The computer-networked system of claim 1, wherein said computer network is selected from the group consisting of the Internet, wireline telecomputing devices and wireless telecomputing devices.

18. A computer usable medium having computer readable program code means embodied therein for causing at least one computer to implement a system for providing secured agent-rule based exchange of personal information over a computer network, said computer readable program code means in said article of manufacture comprising:

computer readable program code means for causing a computer to establish at least one network community;

computer readable program code means for causing a computer to encapsulate personal information of a plurality of community network members in the form of a plurality of community member profiles; and

computer readable program code means for causing a computer to exchange personal information according to at least one set of information exchange rules.

19. A method for exchanging an entity's information on a computer network, said method being implemented on at least one computer network server and comprising the steps of:

authorizing said individual to join at least one network community, where said network community further comprises a community name and a set of admission rules;

acquiring said information wherein said information comprises at least one object;

storing said information in a manner whereby said information objects may be assigned at least one rule, wherein said rule states the necessary conditions for others to access and process said information objects;

creating an agent, said agent comprising said information; and

assigning an itinerary to said agent, said itinerary directing the activity of said agent.

20. A computer usable medium having computer readable program code embodied therein for exchanging an entity's information on a computer network, said computer readable program code in the article of manufacture comprising:

computer readable program code for establishing at least one network community;

computer readable program code for establishing a plurality of individuals as members of said network community; computer readable program code for establishing an agent for each said individual; and

computer readable program code for establishing an itinerary for said agent.

21. The computer usable medium as in claim 20, wherein said network community further comprises a community name and a set of admission rules.

22. The computer usable medium as in claim 20 further comprising computer readable program code for acquiring

information on each said entity, wherein said information further comprises personal information objects and rules and wherein said rules define the necessary condition to process said personal information objects;

23. The computer usable medium as in claim 20 wherein said agent further comprises at least a sub-set of said personal information.

24. The computer usable medium as in claim 20 further comprising computer readable program code for allowing said agent to query said personal information, whereby said rules are checked and access limited to said information objects that meets said necessary conditions.

25. An electronic-being to command and control information objects belonging to an entity, said electronic-being fixed in media in computer readable form and present in a general purpose computer system, comprising:

a digital certificate;

information objects relating to said person or entity; and

rules related to said information objects whereby said rules govern the accessing and processing of said information objects;

26. An electronic-being as in claim 25 wherein said electronic being is further comprised of:

means for creating an audit trail of all information processing and electronic personal agent information interactions;

trusted tokens; and

a set of interact protocols.

wherein said trusted tokens grants said electronic being a primary and necessary privilege to perform a secured interaction and wherein said interact protocols govern the interaction with other electronic beings.

27. An electronic-being as in claim 26 wherein said interact protocols are further comprised of:

privilege rules which determine if said electronic being has the necessary rights to begin information processing; and transitive privilege rules which allow said electronic being to state what conditions its information objects, if passed onto another entity in the form of another electronic personal information agent, must maintain, protecting the original entities command and control.

28. An autonomous electronic being to an entity's information, said autonomous electronic being fixed in media in computer readable form and present in a general purpose computer system, comprising:

a digital certificate;

information relating to said person or entity, whereby said information is further comprised of at least one information object;

rules related to said information objects whereby said rules govern the accessing and processing of said information objects; and

an itinerary directing the activity of said agent.

29. An autonomous electronic being in claim 28 wherein said itinerary further comprises:

an itinerary name;

transitive privilege rules related to said information objects whereby said transitive rules define a necessary condition for the processing of said information objects to parties subsequent to processing by said entity;

interact instructions which direct the actions of said autonomous electronic being; and

privilege rules which must be checked and satisfied on all interact instructions.

30. An autonomous electronic being as in claim 29 wherein said interact instructions further comprises:

privilege rules which must be checked and satisfied on all interact instructions; and

transitive privilege rules related to said information objects whereby said transitive rules define a necessary condition for the processing of said information objects to parties subsequent to processing by said entity.

31. An electronic community for use in a personal

security and exchange tool being fixed in a computer readable medium comprising:

a name for said electronic community;

a single or plurality of electronic personal information agents;

a single or plurality of electronic brokers;

a single or plurality of additional electronic communities.

32. A trusted electronic exchange process operating on a programmable computer system, said process comprising the steps: receiving a first communication from a first source, with said first communication further comprising:

a certificate having at least the name of said first source;

information relating to said first source, whereby said information is further comprise of information objects;

rules related to said information objects whereby said rules define a necessary condition for the processing of said information objects;

verifying said first communication was originated by said first source;

verifying said rules were originated by said first source;

executing said rules on said information objects to determine if said information objects meet said necessary condition;

collecting electronic personal information agents that satisfy said criteria;

dispatching said electronic personal information agents to request another electronic personal agent or autonomous electronic personal agent.

33. A method for an entity to command and control processing of their individual information on a computer network, said method being implemented on at least one computer network server and comprising the steps of:

becoming a member of at least one network community, where said network community further comprises a community name and a set of admission rules;

compiling said individual information whereby said individual information is further comprised of at least one individual information object;

assigning at least one rule to said individual information objects, where said rule states the necessary conditions for others to process said information objects; and

assembling and directing an electronic agent, said agent comprising said individual information, said rules, and an itinerary, said itinerary directing the activity of said agent.

34. A networked computer system for securing the flow of personal information comprising:

means for providing a mechanism for entities to securely author and encapsulate personal information objects and processing rules governing the exchange and processing of personal information; and

means for empowering the entity to command and control its personal information within a networked computing environment.

35. A distributed object resource management system for use in a personal security and exchange tool being fixed in a computer readable medium comprising:

a messaging subsystem which receives and dispatches electronic autonomous personal information agents;

an interaction processor which processes requests from said electronic autonomous personal information agents through an electronic broker;

a rules processor which validates and processes rules from electronic autonomous personal information agents and handles conversions to SQL statements;

an electronic broker which securely intermediates between electronic autonomous personal information agents and electronic personal information agents; and an object repository which is where electronic brokers, electronic personal agents and electronic communities are maintained persistently.

36. An electronic bazaar for the purpose of facilitating electronic commerce by auction comprising:

an electronic bazaar electronic broker which securely processes a transaction to ensure that rules are satisfied before a transaction is processed;

an electronic personal information agent which securely encapsulates entities' personal information objects and rules governing processing;

commercial activity dispatcher which handles all incoming transaction requests with said electronic bazaar electronic broker;

public product database which persistently stores product information processed by said electronic bazaar electronic broker;

trusted token processor which stores and processes public keys from said electronic personal information agents and issues and validates trusted tokens presented by said electronic personal information agents;

advertiser directory which stores and processes orders, product information and order forms as initiated by transaction requests; and

private activities database which stores advertiser pending orders, inventories, and information necessary to carry out transactions.

37. An electronic bazaar as in claim 36 which operates on a semi real-time basis.

38. An electronic bazaar as in claim 36 which processes aggregate orders utilizing electronic personal information agents.

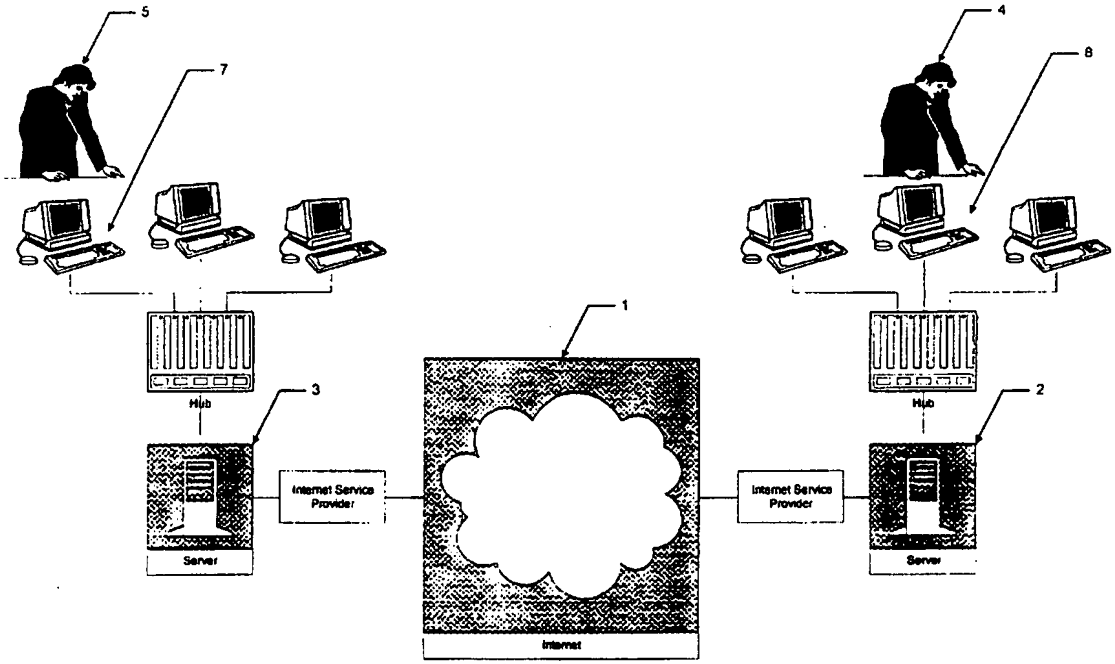

5
7
4
8
1
3
2
Hub
Hub
Server
Server
Internet Service Provider
Internet Service Provider
Internet

Figure 1

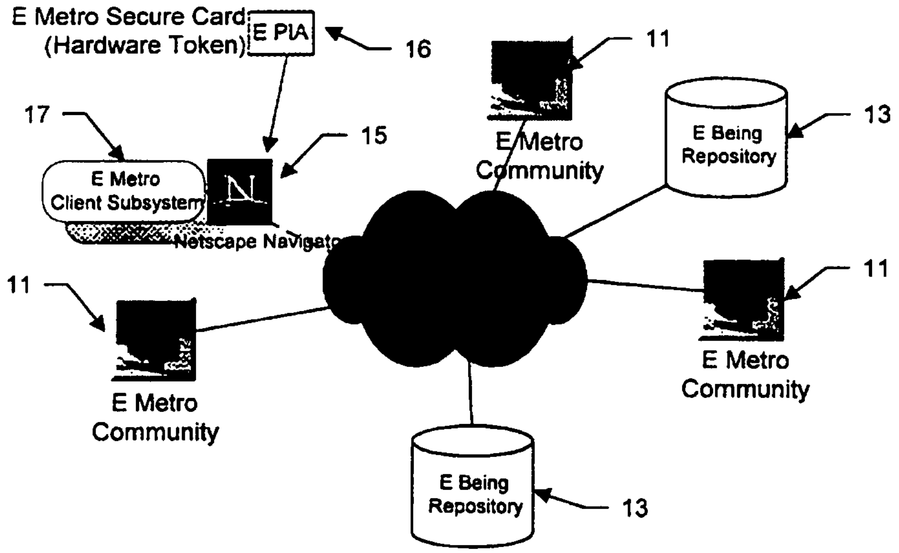

E Metro Secure Card
(Hardware Token)
E PIA
16
17
E Metro
Client Subsystem
15
Netscape Navigato
11
E Metro
Community
E Being
Repository
13
11
E Metro
Community
11
E Metro
Community
E Being
Repository
13

Figure 2

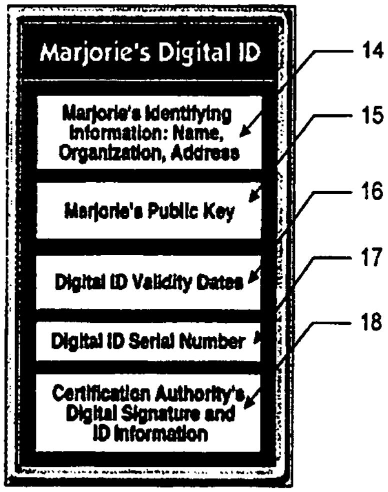
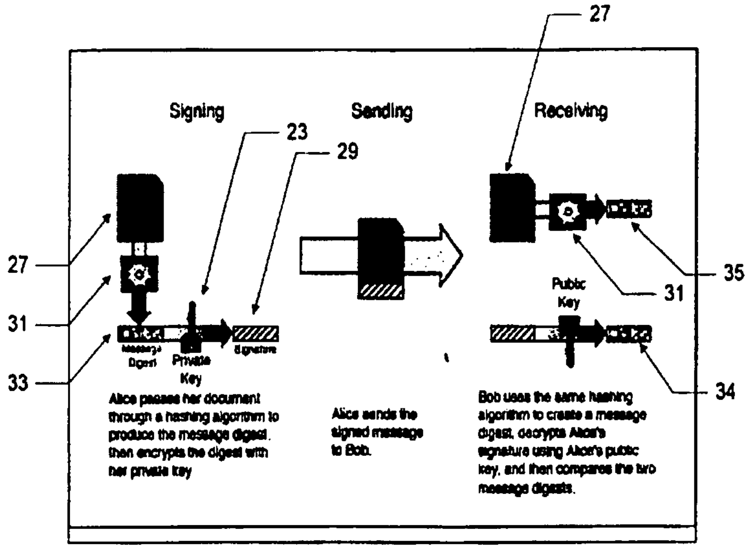

Marjorie's Digital ID
Marjorie's Identifying Information: Name, Organization, Address
Marjorie's Public Key
Digital ID Validity Dates
Digital ID Serial Number
Certification Authority's Digital Signature and ID Information
14
15
16
17
18

Figure 3



Alice passes her document through a hashing algorithm to produce the message digest. then encrypts the digest with her private key

Alice sends the signed message to Bob.

Bob uses the same hashing algorithm to create a message digest, decrypts Alice's signature using Alice's public key, and then compares the two message digests.

Figure 4

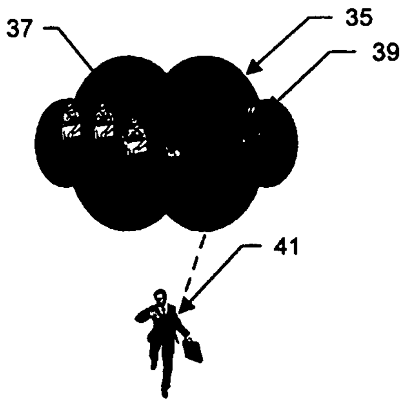


Figure 5

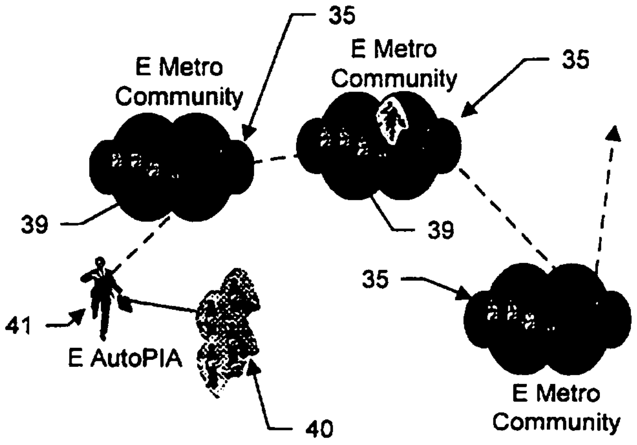

35
E Metro Community
35
E Metro Community
35
39
39
35
41
E AutoPIA
40
E Metro Community

Figure 6

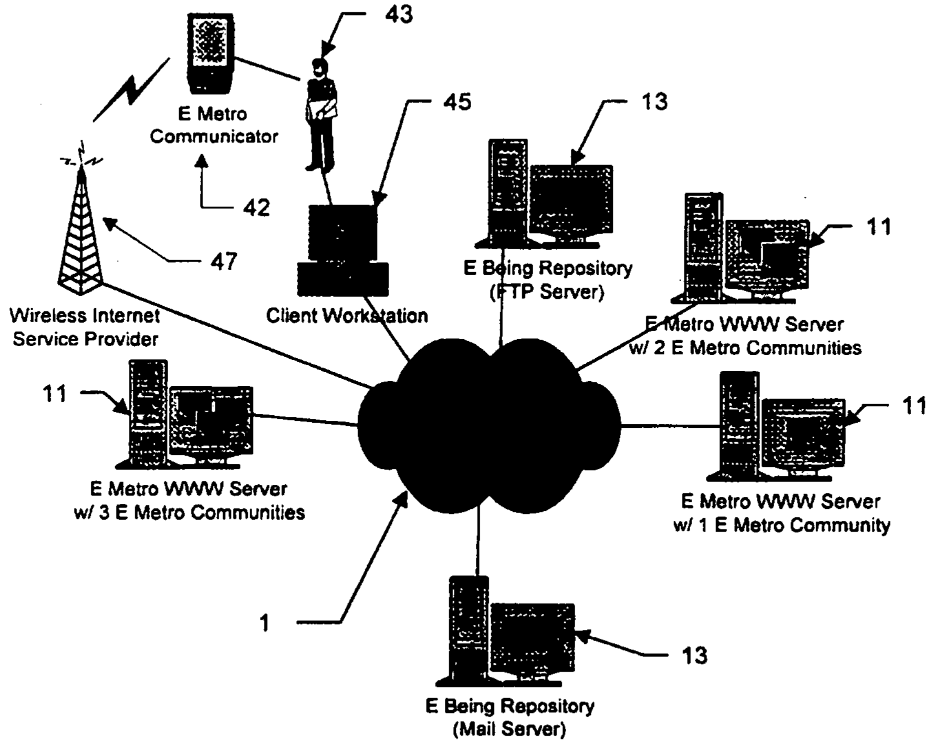

43
45
13
E Metro
Communicator
42
47
E Being Repository
(FTP Server)
11
Wireless Internet
Service Provider
Client Workstation
E Metro WWW Server
w/ 2 E Metro Communities
11
11
E Metro WWW Server
w/ 3 E Metro Communities
E Metro WWW Server
w/ 1 E Metro Community
1
13
E Being Repository
(Mail Server)

Figure 7

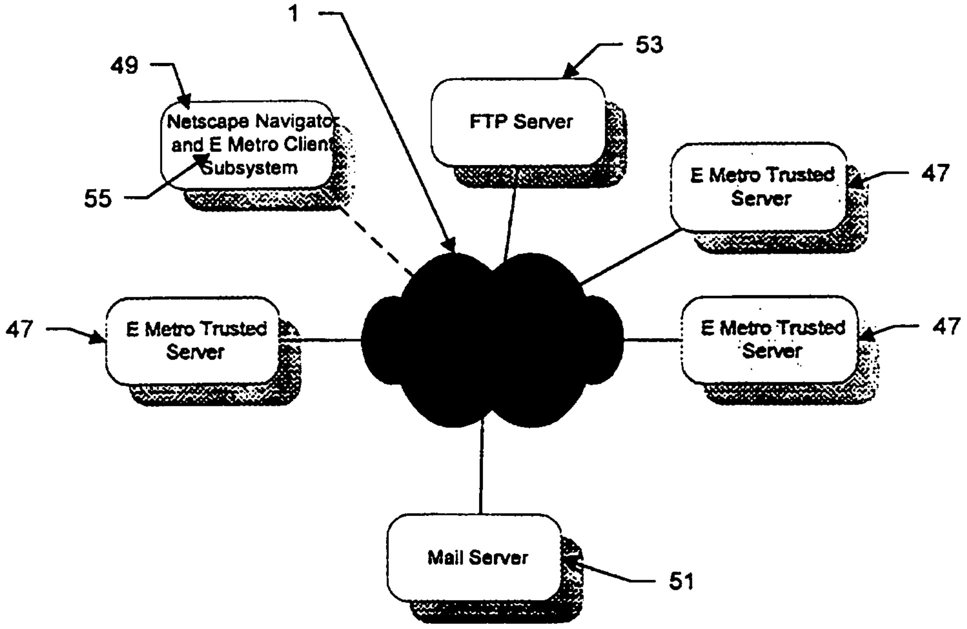

1
49
Netscape Navigator and E Metro Client Subsystem
55
53
FTP Server
E Metro Trusted Server
47
47
E Metro Trusted Server
E Metro Trusted Server
47
Mail Server
51

Figure 8

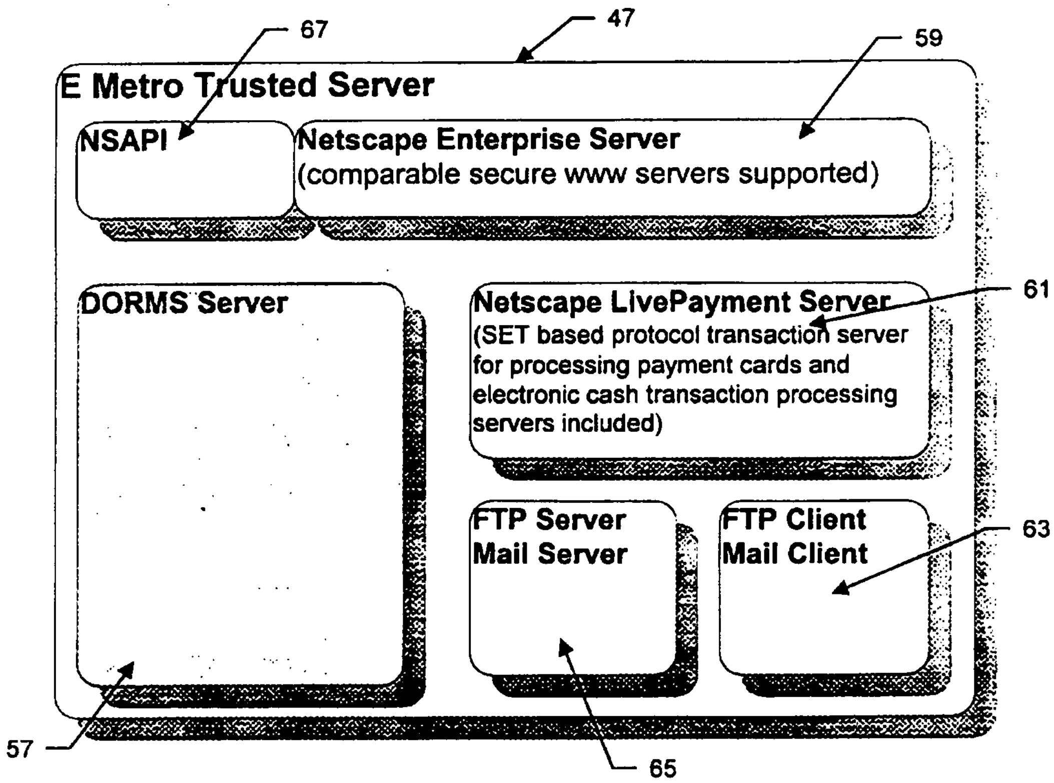

67
47
59
E Metro Trusted Server
NSAPI
Netscape Enterprise Server
(comparable secure www servers supported)
DORMS Server
Netscape LivePayment Server
(SET based protocol transaction server for processing payment cards and electronic cash transaction processing servers included)
61
FTP Server
Mail Server
FTP Client
Mail Client
63
57
65

Figure 9

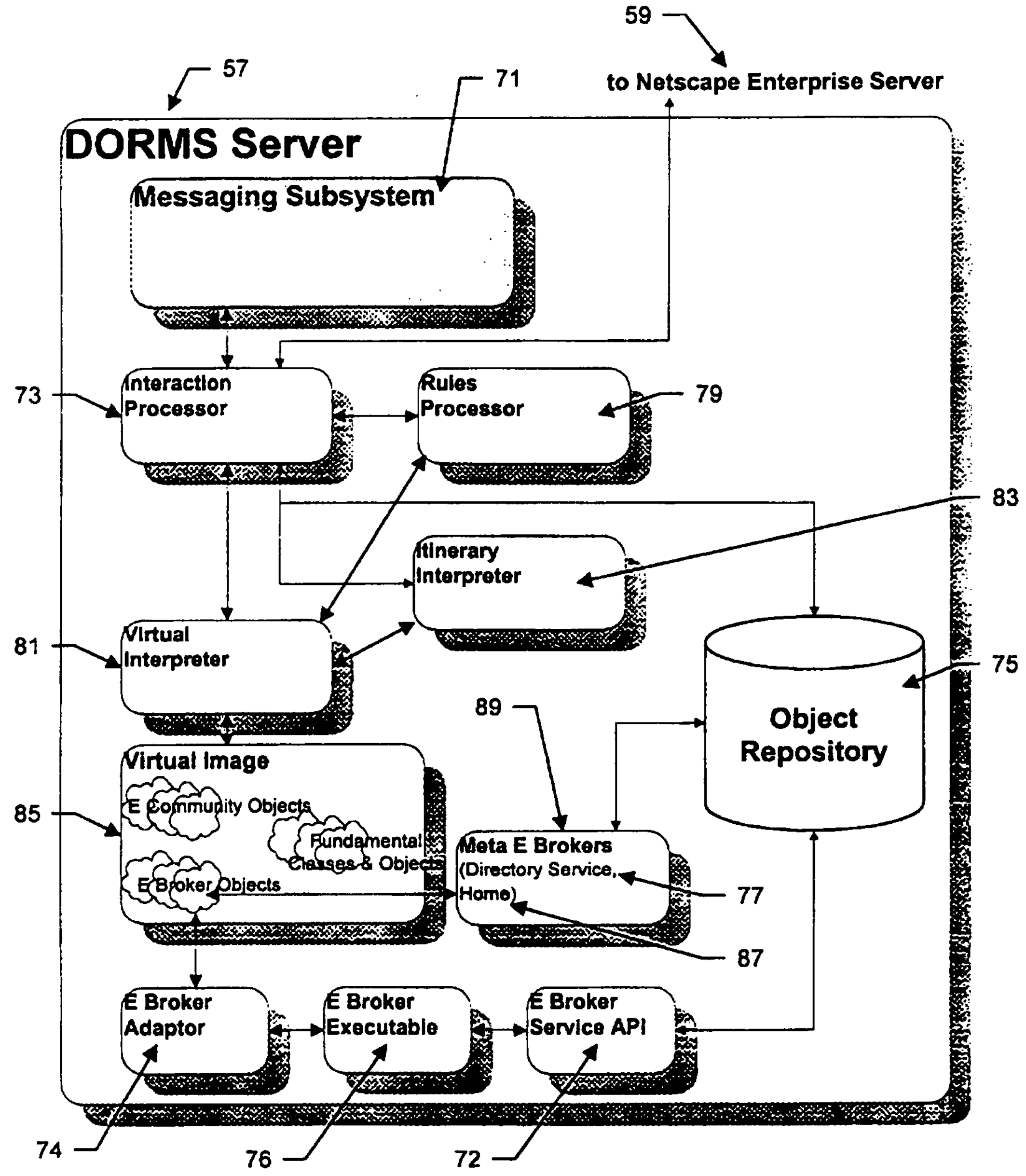
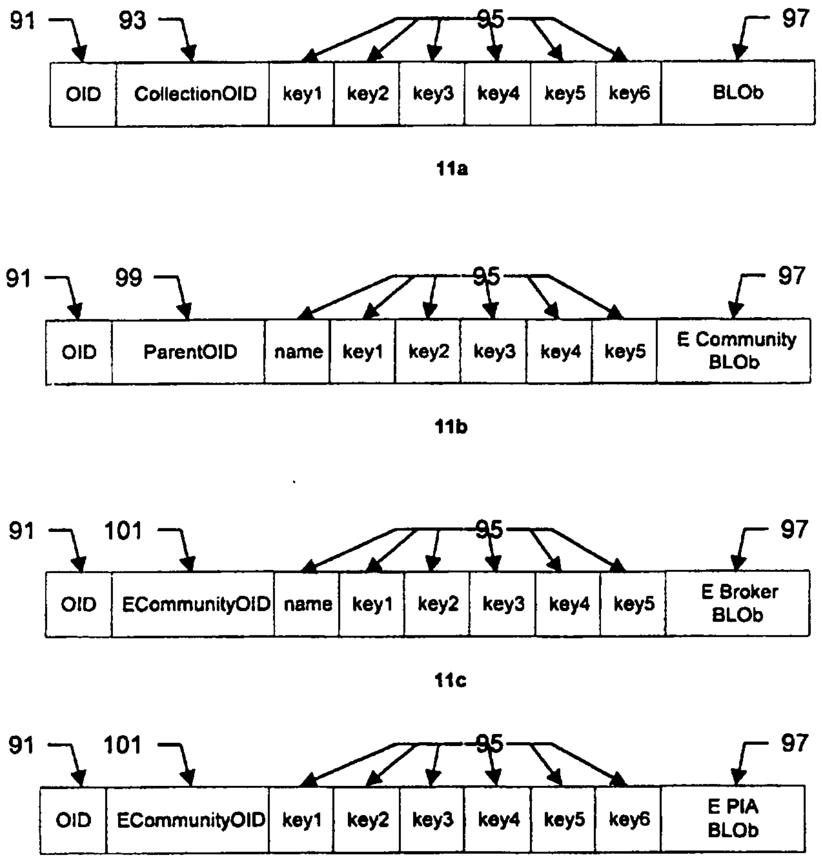

59
to Netscape Enterprise Server
57
71
DORMS Server
Messaging Subsystem
73
Interaction Processor
Rules Processor
79
83
Itinerary Interpreter
81
Virtual Interpreter
75
Object Repository
89
Virtual Image
85
E Community Objects
Fundamental Classes & Objects
E Broker Objects
Meta E Brokers (Directory Service, Home)
77
87
E Broker Adaptor
E Broker Executable
E Broker Service API
74
76
72

Figure 10



11a

11b

11c

11d

Figure 11

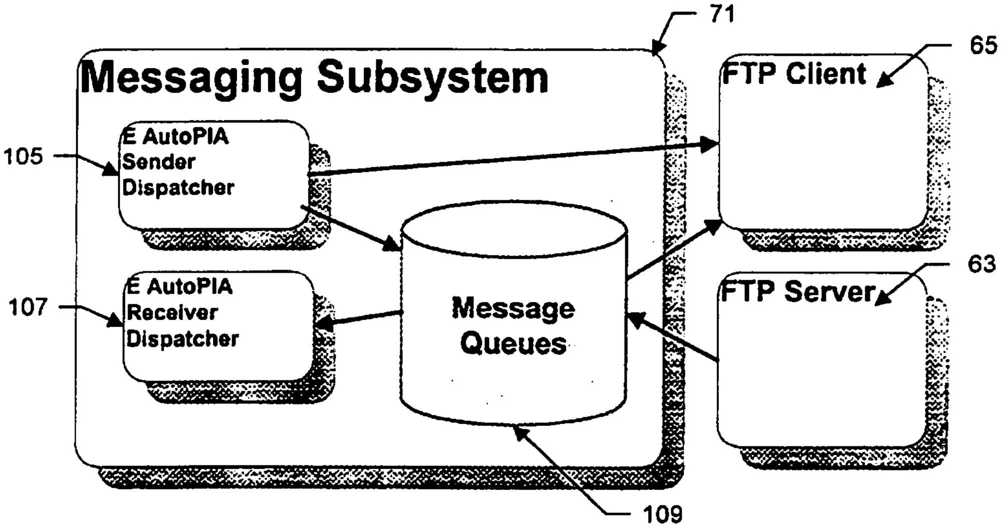

71
Messaging Subsystem
105
E AutoPIA Sender Dispatcher
107
E AutoPIA Receiver Dispatcher
Message Queues
109
FTP Client
65
FTP Server
63

Figure 12

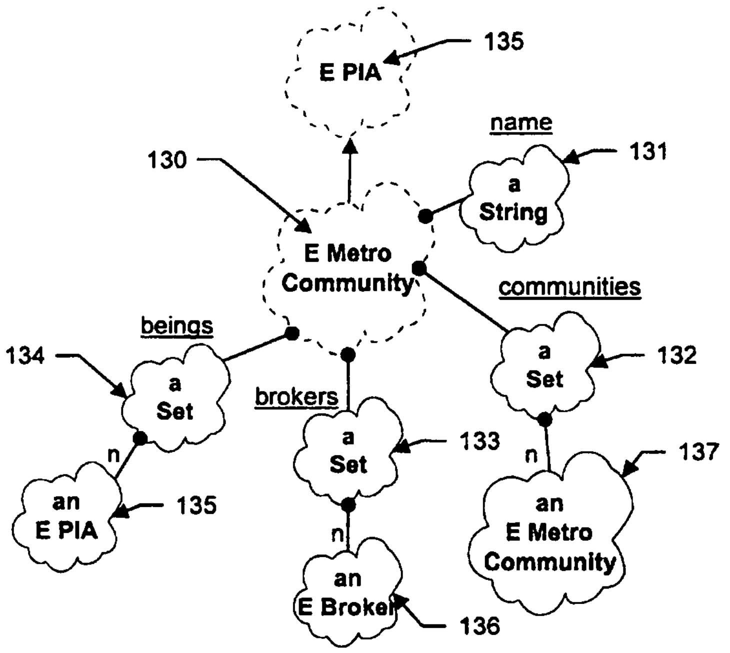

E PIA
135
name
130
131
a
String
E Metro
Community
communities
beings
134
a
Set
132
a
Set
brokers
a
Set
133
n
137
n
an
E PIA
135
n
an
E Metro
Community
an
E Broker
136

Figure 13

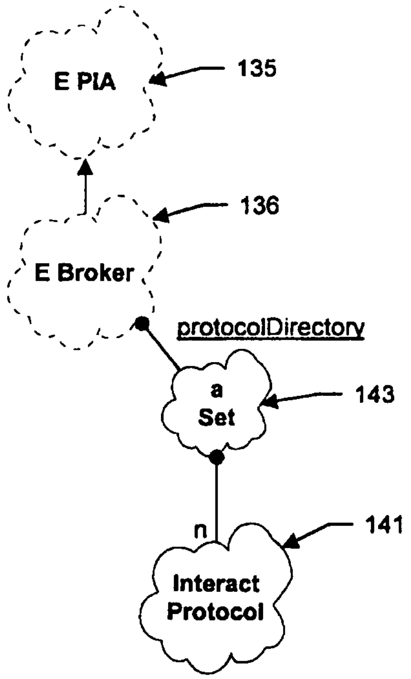
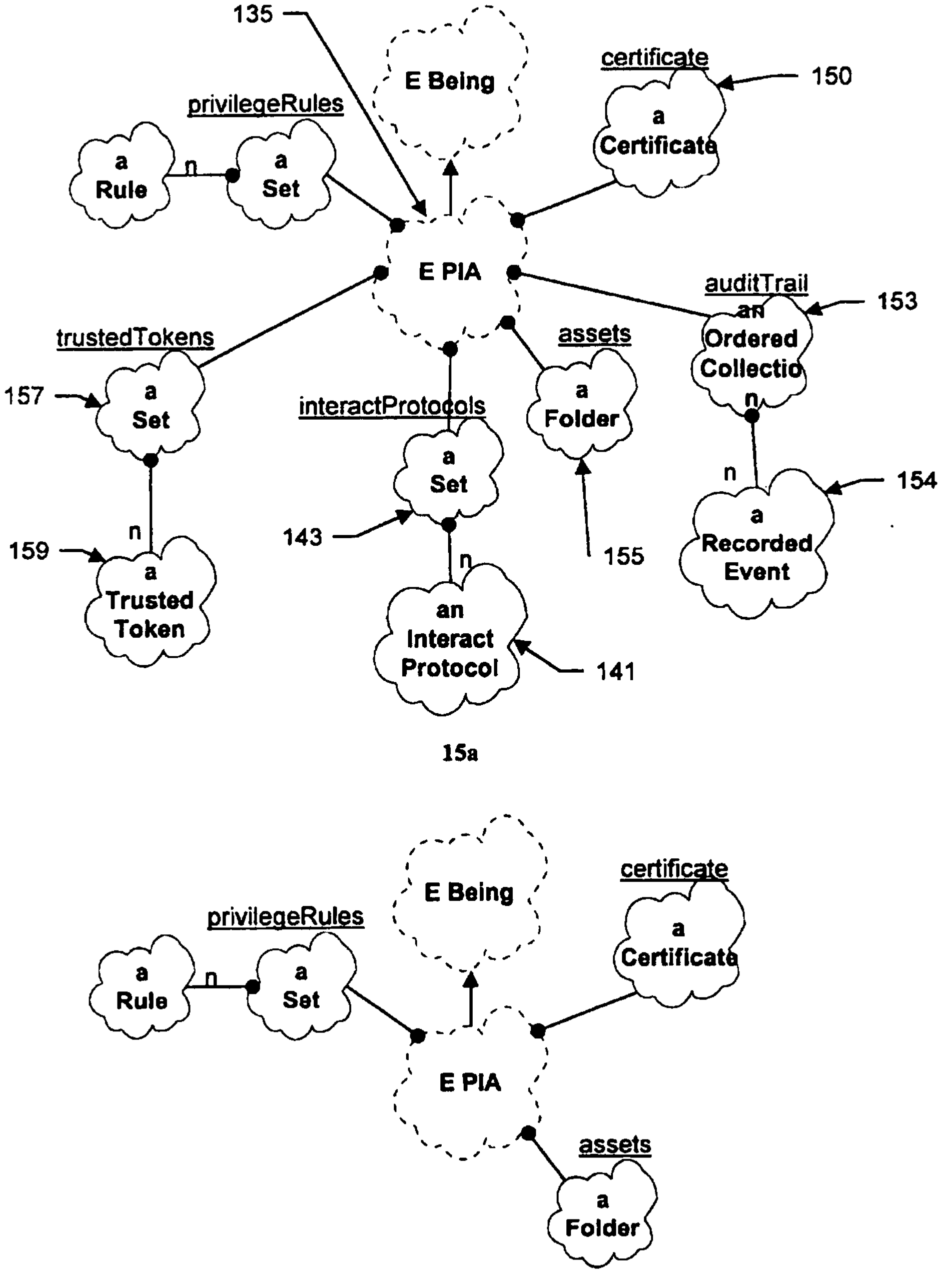

E PIA
135
136
E Broker
protocolDirectory
a
Set
143
n
141
Interact
Protocol

Figure 14



15a

15b

Figure 15

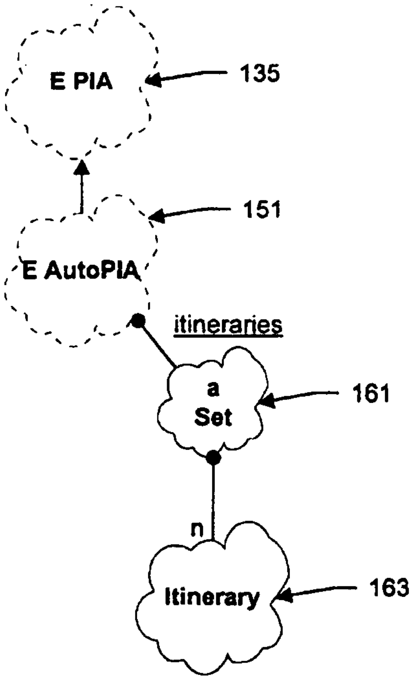


Figure 16

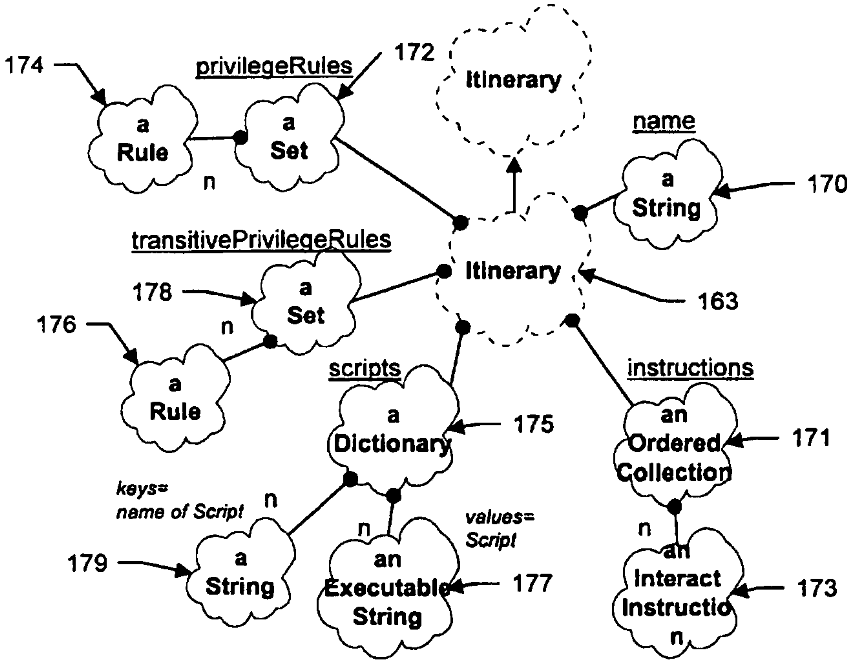

174
privilegeRules
172
Itinerary
a Rule
n
a Set
name
a String
170
transitivePrivilegeRules
178
a Set
Itinerary
163
176
n
a Rule
scripts
instructions
a Dictionary
175
an Ordered Collection
171
keys= name of Script
n
values= Script
n
n
179
a String
an Executable String
177
an Interact Instruction
173

Figure 17

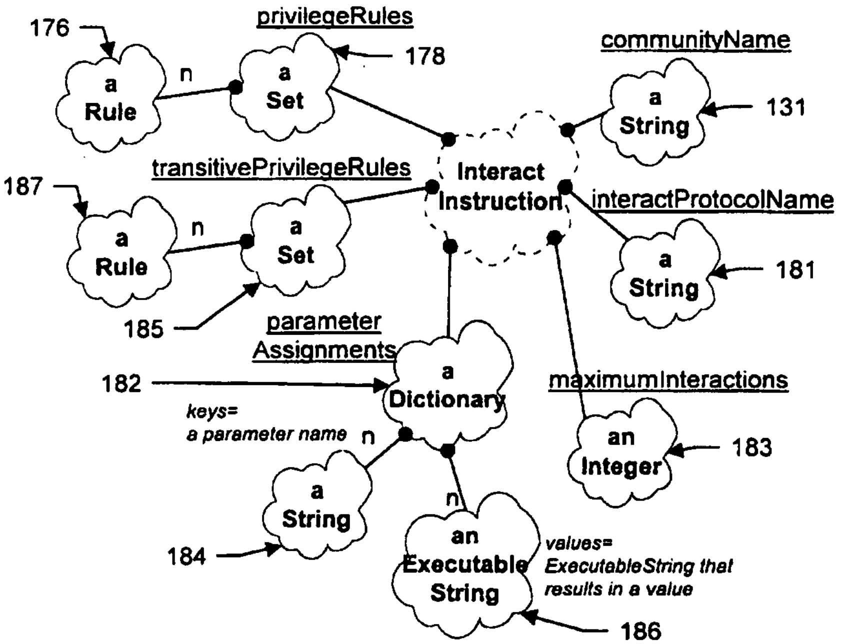

176
a Rule
n
privilegeRules
a Set
178
communityName
a String
131
Interact Instruction
187
transitivePrivilegeRules
a Rule
n
a Set
interactProtocolName
a String
181
185
parameter Assignments
182
a Dictionary
maximumInteractions
keys=
a parameter name
n
an Integer
183
a String
n
an Executable String
values=
ExecutableString that results in a value
184
186

Figure 18

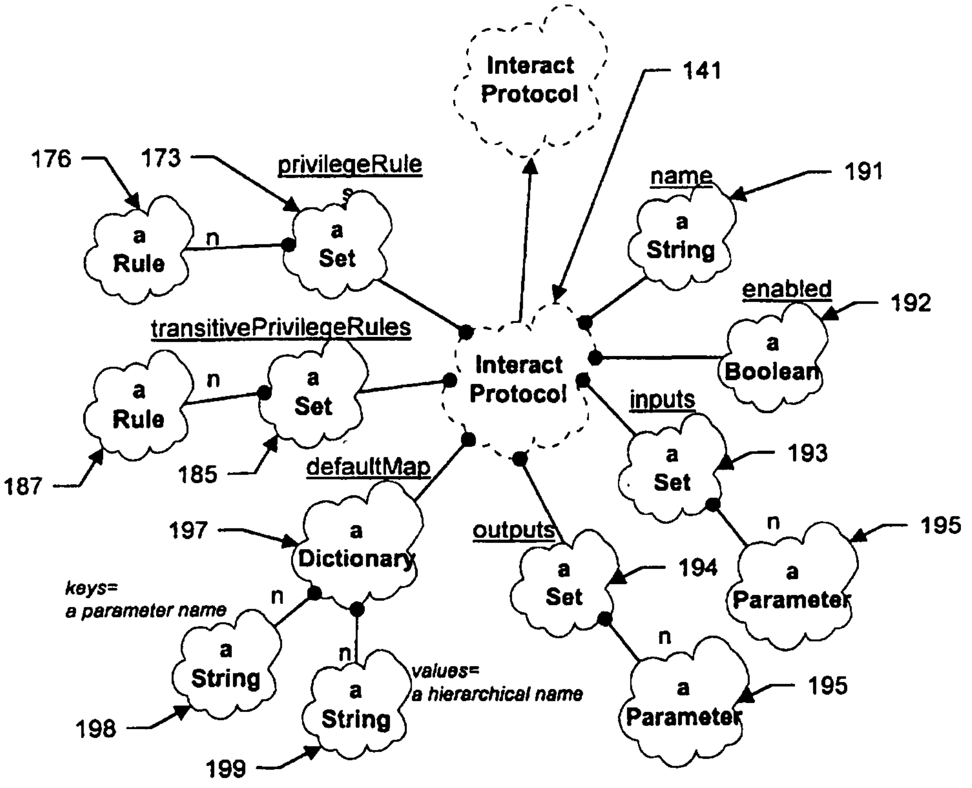

Interact
Protocol
141
176
173
privilegeRules
a
Rule
n
a
Set
name
191
a
String
enabled
192
a
Boolean
transitivePrivilegeRules
a
Rule
n
a
Set
Interact
Protocol
inputs
a
Set
193
187
185
defaultMap
197
a
Dictionary
outputs
n
195
a
Parameter
a
Set
194
keys=
a parameter name
n
a
String
n
n
a
String
values=
a hierarchical name
a
Parameter
195
198
199

Figure 19

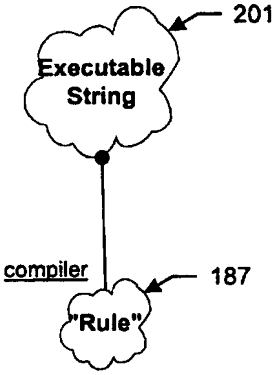


Figure 20

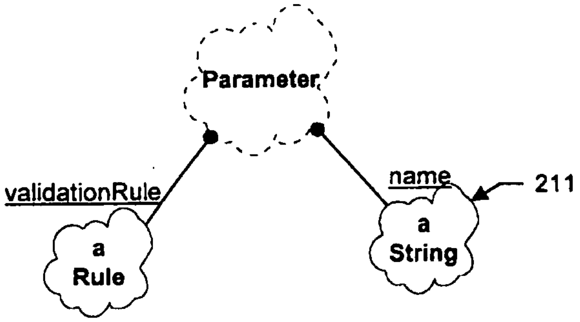


Figure 21

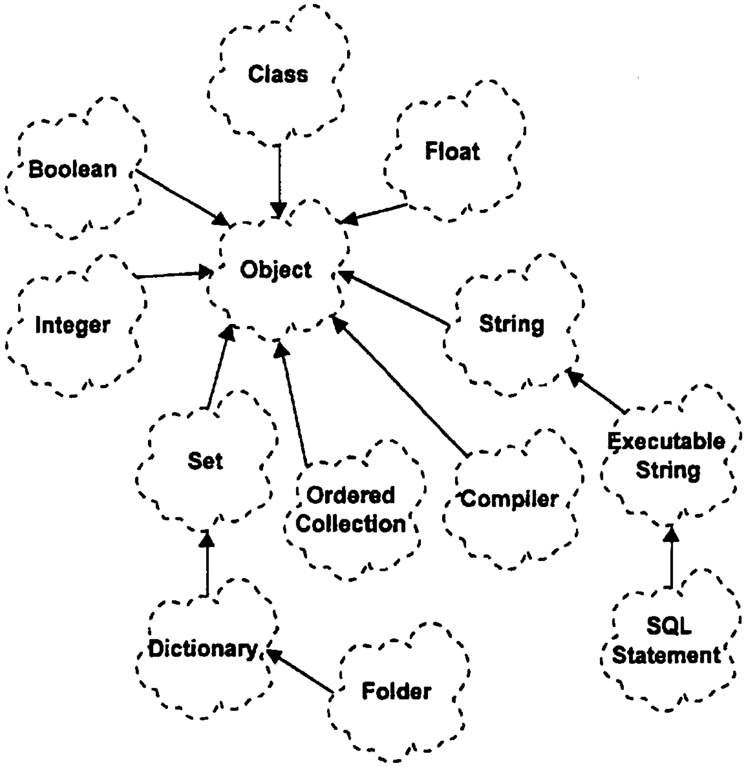
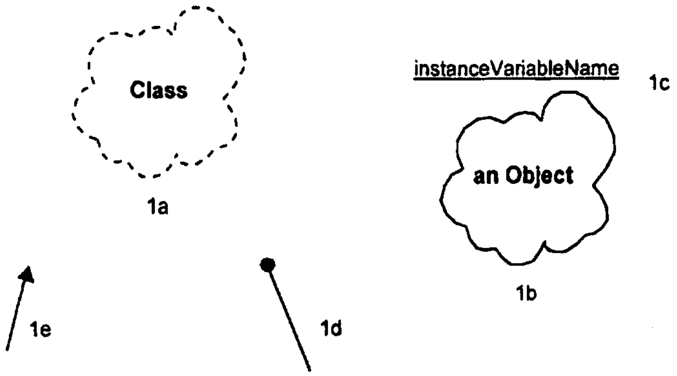

Class
Boolean
Float
Object
Integer
String
Set
Ordered Collection
Compiler
Executable String
Dictionary
Folder
SQL Statement

Figure 22



The basic Booch symbols employed in the visual descriptions within this document. (1a) a Class, (1b) an Object, (1c) instance variable name, (1d) uses for implementation, (1e) inherits

Figure 23

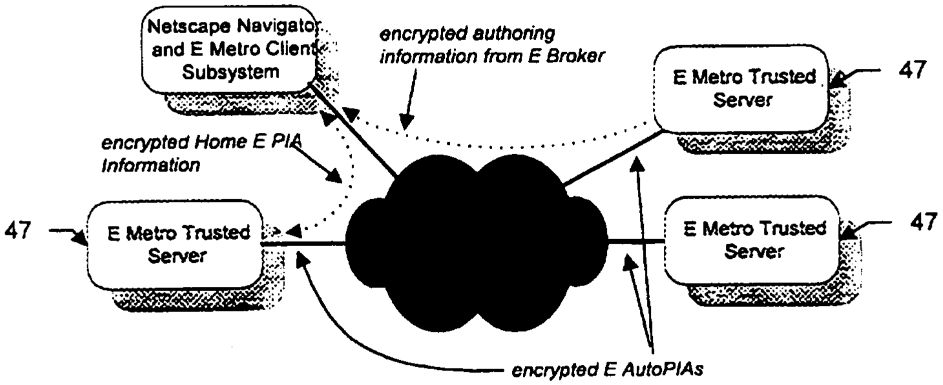
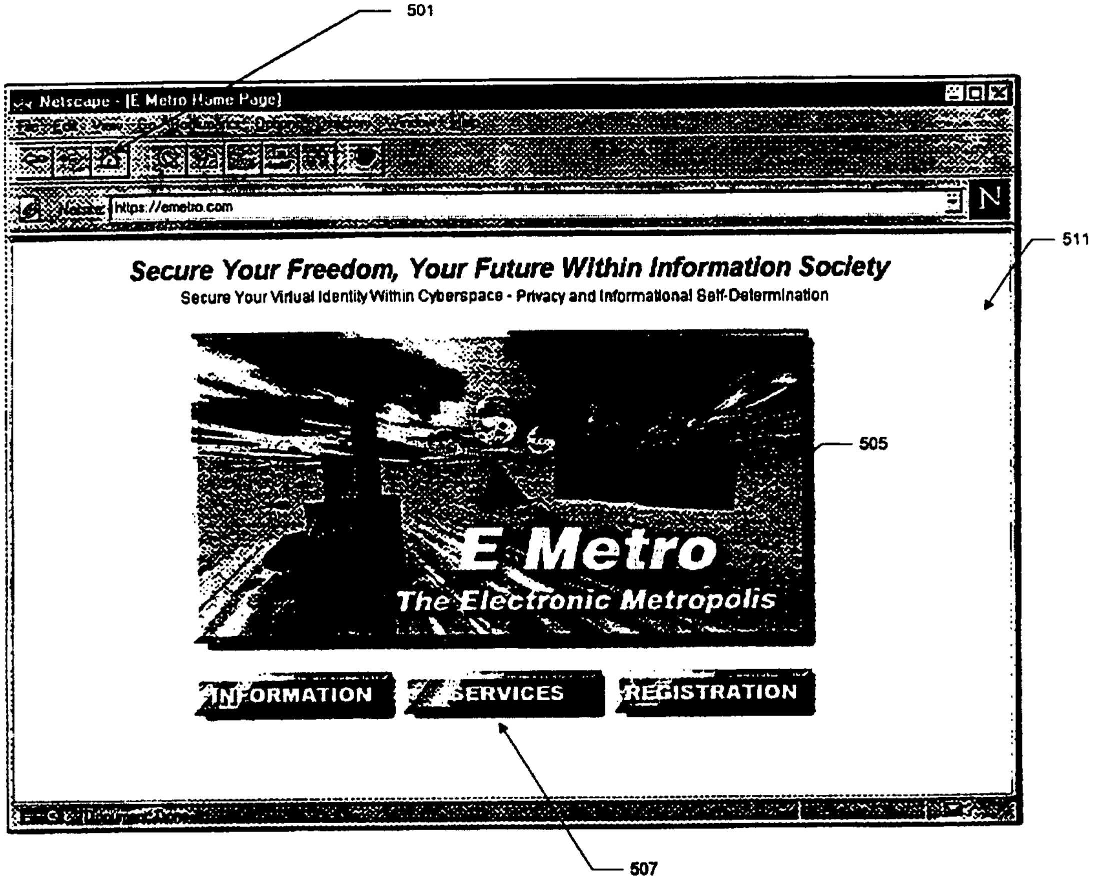

Netscape Navigator and E Metro Client Subsystem
encrypted authoring information from E Broker
E Metro Trusted Server
47
encrypted Home E PIA Information
47
E Metro Trusted Server
E Metro Trusted Server
47
encrypted E AutoPIAs

Figure 24

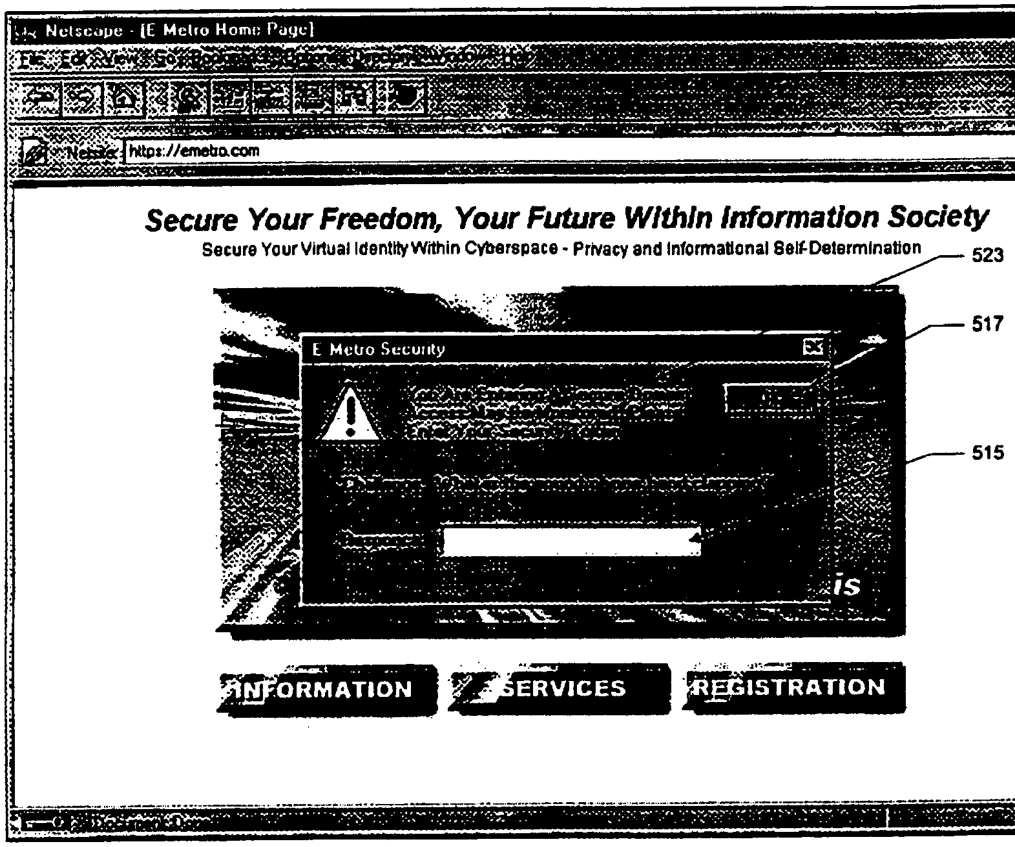


Secure Your Freedom, Your Future Within Information Society

Secure Your Virtual Identity Within Cyberspace - Privacy and Informational Self-Determination

Figure 101

25/35



Netscape - [E Metro Home Page]

https://emetro.com

Secure Your Freedom, Your Future Within Information Society

Secure Your Virtual Identity Within Cyberspace - Privacy and Informational Self-Determination

E Metro Security

Figure 102

26/35

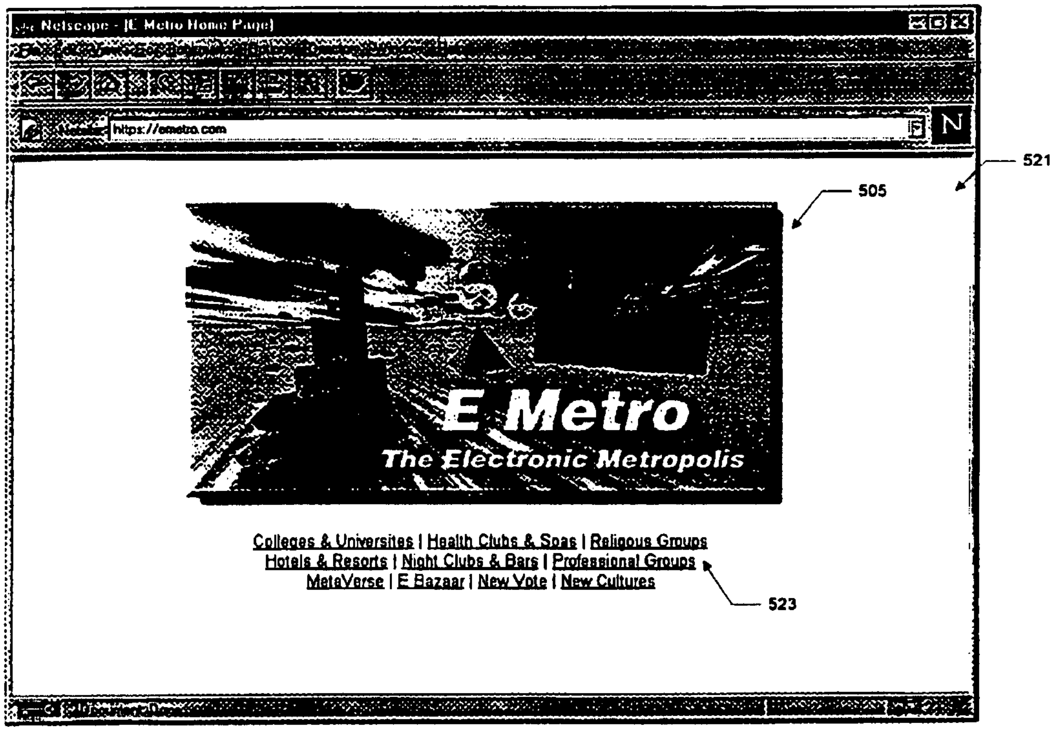
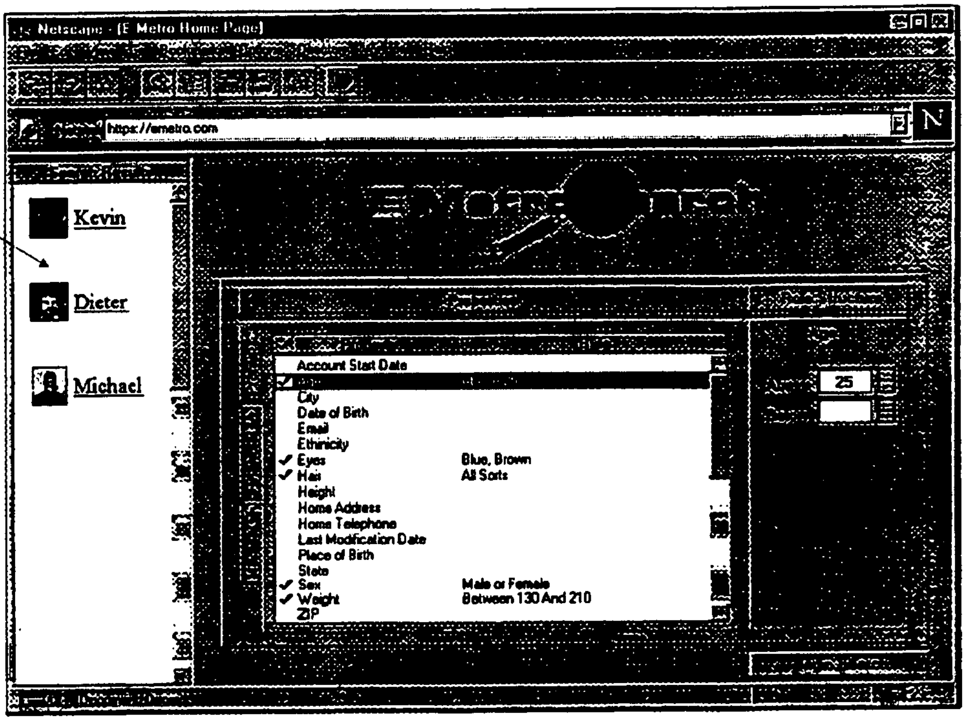

Netscape - [E Metro Home Page]
https://emetro.com
E Metro
The Electronic Metropolis
Colleges & Universites | Health Clubs & Spas | Religous Groups
Hotels & Resorts | Night Clubs & Bars | Professional Groups
MetaVerse | E Bazaar | New Vote | New Cultures
505
521
523

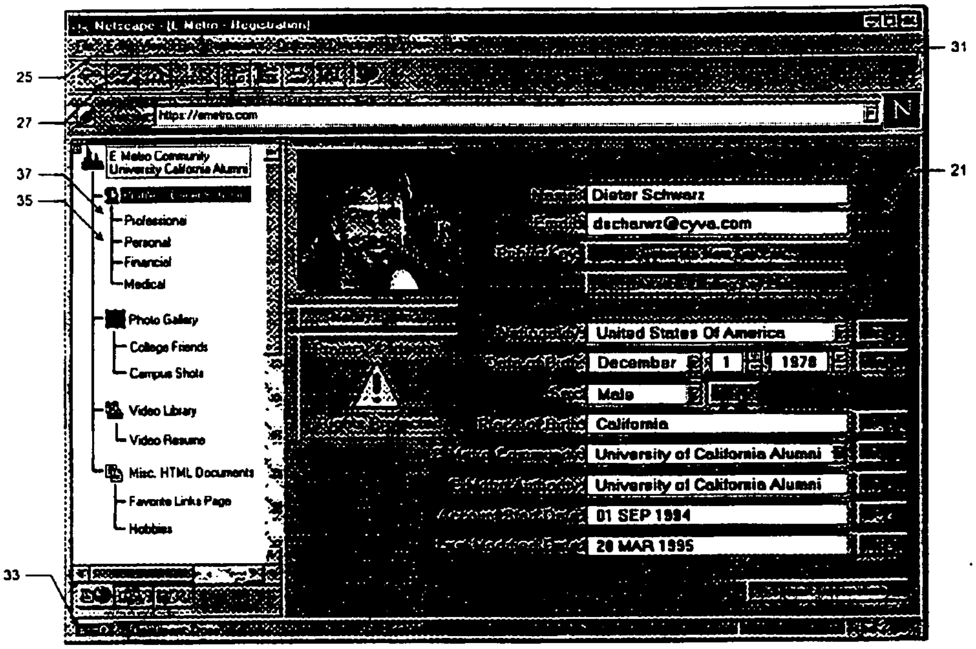
Figure 103



	Account Start Date	
✓	[illegible]	
	City	
	Date of Birth	
	Email	
	Ethnicity	
✓	Eyes	Blue, Brown
✓	Hair	All Sorts
	Height	
	Home Address	
	Home Telephone	
	Last Modification Date	
	Place of Birth	
	State	
✓	Sex	Male or Female
✓	Weight	Between 130 And 210
	ZIP	

Figure 104

This is simply filler as there is no figure 105.



Name: Dieter Schwarz

Email: dscharwz@cyva.com

Public Key:

Nationality: United States Of America

Date of Birth: December 1 1978

Sex: Male

Place of Birth: California

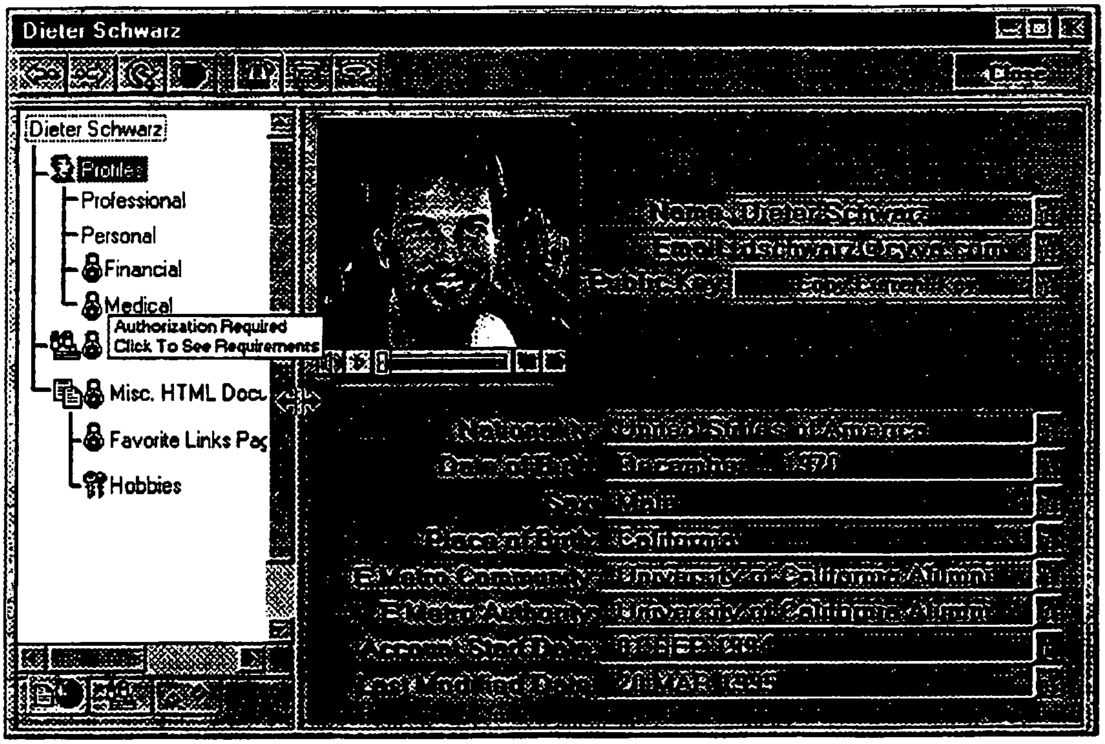
E Metro Community: University of California Alumni

[illegible]: University of California Alumni

Account Start Date: 01 SEP 1994

Last Modified Date: 28 MAR 1995

Figure 106



Name: Dieter Schwarz

Email: dschwarz@[illegible]

Public Key: [illegible]

Nationality: United States of America

Date of Birth: December [illegible] 1971

Sex: Male

Place of Birth: Columbia

E-Metro Community: University of California Alumni

E-Metro Authority: University of California Alumni

Account Start Date: [illegible] FEB [illegible]

Last Modified Date: [illegible] MAR [illegible]

Figure 107

37/35

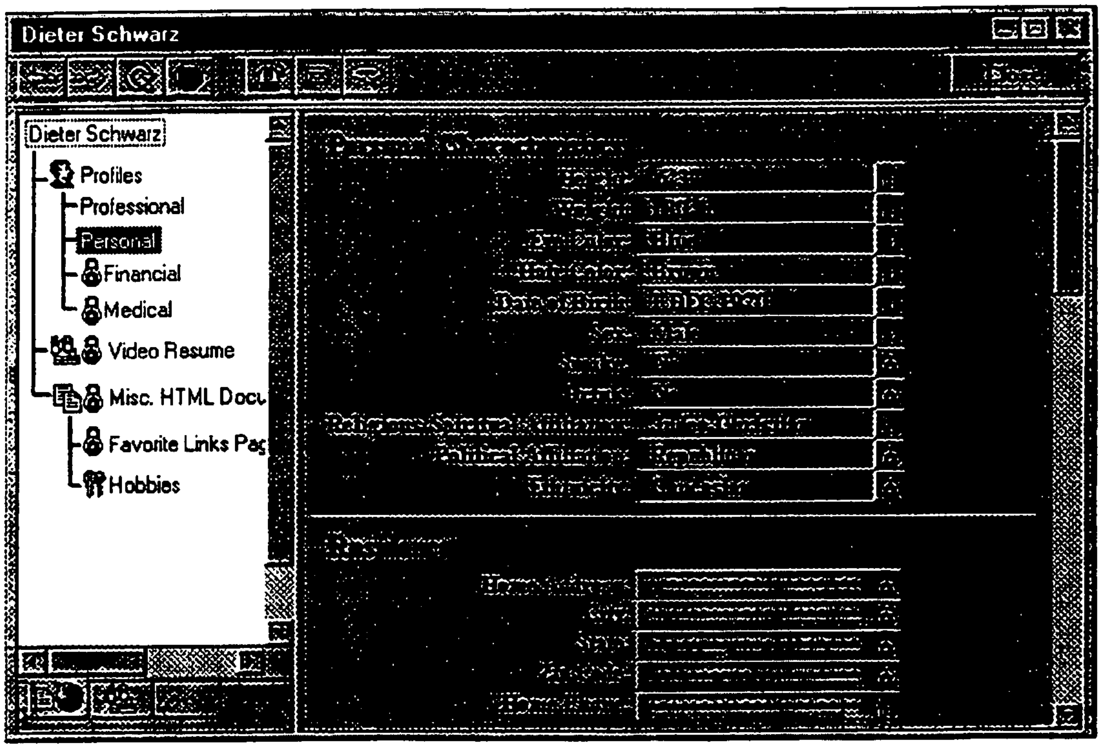
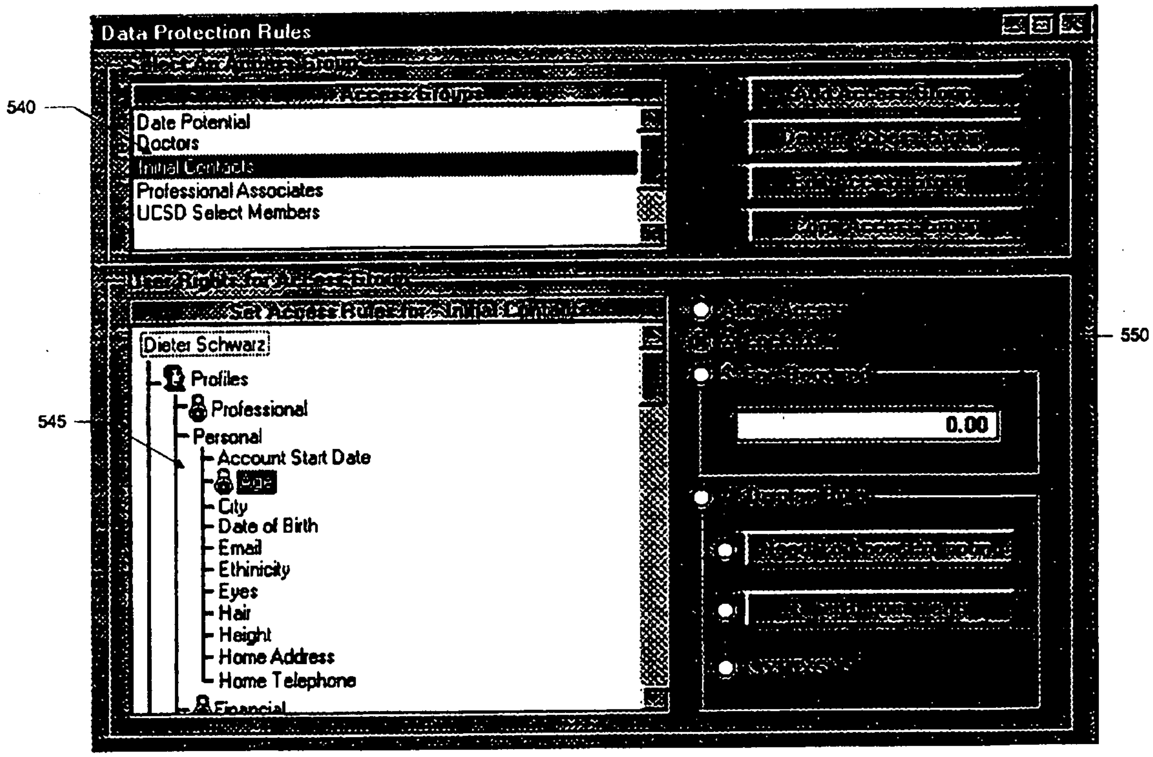

Dieter Schwarz
Dieter Schwarz
Profiles
Professional
Personal
Financial
Medical
Video Resume
Misc. HTML Docu
Favorite Links Pag
Hobbies

Figure 108



Data Protection Rules

Access Groups

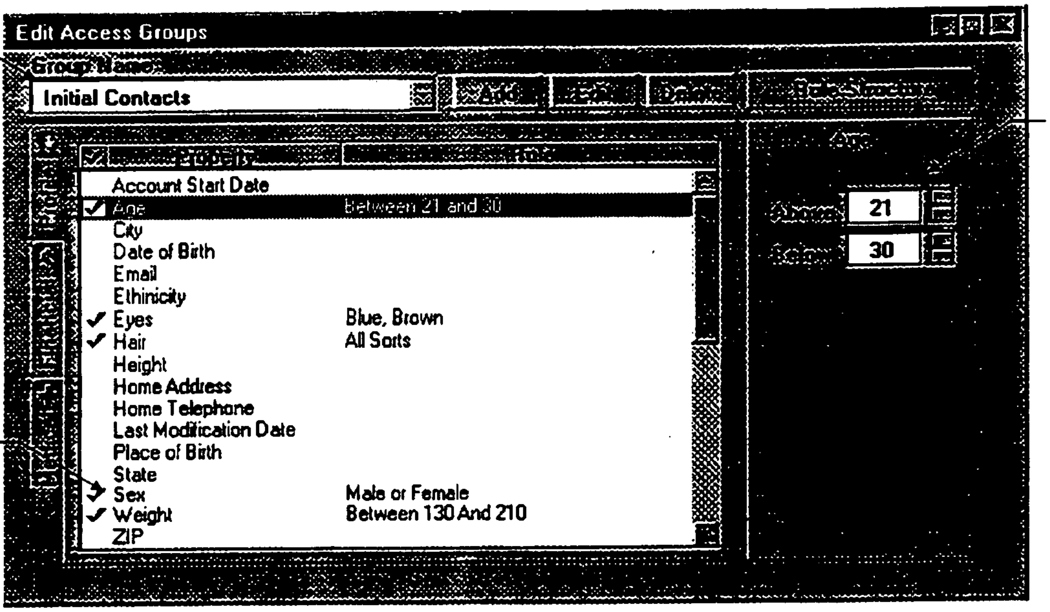
Date Potential
Doctors
Initial Contacts
Professional Associates
UCSD Select Members

Dieter Schwarz
- Profiles
  - Professional
  - Personal
    - Account Start Date
    - Age
    - City
    - Date of Birth
    - Email
    - Ethinicity
    - Eyes
    - Hair
    - Height
    - Home Address
    - Home Telephone
  - Financial

0.00

Figure 109

33/35



Group Name: Initial Contacts

	Property	Rule
	Account Start Date	
✓	Age	Between 21 and 30
	City	
	Date of Birth	
	Email	
	Ethinicity	
✓	Eyes	Blue, Brown
✓	Hair	All Sorts
	Height	
	Home Address	
	Home Telephone	
	Last Modification Date	
	Place of Birth	
	State	
✓	Sex	Male or Female
✓	Weight	Between 130 And 210
	ZIP	

Above 21

Below 30

Figure 110

34/35

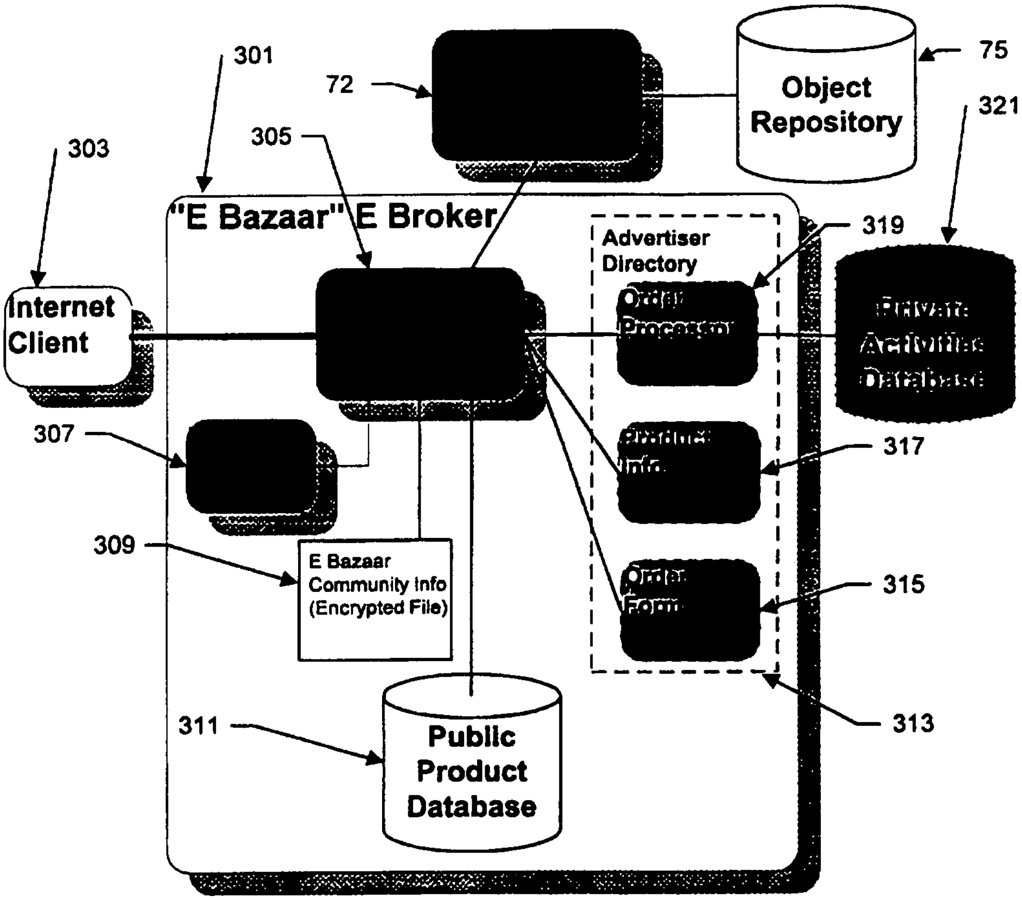

301
72
75
Object Repository
321
303
305
"E Bazaar" E Broker
Advertiser Directory
319
Internet Client
Order Processor
Private Activities Database
307
Product Info.
317
309
E Bazaar Community Info (Encrypted File)
Order Form
315
313
311
Public Product Database

Figure 201

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **G06F 17/60, H04L 29/06, G06F 17/30**	**A3**	**(11) International Publication Number:** **WO 98/03927** **(43) International Publication Date:** 29 January 1998 (29.01.98)

(21) International Application Number: PCT/US97/13309

(22) International Filing Date: 22 July 1997 (22.07.97)

(30) Priority Data:
60/022,035 22 July 1996 (22.07.96) US

(71) Applicant: CYVA RESEARCH CORPORATION [US/US]; Suite 219, 437 South Highway 101, Solana Beach, CA 92075 (US).

(72) Inventors: O'NEIL, Kevin; 3540 Seahorn Circle, San Diego, CA 92031 (US). SEIDMAN, Glenn, R.; 830 West California Way, Woodside, CA 94062 (US).

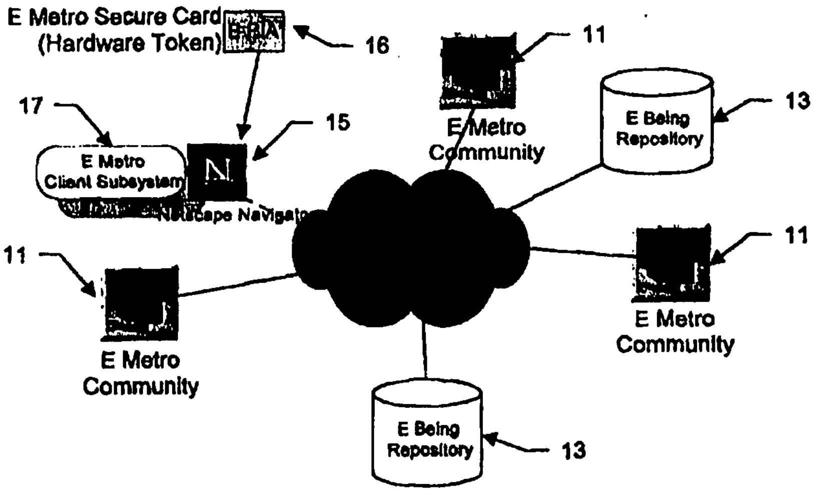
(74) Agents: TEKANIC, Jeffrey, D. et al.; Lyon & Lyon, First Interstate World Center, Suite 4700, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

(81) Designated States: DE, IL, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
12 March 1998 (12.03.98)

(54) Title: PERSONAL INFORMATION SECURITY AND EXCHANGE TOOL



(57) Abstract

Utilization of the E-Metro Community and Personal Information Agents assure an effective and comprehensive agent-rule based command and control of informational assets in a networked computer environment. The concerns of informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to author, secure, search, process, and exchange personal and/or confidential information in a networked computer environment. The formation of trusted electronic communities wherein members command and control their digital persona, exchanging or brokering for value the trusted utility of their informational assets is made possible by the invention. The present invention provides for the trusted utilization of personal data in electronic markets, providing both communities and individuals aggregate and individual rule-based control of the processing of their personal data.

INTERNATIONAL SEARCH REPORT

Intr ional Application No
PCT/US 97/13309

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F17/60 H04L29/06 G06F17/30

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHESS D ET AL: "ITINERANT AGENTS FOR MOBILE COMPUTING" IEEE PERSONAL COMMUNICATIONS, vol. 2, no. 5, 1 October 1995, pages 34-49, XP000531551	18
Y	see page 34, right-hand column, line 30 - page 35, right-hand column, line 50	1-6,12, 13,17
Y	see page 36, right-hand column, line 1 - page 38, right-hand column, line 4	19-23, 25,28,31
Y	see page 39, left-hand column, line 1-28	32,36
	see page 41, left-hand column, line 1-57	
A	see page 42, left-hand column, line 30 - right-hand column, line 1	14,23, 26,29, 33-38
	see page 43, right-hand column, line 4 - page 46, right-hand column, line 7	
	see page 47, right-hand column, line 1 - page 48, left-hand column, line 31	

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

8

Date of the actual completion of the international search 14 January 1998	Date of mailing of the international search report 28/01/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Dupuis, H

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 97/13309

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	ROSCHEISEN M ET AL: "BEYOND BROWSING: SHARED COMMENTS, SOAPS, TRAILS, AND ON-LINE COMMUNITIES" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 27, no. 6, 1 April 1995, pages 739-749, XP000565174 see page 740, left-hand column, line 16-27	1-6,12, 13,17, 19-23, 25,28,31
A	see page 742, left-hand column, line 6 - page 743, left-hand column, line 17 see paragraph 3.1.2 see paragraph 3.2 - paragraph 3.2.3 ---	14,24,33
Y	JERMAN-BLAZIC B ET AL: "A TOOL FOR SUPPORT OF KEY DISTRIBUTION AND VALIDITY CERTIFICATE CHECK IN GLOBAL DIRECTORY SERVICE" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 28, no. 5, 1 March 1996, pages 709-717, XP000555878	32
A	see abstract see paragraph 2 - paragraph 3 ---	20,25
Y	EP 0 649 121 A (IBM) 19 April 1995 see page 13, line 22 - page 16, line 36; figure 13 ---	36
X	EP 0 715 245 A (XEROX CORP) 5 June 1996	25-27
A	see page 6, line 46-51 see page 7, line 31 - page 8, line 28 see page 10, line 7-51 see page 15, line 28 - page 16, line 26 see page 18, line 5-38 see page 19, line 54 - page 20, line 31 see page 21, line 58 see page 24, line 33-35 -----	6,7,10, 11

8

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int(lonal Application No
PCT/US 97/13309

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0649121 A	19-04-95	JP 7175868 A	14-07-95
EP 0715245 A	05-06-96	US 5629980 A JP 8263441 A	13-05-97 11-10-96

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Interview Summary	Application No.	Applicant(s)
	Examiner	Art Unit

All participants (applicant, applicant's representative, PTO personnel):

(1) Wesley W. Monroe (3) ____________

(2) Jim Trammell (4) ____________

Date of Interview 11/20/03

Type: a) ☒ Telephonic b) ☐ Video Conference
c) ☐ Personal [copy is given to 1) ☐ applicant 2) ☐ applicant's representative]

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☐ No. If yes, brief description:

Claim(s) discussed: 1, 8, 15, 26

Identification of prior art discussed:

Agreement with respect to the claims f) ☐ was reached. g) ☐ was not reached. h) ☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments:

Agreement that there are potentially differences between the claimed invention and the prior art applied against the claims. This interview is considered a complete response to the last office action.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

i) ☐ It is not necessary for applicant to provide a separate record of the substance of the interview (if box is checked).

Unless the paragraph above has been checked, THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

SW

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 11/06/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	PAPER NUMBER
3621	#22

DATE MAILED: 11/06/2003

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

PTO-90C (Rev. 10/03)

9/30/03 SW

Office Action Summary	Application No. 09/295,966	Applicant(s) Koichiro, Ikudome et al.
	Examiner Pierre E. Elisca	Art Unit 3621

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *THREE* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *Jun 30, 2003* .

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

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

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above, claim(s) *none* is/are withdrawn from consideration.

5)☐ Claim(s) ______ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) ______ is/are objected to.

8)☐ Claims ______ are subject to restriction and/or election requirement.

Application Papers

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

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

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

11)☐ The proposed drawing correction filed on ______ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

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

a)☐ All b)☐ Some* c)☐ None of:

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

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

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

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

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

a)☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). ______

4) ☐ Interview Summary (PTO-413) Paper No(s). ______

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other:

Examiner Pierre Eddy Elisca
United States Department of Commerce
Patent and Trademark Office
Washington, D.C. 20231

DETAILED ACTION

1. In view of the Reply/Brief filed on 06/30/2003, PROSECUTION IS HEREBY REOPENED in view of new ground of rejection set forth below.

2. Regarding the status of the claims in the instant application, the Examiner has found new prior art. Thus, the finality of the prior Office action has been withdrawn and a new rejection follows. The Examiner regrets the delayed process of the application. Accordingly, claims 1-29 are pending.

Claim Rejections - 35 USC § 103

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

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

> skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-29 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Shiva Corp. Horowitz et al. (WO 96/05549) in view of Grube et al. (U.S. pat. No. 6,157,829).**

As per claims 1, 8, 15, Horowitz discloses a system/method comprising:

a dial-up network server (or network server) that receives user IDs from user's computers (see., abstract);

a redirection server (a firewall or filter or gateway) to the dial-up network server, an authentication accounting server connected to the database, the dial-up network server and the redirection server (see., figs 1 and 2, col 3, lines 8-34, col 4, lines 1-34);

wherein the dial-up network server communicates a first user ID <u>for one of the users' computers</u> and a temporarily assigned network address for the first user ID to the authentication accounting server (see.,abstract, col 4, lines 23-34);

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individual rule set **(see., this limitation is disclosed by Horowitz, in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string**

having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string, please note that the process of identifying the remote user is seen to read as the step of the users's computers rule set or portion of rule set, and the step of redirecting server is also disclosed in page 4, lines 6-18, specifically wherein it is stated that if the server locates an access filter for a remote user which indicates that the remote user should-not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network, also please note that the fact that the remote user will be able to communicate with other non-restricted parts of the network, thus the remote user in fact has been redirected toward another direction).

It is to be noted that Horowitz fails to explicitly disclose wherein said the dial up network server communicates a first user ID (first ID or permanent ID) for one of the users' computers and a temporarily assigned (temporarily assigned or temporarily ID) network address for the first user ID. However, Grube discloses a central service agent that assigns a temporary alias ID and a permanent ID that is communicated, on a temporary basis, to a specific calling unit (see., abstract, col 2, lines 50-67, col 3, lines 47-67). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the local computer network of Horowitz by including the limitation detailed above as taught by Grube because this would prevent unauthorized access to the network.

As per claims 2-6, 9-13, 16-29 Horowitz discloses the claimed limitation, wherein the redirection server (or filter) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (see., abstract, col 9, lines 13-34).

As per claims 7, 14, Horowitz discloses the claimed limitation, wherein the database entires for a plurality of the plurality of users's IDs are correlated with a common individualized rule set (see., abstract, col 8, lines 28-34, col 9, lines 24-34).

Conclusion

5. Any inquiry concerning this communication from the examiner should be directed to Pierre Eddy Elisca at (703) 305-3987. The examiner can normally be reached on Tuesday to Friday from 6:30AM. to 5:00PM.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768.

Any response to this action should be mailed to:

Commissioner of patents and Trademarks
Washington, D.C. 20231

The Official Fax Number For TC-3600 is:

(703) 305-7687

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Pierre Eddy Elisca

Patent Examiner

September 08, 2003

Notice of References Cited	Application/Control No. **09/295,966**	Applicant(s)/Patent Under Reexam **Koichiro, Ikudome et al.**
	Examiner **Pierre E. Elisca**	Art Unit **3621** | **Page 1 of 1**

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY[1]	Name	Classification[2]	
	A	6,157,829	12/2000	Grube et al.	455	414
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY[1]	Country	Name	Classification[2]	
	N						
	O						
	P						
	Q						
	R						
	S						
	T						

NON-PATENT DOCUMENTS

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

* A copy of this reference is not being furnished with this Office action. See MPEP § 707.05(a). [1] Dates in MM-YYYY format are publication dates. [2] Classifications may be U.S. or foreign.

U. S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)

Notice of References Cited

#20/ Reply Brief

Lawan
7-10-03

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on June 30, 2003.

Margaret A. Sullivan
Name

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre E. Elisca
Docket No.	:	34503/WWM/A522

APPLICANTS' REPLY BRIEF

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

Post Office Box 7068
Pasadena, CA 91109-7068
June 30, 2003

Commissioner:

The Examiner's Answer mailed May 13, 2003 fails to respond to several arguments raised in Applicants' Appeal Brief and previous Responses to Office Actions. These arguments are discussed below. Some of these arguments have been made since the beginning of prosecution of this application and have never been addressed by the Examiner. The Examiner's Answer merely recites verbatim the wording of the Final Rejection. Applicants respectfully request that the claims be allowed because the Applicants' arguments are unrefuted or that prosecution be reopened so that these arguments may be addressed by the Examiner.

Specifically, the Examiner's Answer fails to address Applicants' argument discussed in relation to Group III (claims 15-29) that *Horowitz* contains no teaching or suggestion of "automated modification of at least a portion of the rule set correlated to the temporarily assigned network address." This limitation has, in fact, never been addressed by the Examiner, despite Applicants repeatedly bringing this limitation to the Examiner's attention since the beginning of prosecution. The Examiner has failed to show any teaching or suggestion in *Horowitz* of this limitation, and has not addressed this limitation at any point in the prosecution. Applicants respectfully request that the rejections to these claims, therefore, be withdrawn.

Application No. 09/295,966

Regarding Group II (claims 5-6 and 12-13), Applicants repeatedly refuted the Examiner's argument, stating that not allowing a particular user into a zone is considered *redirection by the server* as the term "redirection" is used in the specification or in the art. Applicants pointed out in the Response to the Final Rejection and in the Appeal Brief that *Horowitz* did not teach or suggest this limitation, citing support in the specification. The Examiner's Answer, however, fails to address this argument or the support cited by the Applicants, and merely repeats verbatim the refuted argument from the Final Rejection. Because the Examiner has failed to refute Applicants' arguments, Applicants respectfully request that these claims be allowed.

Applicants also repeatedly refuted the Examiner's argument regarding Group I (claims 1-4, 7-11 and 14). Applicants pointed out in the Response to the Final Rejection and in the Appeal Brief that *Horowitz* does not teach or suggest "directing data to a public network." More specifically, Applicants argued that the "communication and network ports" in Horowitz cited by the Examiner are not used by Horowitz to direct data to a public network with specific reference to the relevant portions of Horowitz supporting Applicants' view. However, the Examiner did not address this detailed analysis of the Horowitz disclosure, but rather only repeated, verbatim, his previous language from the Final Rejection. Because the Examiner has failed to refute the Applicants' arguments, Applicants respectfully request that these claims be allowed.

For all of the foregoing reasons, the Examiner has not stated a *prima facie* case for obviousness and thus the claims should be allowed.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By

Wesley W. Monroe
Reg. No. 39,778
626/795-9900

RAH/rah
MAS PAS512601.1-*-06/30/03 5:04 PM

facsimile
TRANSMITTAL

Date: June 30, 2003

No. of Pages: 3 (including this cover sheet)

Fax No.: (703) 746-7238

PLEASE DELIVER THE FOLLOWING PAGES IMMEDIATELY TO:

Name: Commissioner of Patents

Art Unit: 3621

Examiner: Pierre E. Elisca

Phone: (703) 305-9768

From: Wesley W. Monroe
Reg No. 39,778

Re: Application No. 09/295,966; Filed April 21, 1999
Entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

File: 34503/WWM/A522

I HEREBY CERTIFY THAT THIS PAPER IS BEING FACSIMILE TRANSMITTED TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **June 30, 2003.**

Margaret A. Sullivan
Margaret A. Sullivan

*Correspondence: Applicants' Reply Brief.

*Correspondence:

For Office Services Use Only
Return to Marti Carrillo

Christie, Parker & Hale, LLP
350 West Colorado Boulevard
Post Office Box 7068
Pasadena, CA 91109-7068
626-795-9900
Fax: 626-577-8800

confidential

The information in this transmission is confidential and is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone collect, and return the original message to us at the above address via U.S. mail. We will reimburse you for postage. Thank you.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 04/23/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	PAPER NUMBER
3621	#16

DATE MAILED: 04/23/2003

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

PTO-90C (Rev. 07-01)

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.

EXAMINER	

ART UNIT	PAPER NUMBER
	16

DATE MAILED:

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

Commissioner of Patents and Trademarl

The holding of abandonment mailed 3-24-03, has been withdrawn. The above-mentioned patent application has been returned to pending status.

Any inquiry concerning this communication should be directed to Jackie Waldo, Head Supervisory Legal Instrument Examiner, whose number is 703-308-3902.

Effie Adams

Effie Adams, Supervisory Legal
Instrument Examiner, TC 3600

8

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 05/13/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	PAPER NUMBER
3621	19

DATE MAILED: 05/13/2003

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

PTO-90C (Rev. 07-01)

United States Patent and Trademark Office

Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS

AND INTERFERENCES

Paper No. 19

Application Number: 09/295,966

Filing Date: April 21, 1999

Appellant(s): Koichiro, Ikudome et al.

Wesley W. Monroe

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/02/2002.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1-29 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal. Claims 1-29 are rejected under 35 U.S.C. 102 (b) as being anticipated by Horowitz et al. (WO96/05549). This rejection is set forth in the office action, paper # 9

WO96/05549	Horowitz et al.	2/1996

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in thi country, more than one year prior to the date of application for patent in the United States.

Claims 1-29 are rejected under 35 U.S.C. 102 (b) as being anticipated by Shiva Corp. Horowitz et al. (WO 96/05549).

As per claims 1, 8, 15, Horowitz discloses a system/method comprising:

a dial-up network server (or network server) that receives user IDs from user's computers (see., abstract);

a redirection server (a firewall or filter or gateway) to the dial-up network server, an authentication accounting server connected to the database, the dial-up network server and the redirection server (see., figs 1 and 2, page 3, lines 8-34 or col 3, lines 8-34, page 4, lines 1-34 or col 4, lines 1-34);

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server (see.,abstract, page 4, lines 23-34 or col 4, lines 23-34, page 8, lines 9-34 or col 8, lines 9-34);

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the user ID and the temporarily assigned network address to the redirection server (see.,abstract, page 7, lines 1-34 or col 7, lines 1-34, page 9, lines 4-34 or col 9, lines 4-34); and

wherein data redirected toward the public network from the one of the users' computers are processed by the redirection server according to the individual rule set **(see., this limitation is disclosed by Horowitz, in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string, please note that the process of identifying the remote user is seen to read as the step of the users's computers rule set or portion of rule set, and the step of redirecting server is also disclosed in page 4, lines 6-18, specifically wherein it is stated that if the server locates an access filter for a remote user which indicates that the remote user should-not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network, also please note that the fact that the remote user will be able to communicate with other non-restricted parts of the network, thus the remote user in fact has been redirected toward another direction).**

As per claims 2-6, 9-13, 16-29 Horowitz discloses the claimed limitation, wherein the redirection server (or filter) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (see., abstract, page 9, lines 13-34 or col 9, lines 13-34).

As per claims 7, 14, Horowitz discloses the claimed limitation, wherein the database entires for a plurality of the plurality of users's IDs are correlated with a common individualized rule set (see., abstract, page 8, lines 28-34 or col 8, lines 28-34, page 9, lines 24-34 or col 9, lines 24-34).

(11) Response To Argument

In response to claims 1-29, Applicant argues that the prior art of record (Horawitz et al) does not teach or suggest: " user ID for one of the users' computers and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individual rule set or rule set correlated to the temporarily assigned network address". However, these newly added limitations is also disclosed by Horowitz **in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string, please note that the process of identifying the remote user is seen to read as the step of the users's computers rule set or portion of rule set correlated to the temporarily assigned network address (network address or access filter associated with the string), and the step of redirecting server is also disclosed in page 4, lines 6-18, specifically**

wherein it is stated that if the server locates an access filter for a remote user which indicates that the remote user should-not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network, also please note that the fact that the remote user will be able to communicate with other non-restricted parts of the network, thus the remote user in fact has been redirected toward another direction).

For the above reasons, it is believed that the rejections should be sustained.

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Pierre Eddy Elisca

Patent Examiner

Respectfully submitted,

Conferee
SMG STEPHEN GRAVINI
PRIMARY EXAMINER

Christie, Parker & Hale, LLP

Post Office Box 7068

Pasadena, Ca 91109-7068

Conferee
HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Exhibit A

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PETITION FOR EXTENSION OF TIME
FROM THE NOTICE OF APPEAL

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div	:	3621
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Notice of Appeal filed April 12, 2002 and made under 37 CFR § 1.136(a) for one month(s) from October 22, 2002 to November 22, 2002.

The fee for extension of time required by 37 CFR § 1.17 is calculated below.

FEE CALCULATION

LENGTH OF EXTENSION	SMALL ENTITY	LARGE ENTITY	FEE
WITHIN FIRST MONTH	$ 55	$110	$
WITHIN SECOND MONTH	$200	$400	$
WITHIN THIRD MONTH	$460	$920	$
WITHIN FOURTH MONTH	$720	$1440	$

PETITION FOR EXTENSION OF TIME
Application No. 09/295,966

WITHIN FIFTH MONTH	$980	$1960	$260.00 (difference between the fourth and fifth month extension fees - 4th extension was filed on October 22, 2002)

Submitted herewith is a check for **$260.00** to cover the cost of the extension.

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ____________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/eaj
EAJ PAS476047.1-*-11/22/02 5:38 PM

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

SUBMISSION OF APPELLANT'S BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Post Office Box 7068
Pasadena, CA 91101-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Enclosed for filing are the **original and two copies** of Appellant's Brief for this application.

X An extension of time to file Appellant's Brief is requested, and a Petition for Extension of Time and the applicable fee are enclosed.

X Our check for $160.00 to cover the fee for the appeal brief is enclosed.

___ An oral hearing of the appeal is requested, and our check for $, the fee for the oral hearing, is enclosed.

The Commissioner is hereby authorized to charge any further fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/eaj

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Name

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre E. Elisca
Docket No.	:	34503/WWM/A522

APPELLANT'S BRIEF

Post Office Box 7068
Pasadena, CA 91109-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

This is an appeal from the Final Rejection, dated October 12, 2001, of the claims in the above-referenced application.

1. REAL PARTY IN INTEREST

The real party in interest is the assignee of the subject application, Auric Web Systems.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-29 are pending in the present application.

Claims 1-29 have been rejected in a final rejection, dated October 12, 2001 under 35 U.S.C. §102(b).

The claims on appeal are claims 1-29.

4. STATUS OF AMENDMENTS

Appellants submitted additional remarks in a response to the final rejection. This response did not amend any claims. The response was not deemed to overcome the rejections. *See*, Paper 14, dated October 22, 2002. There are no outstanding, unentered amendments.

5. SUMMARY OF INVENTION

The invention is an improved database system and method for redirecting and filtering Internet traffic. *Appellants' Specification* (hereinafter "Specification"), 1:10-11 (passages are indicated by page:line). One embodiment of the invention relates to a system and method including a database 206[1] with entries correlating each of a plurality of user IDs with an individualized rule set. A dial-up network server 102 receives user IDs from users' computers 100, and a redirection server 208 is connected to the dial-up network server 102 and a public network 110. An authentication accounting server 204 is connected to the database 206, the dial-up network server 102 and the redirection server 208. The dial-up network server 102 communicates a first user ID for one of the users' computers 100 and temporarily assigned network address for the first user ID to the authentication accounting server 204. The authentication accounting server 204 accesses the database 206 and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server 208. *Specification*, 4:8-13. Data directed toward the public network 110 from one of the users' computers 100 are processed by the redirection server 208 according the individualized rule set. *Specification*, 3:30-4:7.

One embodiment of the invention also redirects the data to and from the users' computers as a function of the individualized rule set. *Specification*, 3:26-28. In another embodiment, at least a portion of the rule set for a temporarily assigned network address is automatically modified or at least a portion of the rule set is modified while that rule set remains correlated to the temporarily assigned network address. *Specification*, 3:28-30.

[1] All numerals refer to FIG. 2.

6. ISSUES

(1) Whether claims 1-29 are unpatentable under 35 U.S.C. § 102(b) over Horowitz, et al. (WO 96/05549).

7. GROUPING OF CLAIMS

For purposes of this appeal, the claims are grouped as follows and for the purposes of this appeal only, the claims within each group stand and fall together. The claims consist of four independent claims, claims 1, 8, 15, and 26. Claims 1 and 15 claim systems and claims 8 and 26 claim methods corresponding to those systems. For determining anticipation within the meaning of 35 U.S.C. § 102(b), the groups are:

Group I - 1-4, 7-11, 14

Group II - 5-6, 12-13

Group III- 15-29

8. ARGUMENT

A. GROUP I

Group I includes claims 1-4, 7-11 and 14. Independent claim 1 recites a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network; and an authentication accounting server connected to the database, the dial-up network server and the redirection server, wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server, wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

The Examiner has rejected independent claim 1 under 35 U.S.C. §102(b) as being anticipated by *Horowitz*. *Horowitz* is directed to a local network[2] remote access server. *Horowitz*, Abstract. Remote users, such as telecommuters, can dial directly into a remote access server[3] that checks the remote users' IDs and passwords against a database. *Horowitz*, 3:15-28. The database also includes pre-programed access filters indicating to which of the known devices connected to the local network (e.g., other computers, printers, etc.) the user can have access. *Horowitz*, 3:32-4:5. The remote access server can then allow or block the user from access to a particular device.

Similar packet filtering is discussed in the Appellants' background section. Specifically, "packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device." *Specification*, 2:30-34. However, this disadvantage can be largely irrelevant on a local network because the devices and networks[4] on which the access filters are based are relatively static and known by the network administrator. *Horowitz* teaches that the database is "maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof." *Horowitz*, 8:31-9:2. Such control over a constantly changing *public* network, such as the Internet, is not feasible.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). *Horowitz* neither expressly nor inherently discloses every limitation of claim 1. Specifically, *Horowitz* does not disclose the claim element, "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." The entirety of the Examiner's grounds for rejection with respect to this element is that the element is "disclosed by *Horowitz*, in the abstract, specifically wherein it is stated that the server also includes processing

[2] *See*, e.g., *Horowitz*, Abstract, 1:5-10 and 3:1-7.

[3] *See Horowitz*, 4:6-23.

[4] *See Horowitz*, 3:29-4:5.

electronics which control the communication and network ports." *See* Final Office Action, p. 3. In an advisory action,[5] the Examiner essentially repeated this ground stating:

> Applicant's representative argues that Horowitz does not [disclose] any about 'a system that control a user's access to a public network'...However, the Examiner respectfully disagrees because Horowitz in the Abstract, specifically wherein it is stated that processing [electronics] which control the communication...see office action mailed on 10/12/2001.

For a finding of anticipation, "the identical invention must be shown in as complete detail as is contained in the ...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). However, nothing in the reference's passage from the Abstract cited by the Examiner discloses any data directed to a public network.

Although not explicitly stated, the Examiner appears to be making an assumption that "communication and network ports" inherently direct data to a public network. First, *Horowitz* fails to inherently anticipate the claimed element. "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295 (Fed. Cir. 2002). While it is true that it is possible to use "communication and network ports" to direct data to a public network, "communication and network ports" are often used in systems without directing data to a public network. For example, two stand alone computers directly connected over a telephone line with modems or two computers connected to each other in a simple LAN have "communication and network ports" controlled by processing electronics, but do not direct data toward a public network. Appellants therefore submit that the missing description of "directing data toward a public network" falls far short of being "necessarily present" in *Horowitz*, as is required by *Trintec Indus., Inc. v. Top-U.S.A. Corp.*

Second, the specific "communication and network ports" disclosed in *Horowitz* do not expressly teach or suggest anything about public networks or directing data to a public network. The "communication and network ports" in the *Horowitz* abstract cannot be read in

[5] *See*, Paper No. 14, sent November 8, 2002.

a vacuum. They must be read in the context of the *Horowitz* disclosure. The entirety of *Horowitz* that discusses these ports is as follows:

> Referring now to FIG. 4, in one embodiment, the remote access server 16 includes electronics 38, a plurality of serial communication ports 40_1-40_N, and a plurality of network ports 42_1-42_N. The server 16 also can include a plurality of internal modems 44_1-44_N. The serial ports 40 and the network ports 42 are controlled by the electronics 38.
>
> The electronics 38 include, in some embodiments, a powerful 16 MHz 68EC020 microprocessor and memory such as up to 1 megabyte of battery backed-up static random access memory (SRAM) and possible 64 kilobytes in an erasable programmable read only memory (EPROM).
>
> Each of the serial communication ports 40 is for coupling with a communication device (e.g., the modem 26 of FIG. 1), or for coupling directly with the telephone lines 22, *to provide for communication with a remote computer (e.g., the remote computer 12 of FIGS 1 and 2)* over the telephone lines 22. A connecting cable can be used to couple a serial port 40 with the communication device or with the telephone lines. Each of the serial ports 40 can simultaneously be coupled to a different one of the plurality of remote computers so as to provide simultaneous access to a local computer network for each of the remote computers, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC)...
>
> Each of the network ports 42 *is for coupling with a local computer network (e.g., the network 14 of FIGS. 1 and 2)*, via a connecting cable, to provide for communication with the network...In some embodiments, the server 16 includes three network ports 42, one for 10BaseT Ethernet, one for Thin Ethernet, and one for Thick Ethernet. In some other embodiments, the server 16 includes a single network port 42 for Token Ring. In some other embodiments, the server 16 includes a single network port 42 for use with Apple LocalTalk.

Horowitz, 16:24-17:14, 17:24-18:1 (emphasis added). As indicated in the emphasized portion of this disclosure, the "communications ports" provide communication with remote computers used to remotely access the network that includes the communication ports, not a public network. Similarly, the "network ports" are coupled to a local computer network, not a public network. Nowhere in this discussion is there any teaching or suggestion of a public network or the "communication and network ports" being connected to one, and, in fact, the entire disclosure is expressly directed to only a *private* network.

As discussed above, the differences between public and private networks are important. In private networks, such as in *Horowitz*, all of the resources and services are known. Private networks are "maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof." *Horowitz*, 8:31-9:2. All of the resources and services are known. Additionally, since these networks are "private," they are not accessible to the public. In a public network, the available resources and services are unknown and constantly changing. *Horowitz* states that an object of its access filter is to provide "security features" and "restrict access to the network on a per-user basis." Public networks are not secure and access is unrestricted. Because *Horowitz* fails to disclose the cited limitations either expressly or inherently, Appellants respectfully submit that claim 1 is not anticipated by *Horowitz*.

Independent claim 8 recites a method that corresponds to the system recited in claim 1. Appellants respectfully submit that claim 8 and its dependent claims 9-14 are therefore patentable over *Horowitz*. Appellants respectfully request that the rejections to claims 8-14 be withdrawn.

For all of the reasons stated above, Appellants respectfully submit that claim 1, its dependent claims 2-7, claim 8 and its dependent claims 9-14 are patentable over *Horowitz* and respectfully request that the rejection under §102 be withdrawn.

B. <u>GROUP II</u>.

Group II includes claims 5-6 and 12-13. Claims 5-6 and 12-13 recite systems and methods that redirect data to and from the users' computers via the redirection server as a function of the individualized rule set. The passages in *Horowitz* cited by the Examiner do not teach or suggest this limitation. Instead, these passages relate to only blocking or allowing access to the private network, or particular devices on the private network. *Horowitz*, Abstract, 9:20-29. The Appellants can find no teaching or suggestion anywhere in *Horowitz* of directing the data to or from the user to an alternate location based on the individualized rule set and the Examiner has not identified such teaching or suggestion.

Appellants include an extensive discussion regarding redirection of data in their specification. *Specification*, 1:29-2:16. Redirection involves the server "directing" the user to another area of the network. If the user chooses on its own to try to access another, allowable area of the network, this is clearly not redirection by tho server. *Horowitz*, therefore, does not disclose any server that redirects data, but rather only passively blocks or allows data. As this limitation is neither expressly or inherently present in *Horowitz*, Appellants respectfully request that the rejections to Group II be withdrawn. Additionally, Appellants submit that claims 5-6 and 12-13 are dependent on patentable independent claims 1 and 8, respectively, and should therefore be allowed. The difference between passive blocking and allowing data and the redirection in this group of claims also makes these claims patentably distinct from the claims in Group I, because the claims in Group I would cover passive blocking and allowing data.

C. GROUP III.

Group III includes claims 15-29. Independent claim 15 recites a system comprising a redirection server programed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network; and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address.

The Examiner has rejected independent claim 15 under 35 U.S.C. §102(b) as being anticipated by *Horowitz*. As discussed in relation to Group I, above, *Horowitz* contains no express or inherent teaching or suggestion of a public network, or a rule set with functions used to control passing between the user and a public network. Appellants therefore respectfully submit that claim 15 and its dependent claims 16-25 are allowable and request that their rejections be withdrawn.

Additionally, *Horowitz* contains no teaching or suggestion of "automated modification of at least a portion of the rule set correlated to the temporarily assigned network address." Although Appellant brought the absence of this element to the Examiner's attention in every communication,[6] the Examiner has failed to cite any teaching or suggestion in *Horowitz* that meets this element or respond to Appellants' argument in any way. Appellant respectfully submits that the Examiner has failed to show that claims 15-25 are expressly or inherently anticipated by *Horowitz*, and therefore requests that the rejections to these claims be withdrawn. The automated modification element also distinguishes the claims of Group III from the claims of Group I as even if the claims of Group I were anticipated by *Horowitz*, there would be no anticipation of the Group III claims because *Horowitz* does not disclose or suggest the automated modification element.

Independent claim 26 recites a method that corresponds generally to the system recited in claim 15. Appellants respectfully submit that claim 26 and its dependent claims 27-29 are therefore patentable over *Horowitz*. Specifically, the Examiner has not cited any portion of *Horwitz* as disclosing "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address." Appellants respectfully request that the rejections to Group III be withdrawn.

D. CONCLUSION.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Regarding Group I, the reference cited by the Examiner in support of his 35 U.S.C. §102(b) rejection fails to expressly or inherently teach or suggest "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." *Horowitz*, in fact, contains no teaching or suggestion of a public network at all, and is expressly related to only a private network. Regarding Group II, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "redirection of data to or from a user." Finally, regarding Group III, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "modification of a

[6] *See*, Response to Office Action sent July 30, 2001 p. 7, Telephone conference of October 10, 2002, and Response to Office Action sent October 22, 2002 p. 3.

rule set correlated to a temporarily assigned network address." In fact, the Examiner has offered no argument or reference related to this claim element. Accordingly, the Examiner has failed to make out a prima facie case of anticipation and the issuance of a notice of allowance is appropriate.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

9. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. A system comprising:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

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

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

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

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

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

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

15. A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

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

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

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

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

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

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

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

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

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

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

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

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

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

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server.

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

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

29. The method of claim 26, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of:.

receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

WWM/rah

MC PAS474061.2-*-11/22/02 9:18 PM

Exhibit B

CHRISTIE, PARKER & HALE P.O. BOX 7068, PASADENA, CALIFORNIA 91109-7068

010023

REMITTANCE ADVICE

PLEASE DETACH BEFORE DEPOSITING CHECK

CLIENT NAME	CASE NO. & ATTORNEY	CHECK APPROPRIATE ITEM TO BE CHARGED
AURIC WEB SYSTEMS **A522**	**34503** **WWM/eaj**	___ ISSUE FEE ___ ADVANCE ORDER OF PATENT COPIES ___ FILING AND RECORDING FEE ___ FILING FEE ___ RECORDING FEE ___ FEE FOR ADDITIONAL CLAIMS X FEE FOR EXTENSION OF TIME **$260.00** ___ FILING FEE FOR SIXTH-YEAR DECLARATION ___ RENEWAL FEE ___ MAINTENANCE FEE ___ OTHER ___

USE SEPARATE CHECK FOR EACH CLIENT AND CASE NUMBER

CASE NO. & ATTORNEY
A522:34503/WWM

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

The Citibank Private Bank, Branch 395
787 W. 5th St., 28th Floor
Los Angeles, CA 90071

90-7172
3222

010023

PAY **$**260.00****

NOT VALID IN EXCESS OF $3,000.00

DATE	AMOUNT
Nov 22, 2002	**$260.00**

TO THE ORDER OF ▶ COMMISSIONER OF PATENTS & TRADEMARKS
WASHINGTON, D.C. 20231

Byron C Hibbon

⑈010023⑈ ⑆322271724⑆ 200013092⑈

010023

CHRISTIE, PARKER & HALE P.O. BOX 7068, PASADENA, CALIFORNIA 91109-7068

ACCOUNTING COPY

PLEASE DETACH BEFORE DEPOSITING CHECK

CLIENT NAME	CASE NO. & ATTORNEY	CHECK APPROPRIATE ITEM TO BE CHARGED
AURIC WEB SYSTEMS **A522**	**34503** **WWM/eaj**	___ ISSUE FEE ___ ADVANCE ORDER OF PATENT COPIES ___ FILING AND RECORDING FEE ___ FILING FEE ___ RECORDING FEE ___ FEE FOR ADDITIONAL CLAIMS X FEE FOR EXTENSION OF TIME **$260.00** ___ FILING FEE FOR SIXTH-YEAR DECLARATION ___ RENEWAL FEE ___ MAINTENANCE FEE ___ OTHER ___

USE SEPARATE CHECK FOR EACH CLIENT AND CASE NUMBER

CHRISTIE, PARKER & HALE P.O. BOX 7068, PASADENA, CALIFORNIA 91109-7068 010021

REMITTANCE ADVICE

PLEASE DETACH BEFORE DEPOSITING CHECK

CLIENT NAME	CASE NO. & ATTORNEY	CHECK APPROPRIATE ITEM TO BE CHARGED
AURIC WEB SYSTEMS **A522**	**34503** **WWM/eaj**	____ ISSUE FEE ____ ADVANCE ORDER OF PATENT COPIES ____ FILING AND RECORDING FEE x___ FILING FEE **$160.00** ____ RECORDING FEE FEE FOR ADDITIONAL CLAIMS ____ FEE FOR EXTENSION OF TIME ____ FILING FEE FOR SIXTH-YEAR DECLARATION ____ RENEWAL FEE ____ MAINTENANCE FEE ____ OTHER ____________

USE SEPARATE CHECK FOR EACH CLIENT AND CASE NUMBER

CASE NO. & ATTORNEY
A522:34503/WWM

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

The Citibank Private Bank, Branch 395
787 W 5th St., 28th Floor
Los Angeles, CA 90071
90-7172
3222

010021

PAY **$**160.00****

NOT VALID IN EXCESS OF $3,000.00

DATE	AMOUNT
Nov 22, 2002	**$160.00**

TO THE ORDER OF ▶ COMMISSIONER OF PATENTS & TRADEMARKS
WASHINGTON, D.C. 20231

Byron C. Hibdon

⑈010021⑈ ⑆322271724⑆ 200013092⑈

010021

CHRISTIE, PARKER & HALE P.O. BOX 7068, PASADENA, CALIFORNIA 91109-7068

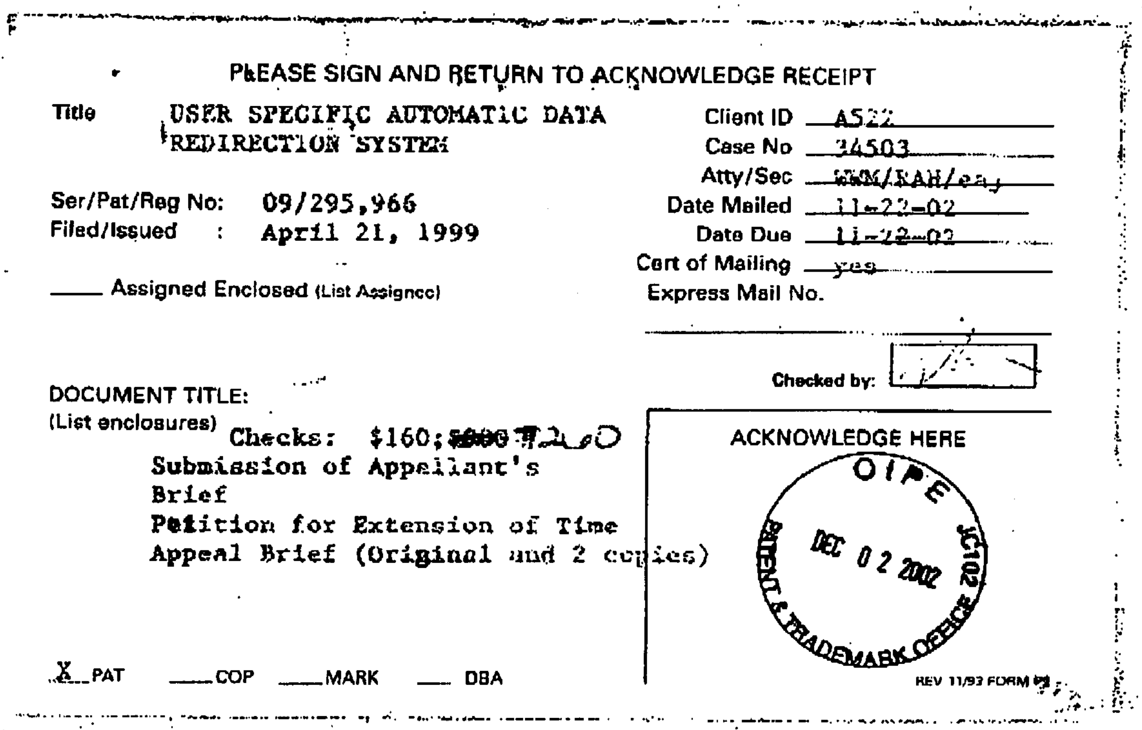
ACCOUNTING COPY

PLEASE DETACH BEFORE DEPOSITING CHECK

CLIENT NAME	CASE NO. & ATTORNEY	CHECK APPROPRIATE ITEM TO BE CHARGED
AURIC WEB SYSTEMS **A522**	**34503** **WWM/eaj**	____ ISSUE FEE ____ ADVANCE ORDER OF PATENT COPIES ____ FILING AND RECORDING FEE x FILING FEE **$160.00** ____ RECORDING FEE ____ FEE FOR ADDITIONAL CLAIMS ____ FEE FOR EXTENSION OF TIME ____ FILING FEE FOR SIXTH-YEAR DECLARATION ____ RENEWAL FEE ____ MAINTENANCE FEE ____ OTHER ____________

USE SEPARATE CHECK FOR EACH CLIENT AND CASE NUMBER

Exhibit C



PLEASE SIGN AND RETURN TO ACKNOWLEDGE RECEIPT

Title USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Ser/Pat/Reg No: 09/295,966
Filed/Issued : April 21, 1999

____ Assigned Enclosed (List Assignee)

Client ID A522
Case No 34503
Atty/Sec WMM/KAH/eaj
Date Mailed 11-22-02
Date Due 11-22-02
Cert of Mailing yes
Express Mail No.

Checked by:

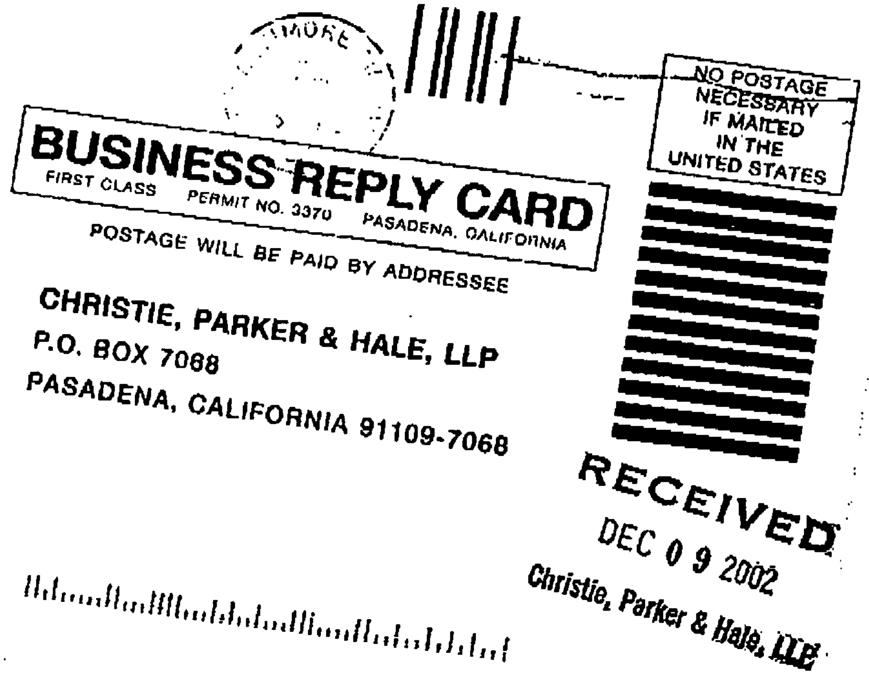
DOCUMENT TITLE:
(List enclosures)

Checks: $160; ~~$000~~ 320
Submission of Appellant's Brief
Petition for Extension of Time
Appeal Brief (Original and 2 copies)

X PAT ____ COP ____ MARK ____ DBA

ACKNOWLEDGE HERE

REV 11/93 FORM



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY CARD

FIRST CLASS PERMIT NO. 3370 PASADENA, CALIFORNIA

POSTAGE WILL BE PAID BY ADDRESSEE

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CALIFORNIA 91109-7068

Copy of

#5 1/7/18

facsimile TRANSMITTAL

Date: April 2, 2003
No. of Pages: 26 (including this cover sheet)
Fax No: (703) 746-7238

PLEASE DELIVER THE FOLLOWING PAGES IMMEDIATELY TO:

Name: James Trammell
Art Unit: 3621
Examiner: Pierre Eddy Elisca
Phone: (703) 305-9768
From: Wesley W. Monroe
Reg. No. 39,778
Re: Application No. 09/295,966; Filed April 21, 1999
Entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
File: **34503/WWM/A522**

Mr. Trammell,

Thank you for your response to Rose Hickman's phone call last week regarding the Patent Office's procedure for resubmitting an Appeal Brief that was lost at the Patent Office. Pursuant to your instructions, we are submitting to your attention: a copy of the originally filed Appeal Brief and transmittal (Exhibit A); copies of the checks that were deposited by the Patent Office (Exhibit B); and a copy of the return postcard indicating receipt of the above by the Patent Office (Exhibit C).

Please let us know when the Appeal has been reinstated or if you have any questions.

Thank you,
Wes Monroe

I HEREBY CERTIFY THAT THIS PAPER IS BEING FACSIMILE TRANSMITTED TO THE PATENT AND TRADEMARK OFFICE ON **April 2, 2003.**

Signature

Christie, Parker & Hale, LLP
350 West Colorado Boulevard
Post Office Box 7068
Pasadena, CA 91109-7068
626-795-9900
Fax: 626-577-8800

For Office Services Use Only
Return to Wes Monroe

confidential

The information in this transmission is confidential and is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone collect, and return the original message to us at the above address via U.S. mail. We will reimburse you for postage. Thank you.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 03/24/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	**PAPER NUMBER**
3621	15

DATE MAILED: 03/24/2003

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

PTO-90C (Rev. 07-01)

Notice of Abandonment	Application No. 09/295,966	Applicant(s) Koichiro, Ikudome et al.	
	Examiner Pierre E. Elisca	Art Unit 3621	

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

This application is abandoned in view of:

1.☒ Applicant's failure to timely file a proper reply to the Office letter mailed on *Nov 8, 2002* .

(a) □ A reply was received on ________________ (with a Certificate of Mailing or Transmission dated ________________), which is after the expiration of the period for reply (including a total extension of time of ____ month(s)) which expired on ________________ .

(b) □ A proposed reply was received on ________________ , but it does not constitute a proper reply under 37 CFR 1.113(a) to the final rejection.

(A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114).

(c) □ A reply was received on ________________ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).

(d) ☒ No reply has been received.

2.□ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).

(a) □ The issue fee and publication fee, if applicable, was received on ______________ (with a Certificate of Mailing or Transmission dated ______________), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).

(b) □ The submitted issue fee of $_______ is insufficient. A balance of $_______ is due.

The issue fee required by 37 CFR 1.18 is $_______ . The publication fee, if required by 37 CFR 1.18(d) is $_______

(c) □ The issue fee and publication fee, if applicable, has not been received.

3.□ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).

(a) □ Proposed new formal drawings were received on ________________ (with a Certificate of Mailing or Transmission dated ________________), which is after the expiration of the period for reply.

(b) □ No corrected drawings have been received.

4.□ The letter of express abandonment which is signed by the attorney or agent of record, the assignee of the entire interest, or all of the applicants.

5.□ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34(a)) upon the filing of a continuing application.

6.□ The decision by the Board of Patent Appeals and Interferences rendered on ________________ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7.□ The reason(s) below:

Petitions to revive under 37 CFR 1.137(a) or (b), or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

#18/Brief Appeal

PATENT

4-25-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Name

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre E. Elisca
Docket No.	:	34503/WWM/A522

APPELLANT'S BRIEF

Post Office Box 7068
Pasadena, CA 91109-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

This is an appeal from the Final Rejection, dated October 12, 2001, of the claims in the above-referenced application.

1. REAL PARTY IN INTEREST

The real party in interest is the assignee of the subject application, Auric Web Systems.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-29 are pending in the present application.

Claims 1-29 have been rejected in a final rejection, dated October 12, 2001 under 35 U.S.C. §102(b).

The claims on appeal are claims 1-29.

4. STATUS OF AMENDMENTS

Appellants submitted additional remarks in a response to the final rejection. This response did not amend any claims. The response was not deemed to overcome the rejections. *See,* Paper 14, dated October 22, 2002. There are no outstanding, unentered amendments.

5. SUMMARY OF INVENTION

The invention is an improved database system and method for redirecting and filtering Internet traffic. *Appellants' Specification* (hereinafter "Specification"), 1:10-11 (passages are indicated by page:line). One embodiment of the invention relates to a system and method including a database 206[1] with entries correlating each of a plurality of user IDs with an individualized rule set. A dial-up network server 102 receives user IDs from users' computers 100, and a redirection server 208 is connected to the dial-up network server 102 and a public network 110. An authentication accounting server 204 is connected to the database 206, the dial-up network server 102 and the redirection server 208. The dial-up network server 102 communicates a first user ID for one of the users' computers 100 and temporarily assigned network address for the first user ID to the authentication accounting server 204. The authentication accounting server 204 accesses the database 206 and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server 208. *Specification,* 4:8-13. Data directed toward the public network 110 from one of the users' computers 100 are processed by the redirection server 208 according the individualized rule set. *Specification,* 3:30-4:7.

One embodiment of the invention also redirects the data to and from the users' computers as a function of the individualized rule set. *Specification,* 3:26-28. In another embodiment, at least a portion of the rule set for a temporarily assigned network address is automatically modified or at least a portion of the rule set is modified while that rule set remains correlated to the temporarily assigned network address. *Specification,* 3:28-30.

[1] All numerals refer to FIG. 2.

6. ISSUES

(I) Whether claims 1-29 are unpatentable under 35 U.S.C. § 102(b) over Horowitz, et al. (WO 96/05549).

7. GROUPING OF CLAIMS

For purposes of this appeal, the claims are grouped as follows and for the purposes of this appeal only, the claims within each group stand and fall together. The claims consist of four independent claims, claims 1, 8, 15, and 26. Claims 1 and 15 claim systems and claims 8 and 26 claim methods corresponding to those systems. For determining anticipation within the meaning of 35 U.S.C. § 102(b), the groups are:

Group I - 1-4, 7-11, 14

Group II - 5-6, 12-13

Group III- 15-29

8. ARGUMENT

A. <u>GROUP I</u>

Group I includes claims 1-4, 7-11 and 14. Independent claim 1 recites a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network; and an authentication accounting server connected to the database, the dial-up network server and the redirection server, wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server, wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

The Examiner has rejected independent claim 1 under 35 U.S.C. §102(b) as being anticipated by *Horowitz*. *Horowitz* is directed to a local network[2] remote access server. *Horowitz,* Abstract. Remote users, such as telecommuters, can dial directly into a remote access server[3] that checks the remote users' IDs and passwords against a database. *Horowitz,* 3:15-28. The database also includes pre-programed access filters indicating to which of the known devices connected to the local network (e.g., other computers, printers, etc.) the user can have access. *Horowitz,* 3:32-4:5. The remote access server can then allow or block the user from access to a particular device.

Similar packet filtering is discussed in the Appellants' background section. Specifically, "packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device." *Specification,* 2:30-34. However, this disadvantage can be largely irrelevant on a local network because the devices and networks[4] on which the access filters are based are relatively static and known by the network administrator. *Horowitz* teaches that the database is "maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof." *Horowitz,* 8:31-9:2. Such control over a constantly changing *public* network, such as the Internet, is not feasible.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.,* 814 F.2d 628, 631 (Fed. Cir. 1987). *Horowitz* neither expressly nor inherently discloses every limitation of claim 1. Specifically, *Horowitz* does not disclose the claim element, "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." The entirety of the Examiner's grounds for rejection with respect to this element is that the element is "disclosed by *Horowitz,* in the abstract, specifically wherein it is stated that the server also includes processing

[2] *See,* e.g., *Horowitz,* Abstract, 1:5-10 and 3:1-7.

[3] *See Horowitz,* 4:6-23.

[4] *See Horowitz,* 3:29-4:5.

electronics which control the communication and network ports." *See* Final Office Action, p. 3. In an advisory action,[5] the Examiner essentially repeated this ground stating:

> Applicant's representative argues that Horowitz does not [disclose] any about 'a system that control a user's access to a public network'...However, the Examiner respectfully disagrees because Horowitz in the Abstract, specifically wherein it is stated that processing [electronics] which control the communication...see office action mailed on 10/12/2001.

For a finding of anticipation, "the identical invention must be shown in as complete detail as is contained in the ...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). However, nothing in the reference's passage from the Abstract cited by the Examiner discloses any data directed to a public network.

Although not explicitly stated, the Examiner appears to be making an assumption that "communication and network ports" inherently direct data to a public network. First, *Horowitz* fails to inherently anticipate the claimed element. "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295 (Fed. Cir. 2002). While it is true that it is possible to use "communication and network ports" to direct data to a public network, "communication and network ports" are often used in systems without directing data to a public network. For example, two stand alone computers directly connected over a telephone line with modems or two computers connected to each other in a simple LAN have "communication and network ports" controlled by processing electronics, but do not direct data toward a public network. Appellants therefore submit that the missing description of "directing data toward a public network" falls far short of being "necessarily present" in *Horowitz,* as is required by *Trintec Indus., Inc. v. Top-U.S.A. Corp.*

Second, the specific "communication and network ports" disclosed in *Horowitz* do not expressly teach or suggest anything about public networks or directing data to a public network. The "communication and network ports" in the *Horowitz* abstract cannot be read in

[5] *See,* Paper No. 14, sent November 8, 2002.

a vacuum. They must be read in the context of the *Horowitz* disclosure. The entirety of *Horowitz* that discusses these ports is as follows:

> Referring now to FIG. 4, in one embodiment, the remote access server 16 includes electronics 38, a plurality of serial communication ports 40_1-40_N, and a plurality of network ports 42_1-42_N. The server 16 also can include a plurality of internal modems 44_1-44_N. The serial ports 40 and the network ports 42 are controlled by the electronics 38.
>
> The electronics 38 include, in some embodiments, a powerful 16 MHz 68EC020 microprocessor and memory such as up to 1 megabyte of battery backed-up static random access memory (SRAM) and possible 64 kilobytes in an erasable programmable read only memory (EPROM).
>
> Each of the serial communication ports 40 is for coupling with a communication device (e.g., the modem 26 of FIG. 1), or for coupling directly with the telephone lines 22, *to provide for communication with a remote computer (e.g., the remote computer 12 of FIGS 1 and 2)* over the telephone lines 22. A connecting cable can be used to couple a serial port 40 with the communication device or with the telephone lines. Each of the serial ports 40 can simultaneously be coupled to a different one of the plurality of remote computers so as to provide simultaneous access to a local computer network for each of the remote computers, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC)...
>
> Each of the network ports 42 *is for coupling with a local computer network (e.g., the network 14 of FIGS. 1 and 2),* via a connecting cable, to provide for communication with the network...In some embodiments, the server 16 includes three network ports 42, one for 10BaseT Ethernet, one for Thin Ethernet, and one for Thick Ethernet. In some other embodiments, the server 16 includes a single network port 42 for Token Ring. In some other embodiments, the server 16 includes a single network port 42 for use with Apple LocalTalk.

Horowitz, 16:24-17:14, 17:24-18:1 (emphasis added). As indicated in the emphasized portion of this disclosure, the "communications ports" provide communication with remote computers used to remotely access the network that includes the communication ports, not a public network. Similarly, the "network ports" are coupled to a local computer network, not a public network. Nowhere in this discussion is there any teaching or suggestion of a public network or the "communication and network ports" being connected to one, and, in fact, the entire disclosure is expressly directed to only a *private* network.

As discussed above, the differences between public and private networks are important. In private networks, such as in *Horowitz,* all of the resources and services are known. Private networks are "maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof." *Horowitz,* 8:31-9:2. All of the resources and services are known. Additionally, since these networks are "private," they are not accessible to the public. In a public network, the available resources and services are unknown and constantly changing. *Horowitz* states that an object of its access filter is to provide "security features" and "restrict access to the network on a per-user basis." Public networks are not secure and access is unrestricted. Because *Horowitz* fails to disclose the cited limitations either expressly or inherently, Appellants respectfully submit that claim 1 is not anticipated by *Horowitz.*

Independent claim 8 recites a method that corresponds to the system recited in claim 1. Appellants respectfully submit that claim 8 and its dependent claims 9-14 are therefore patentable over *Horowitz.* Appellants respectfully request that the rejections to claims 8-14 be withdrawn.

For all of the reasons stated above, Appellants respectfully submit that claim 1, its dependent claims 2-7, claim 8 and its dependent claims 9-14 are patentable over *Horowitz* and respectfully request that the rejection under §102 be withdrawn.

B. <u>GROUP II</u>.

Group II includes claims 5-6 and 12-13. Claims 5-6 and 12-13 recite systems and methods that redirect data to and from the users' computers via the redirection server as a function of the individualized rule set. The passages in *Horowitz* cited by the Examiner do not teach or suggest this limitation. Instead, these passages relate to only blocking or allowing access to the private network, or particular devices on the private network. *Horowitz,* Abstract, 9:20-29. The Appellants can find no teaching or suggestion anywhere in *Horowitz* of directing the data to or from the user to an alternate location based on the individualized rule set and the Examiner has not identified such teaching or suggestion.

Appellants include an extensive discussion regarding redirection of data in their specification. *Specification,* 1:29-2:16. Redirection involves the server "directing" the user to another area of the network. If the user chooses on its own to try to access another, allowable area of the network, this is clearly not redirection by the server. *Horowitz,* therefore, does not disclose any server that redirects data, but rather only passively blocks or allows data. As this limitation is neither expressly or inherently present in *Horowitz,* Appellants respectfully request that the rejections to Group II be withdrawn. Additionally, Appellants submit that claims 5-6 and 12-13 are dependent on patentable independent claims 1 and 8, respectively, and should therefore be allowed. The difference between passive blocking and allowing data and the redirection in this group of claims also makes these claims patentably distinct from the claims in Group I, because the claims in Group I would cover passive blocking and allowing data.

C. GROUP III.

Group III includes claims 15-29. Independent claim 15 recites a system comprising a redirection server programed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network; and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address.

The Examiner has rejected independent claim 15 under 35 U.S.C. §102(b) as being anticipated by *Horowitz.* As discussed in relation to Group I, above, *Horowitz* contains no express or inherent teaching or suggestion of a public network, or a rule set with functions used to control passing between the user and a public network. Appellants therefore respectfully submit that claim 15 and its dependent claims 16-25 are allowable and request that their rejections be withdrawn.

Additionally, *Horowitz* contains no teaching or suggestion of "automated modification of at least a portion of the rule set correlated to the temporarily assigned network address." Although Appellant brought the absence of this element to the Examiner's attention in every communication,[6] the Examiner has failed to cite any teaching or suggestion in *Horowitz* that meets this element or respond to Appellants' argument in any way. Appellant respectfully submits that the Examiner has failed to show that claims 15-25 are expressly or inherently anticipated by *Horowitz,* and therefore requests that the rejections to these claims be withdrawn. The automated modification element also distinguishes the claims of Group III from the claims of Group I as even if the claims of Group I were anticipated by *Horowitz,* there would be no anticipation of the Group III claims because *Horowitz* does not disclose or suggest the automated modification element.

Independent claim 26 recites a method that corresponds generally to the system recited in claim 15. Appellants respectfully submit that claim 26 and its dependent claims 27-29 are therefore patentable over *Horowitz.* Specifically, the Examiner has not cited any portion of *Horwitz* as disclosing "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address." Appellants respectfully request that the rejections to Group III be withdrawn.

D. CONCLUSION.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Regarding Group I, the reference cited by the Examiner in support of his 35 U.S.C. §102(b) rejection fails to expressly or inherently teach or suggest "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." *Horowitz,* in fact, contains no teaching or suggestion of a public network at all, and is expressly related to only a private network. Regarding Group II, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "redirection of data to or from a user." Finally, regarding Group III, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "modification of a

[6] *See,* Response to Office Action sent July 30, 2001 p. 7, Telephone conference of October 10, 2002, and Response to Office Action sent October 22, 2002 p. 3.

rule set correlated to a temporarily assigned network address." In fact, the Examiner has offered no argument or reference related to this claim element. Accordingly, the Examiner has failed to make out a prima facie case of anticipation and the issuance of a notice of allowance is appropriate.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

9. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. A system comprising:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

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

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

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

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

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

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

15. A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

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

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

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

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

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

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

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

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

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

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

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

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

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

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server.

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

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

29. The method of claim 26, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of:.

receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

WWM/rah

MC PAS474061.2-*-11/22/02 9:18 PM

#17/EOT (1)
Lowman

PATENT
4-25-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PETITION FOR EXTENSION OF TIME FROM THE NOTICE OF APPEAL

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Marsha Comfort

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div	:	3621
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Notice of Appeal filed April 12, 2002 and made under 37 CFR § 1.136(a) for one month(s) from October 22, 2002 to November 22, 2002.

The fee for extension of time required by 37 CFR § 1.17 is calculated below.

FEE CALCULATION			
LENGTH OF EXTENSION	SMALL ENTITY	LARGE ENTITY	FEE
WITHIN FIRST MONTH	$ 55	$110	$
WITHIN SECOND MONTH	$200	$400	$
WITHIN THIRD MONTH	$460	$920	$
WITHIN FOURTH MONTH	$720	$1440	$

WITHIN FIFTH MONTH	$980	$1960	$260.00 (difference between the fourth and fifth month extension fees - 4th extension was filed on October 22, 2002)

Submitted herewith is a check for **$260.00** to cover the cost of the extension.

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed**.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/eaj
EAJ PAS475047.1-*-11/22/02 5:38 PM

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	3621
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

SUBMISSION OF APPELLANT'S BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Post Office Box 7068
Pasadena, CA 91101-7068
November 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Enclosed for filing are the **original and two copies** of Appellant's Brief for this application.

X An extension of time to file Appellant's Brief is requested, and a Petition for Extension of Time and the applicable fee are enclosed.

X Our check for $160.00 to cover the fee for the appeal brief is enclosed.

_____ An oral hearing of the appeal is requested, and our check for $, the fee for the oral hearing, is enclosed.

The Commissioner is hereby authorized to charge any further fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/eaj

ﾚ

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 11/08/2002

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	**PAPER NUMBER**
3621	14

DATE MAILED: 11/08/2002

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

PTO-90C (Rev. 07-01)

Advisory Action

Application No. 09/295,966	Applicant(s) Koichiro, Ikudome et al.		
Examiner Pierre E. Elisca		Art Unit 3621	

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

THE REPLY FILED Oct 22, 2002 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE. Therefore, further action by the applicant is required to avoid the abandonment of this application. A proper reply to a final rejection under 37 CFR 1.113 may only be either: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114.

THE PERIOD FOR REPLY [check only a) or b)]

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection. ONLY CHECK THIS BOX WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

1.□ A Notice of Appeal was filed on ____________. Appellant's Brief must be filed within the period set forth in 37 CFR 1.192(a), or any extension thereof (37 CFR 1.191(d)), to avoid dismissal of the appeal.

2.□ The proposed amendment(s) will not be entered because:

(a) □ they raise new issues that would require further consideration and/or search (see NOTE below);

(b) □ they raise the issue of new matter (see NOTE below);

(c) □ they are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) □ they present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: ____________

3.□ Applicant's reply has overcome the following rejection(s): ____________

4.□ Newly proposed or amended claim(s) ____________ -would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

5.☒ The ~~a) □ affidavit, b) □ exhibit, or~~ c) ☒ request for reconsideration has been considered but does NOT place the application in condition for allowance because: APPLICANT'S REPRESENTATIVE ARGUES THAT HOROWITZ DOES NOT DISCLOSE ANY ABOUT "A SYSTEM THAT CONTROL A USER'S ACCESS TO A PUBLIC NETWORK". HOWEVER, THE EXAMINER RESPECTFULLY DISAGREES BECAUSE HOROWITZ IN THE ABSTRACT, SPECIFICALLY WHEREIN IT'S STATED THAT PROCESSING ELECTR WHICH CONTROL THE COMMUNICATION... SEE OFFICE ACTION MAILED ON 10/12/2001.

6.□ The affidavit or exhibit will NOT be considered because it is not directed SOLELY to issues which were newly raised by the Examiner in the final rejection.

7.☒ For purposes of Appeal, the proposed amendment(s) a)□ will not be entered or b)□ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: ____________

Claim(s) objected to: ____________

Claim(s) rejected: 1-29

Claim(s) withdrawn from consideration: ____________

8.□ The proposed drawing correction filed on ____________ is a)□ approved or b)□ disapproved by the Examiner.

9.□ Note the attached Information Disclosure Statement(s) (PTO-1449) Paper No(s). ____________.

10.□ Other:

13 (N) Response after appeal
L. Lewis
10-26-02

PATENT

RESPONSE UNDER 37 CFR 1.116
EXPEDITED PROCEDURE
EXAMINING GROUP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being sent via facsimile to the Commissioner of Patents and Trademarks, Washington, D.C. 20231 on October 22, 2002.

Christina L. Vann

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp/Div.	:	2161
Examiner	:	P. Elisca
Docket No.	:	34503/WWM/A522

RESPONSE TO FINAL ACTION

Box AF
Assistant Commissioner for Patents
Washington, D.C. 20231

Post Office Box 7068
Pasadena, CA 91109-7068
October 22, 2002

Commissioner:

In the Office action dated October 12, 2001, the Examiner rejected claims 1-29 under Section 102(b) as being anticipated by Horowitz et al. Specifically, with respect to the claim element, "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set," the Examiner asserted that this element is "disclosed by Horowitz, in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports." It respectfully submitted that this application of Horowitz is incorrect. Horowitz is entirely about remote access to a private network. See, abstract, "A remote access server limits access to a local computer network." The system of Horowitz acts to limit the access of a user's access to the local private computer network to particular network resources and services as restricted by an access filter. Horowitz does not disclose anything about a system that controls a user's access to a public network, such as the Internet. In fact, applicants could not find any disclosure in Horowitz related to public networks.

To address the examiner's specific conclusion regarding the "processing electronics which control the communication and network ports," these ports only connect between a remote access computer and the local private network. As stated in the abstract, "The server includes at least one communication port for allowing communication with a remote computer and at least one network port for coupling to a local computer network to allow communication with the local computer network." The communication and network ports controlled by processing electronics are further described in the specification as serial communication ports 40_1 - 40_N and network ports 42_1 - 42_N on FIG. 4 and discussed at page 16, line 24 - page 18, line 1. Just like the abstract, this disclosure makes clear that communication ports 40_1 - 40_N and network ports 42_1 - 42_N are only used for connection by remote access computers to the local network, which is private. Thus, as the communication and network ports of Horowitz only carry data between a remote computer and a private network (over private telephone lines) and not between a user and a public network, they cannot be properly read on the claimed processing of data directed toward the public network from the one of the users' computers by a redirection server.

The difference between a access to a private network and a public network is significant. For example, all of the resources and services of a private network are known. They are also, by their nature, not available to the public, absent some particular connection to a remote site, that is also known. In the case of a public network, access to the network is not restricted and the identity of the computers and users that have access to the network is unknown. Further, the resources and services available on the public are not known and, in fact, are in a constant state of flux. The stated reason for the access filter in Horowitz is so to provide "security features" and to "restrict access to the network on a per-user basis." Public networks, by their nature are not secure and access is not restricted. Thus, the motivation for using Horowitz' access filters does not exist for public networks. Thus there it would not be obvious to apply anything in Horowitz to controlling access to a public network.

In the Office action date October 12, 2001, the Examiner comments that the remote user will not be allowed to communicate with a zone or device that the user should not have access to, regardless of the remote computer used in the attempt to gain access, but that the remote user will be able to communicate with non-restricted parts of the network. The examiner contends that this is a redirection towards another direction, in apparent response to applicants' arguments with respect to dependent claims 5, 6, 12 and 13 (first full paragraph on page 7 of Amendment dated July 30, 2001). However, it is respectfully submitted that while the function cited by the examiner blocks access to particular zones or devices, it does not redirect access. Redirection involves the server "directing" the user to another area of the network. If the user chooses on its own to try to access another, allowable area of the network, this is not redirection by the server, but redirection by the user that is simply allowed by the server. Horowitz does not disclose any server that redirects data, but rather only passively blocks or allows data.

With respect to claims 15-29, applicants cannot find any application by the Examiner of Horowitz to the claimed elements, "wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address" (claim 15) or "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server" (claim 26). The Examiner is reminded that applicants also made this argument in the second full paragraph on page 7 of the Amendment dated July 30, 2001, but applicants do not find any response to this argument in the Office action of October 12, 2001.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By

Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/clv

CLV PAS468519.1-*-10/22/02 4:35 PM

facsimile TRANSMITTAL

Date:	October 22, 2002
No. of Pages:	6 (including this cover sheet)
Fax No:	703-746-7238

PLEASE DELIVER THE FOLLOWING PAGES IMMEDIATELY TO:

Name:	Commissioner for Patents
Art Unit:	2161
Examiner:	P. Elisca
Phone:	703-305-3987
From:	Wesley W. Monroe Reg. No. 39,778
Re:	Application No. 09/295,966; Filed April 21,1999 Entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
File:	**34503/WWM/A522**

I HEREBY CERTIFY THAT THIS PAPER IS BEING FACSIMILE TRANSMITTED TO THE PATENT AND TRADEMARK OFFICE ON **October 22, 2002.**

Christina L. Vann

Christie, Parker & Hale, LLP
350 West Colorado Boulevard
Post Office Box 7068
Pasadena, CA 91109-7068
626-795-9900
Fax: 626-577-8800

For Office Services Use Only
Return to Christina L. Vann

confidential

The information in this transmission is confidential and is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is prohibited. If you have received this communication in error, please notify us immediately by telephone collect, and return the original message to us at the above address via U.S. mail. We will reimburse you for postage. Thank you.

128

2854

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE PETITION FOR EXTENSION OF TIME FROM THE NOTICE OF APPEAL

I hereby certify that this correspondence is being sent via facsimile to the Commissioner of Patents and Trademarks, Washington, D.C. 20231 on October 22, 2002.

Christina L. Vann

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div	:	2161
Examiner	:	P. Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
October 22, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Notice of Appeal filed April 22, 2002 and made under 37 CFR § 1.136(a) for four month(s) from June 22, 2002 to October 22, 2002.

The fee for extension of time required by 37 CFR § 1.17 is calculated below.

FEE CALCULATION			
LENGTH OF EXTENSION	SMALL ENTITY	LARGE ENTITY	FEE
WITHIN FIRST MONTH	$ 55	$110	$0
WITHIN SECOND MONTH	$200	$400	$0
WITHIN THIRD MONTH	$460	$920	$0
WITHIN FOURTH MONTH	$720	$1440	$720
WITHIN FIFTH MONTH	$980	$1960	$0

PETITION FOR EXTENSION OF TIME
Application No. 09/295,966

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/clv
CLV PAS408527.1-*-10/22/02 4:42 PM

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/295,966	04/21/1999	KOICHIRO IKUDOME	34503/WWM/A5	7800

23363 7590 10/15/2002

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	PAPER NUMBER
3621	#12

DATE MAILED: 10/15/2002

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

PTO-90C (Rev. 07-01)

Interview Summary	Application No. 09/295,966	Applicant(s) Koichiro, Ikudome et al.	
	Examiner Pierre E. Elisca		Art Unit 3621

All participants (applicant, applicant's representative, PTO personnel):

(1) *Pierre E. Elisca* (3) ________

(2) *West Monroe* (4) ________

Date of Interview *Oct 10, 2002*

Type: a)☒ Telephonic b)□ Video Conference
c)□ Personal [copy is given to 1)□ applicant 2)☒ applicant's representative]

Exhibit shown or demonstration conducted: d)□ Yes e)☒ No. If yes, brief description:

Claim(s) discussed:

Identification of prior art discussed:

Agreement with respect to the claims f)□ was reached. g)□ was not reached. h)□ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments:

DISCUSSED THE CLAIMED INVENTION.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

i)☒ It is not necessary for applicant to provide a separate record of the substance of the interview (if box is checked).

Unless the paragraph above has been checked, THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

UNITED STA DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

#11/Change of Address
8.03.02

CHANGE OF ADDRESS/POWER OF ATTORNEY

FILE LOCATION 36X1 SERIAL NUMBER 09295966 PATENT NUMBER

THE CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER # 23363

THE PRACTITIONERS OF RECORD HAVE BEEN CHANGED TO CUSTOMER # 23363

THE FEE ADDRESS HAS BEEN CHANGED TO CUSTOMER # 23363

ON 07/24/02 THE ADDRESS OF RECORD FOR CUSTOMER NUMBER 23363 IS:

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA CA 91105

AND THE PRACTITIONERS OF RECORD FOR CUSTOMER NUMBER 23363 ARE:

17968 19959 20356 20958 22134 22183 22653 22671 22994 24187
25312 25355 25373 28301 29371 29946 30831 31135 31953 32213
33485 34133 34849 35581 36045 36593 37208 38985 39559 39739
39759 39778 40285 41057 41159 41661 41886 42052 42419 42681
43693 43945 44257 44284 44548 44641 44816 46083 47317 47822
50517 50791 51304

PTO INSTRUCTIONS: PLEASE TAKE THE FOLLOWING ACTION WHEN THE CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER NUMBER: RECORD, ON THE NEXT AVAILABLE CONTENTS LINE OF THE FILE JACKET, 'ADDRESS CHANGE TO CUSTOMER NUMBER'. LINE THROUGH THE OLD ADDRESS ON THE FILE JACKET LABEL AND ENTER ONLY THE 'CUSTOMER NUMBER' AS THE NEW ADDRESS. FILE THIS LETTER IN THE FILE JACKET. WHEN ABOVE CHANGES ARE ONLY TO FEE ADDRESS AND/OR PRACTITIONERS OF RECORD, FILE LETTER IN THE FILE JACKET.
THIS FILE IS ASSIGNED TO GAU 3621.

AF/2700

PATENT #10

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on April 12, 2002.

Angela M. Beddawi

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	2161
Examiner	:	P. Elisca
Docket No.	:	34503/WWM/A522

NOTICE OF APPEAL FROM THE PRIMARY EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Assistant Commissioner for Patents
Washington, D.C. 20231

Post Office Box 7068
Pasadena, CA 91109-7068
April 12, 2002

Commissioner:

Applicant hereby appeals to the Board of Patent Appeals and Interferences from the Office action dated **October 12, 2001** of the Primary Examiner's final action of claims **1-29**.

_X_ A Petition for Extension of Time and the fee are enclosed.
_X_ Our check for $160 to cover the fee for this appeal is enclosed.
____ A Small Entity Claim is enclosed.
____ No fee is required for this Notice of Appeal because the fee was paid in a prior appeal.

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed**.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/amb

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PETITION FOR EXTENSION OF TIME
FROM THE OFFICE ACTION

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on April 12, 2002.

Angela M. Beddawi

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div	:	2161
Examiner	:	P. Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
April 12, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Office action dated **October 12, 2001** for **three** months from **January 12, 2002** to **April 12, 2002.**

The fee for extension of time required by 37 CFR § 1.17 is calculated below.

CALCULATION OF FEE			
LENGTH OF EXTENSION	SMALL ENTITY	LARGE ENTITY	FEE
WITHIN FIRST MONTH	$ 55	$110	$
WITHIN SECOND MONTH	$200	$400	$
WITHIN THIRD MONTH	$460	$920	$460
WITHIN FOURTH MONTH	$720	$1440	$
WITHIN FIFTH MONTH	$980	$1960	$

Submitted herewith is a check for $ **460** to cover the cost of the extension.

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed**.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/amb
AMB PAS428168.1-*-4/12/02 2:57 PM

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

6

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/295,966	04/21/99	IKUDOME	K 34503/WWM/A5

TM02/1012

CHRISTIE PARKER & HALE
P O BOX 7068
PASADENA CA 91109-7068

EXAMINER	
ELISCA, P	
ART UNIT	**PAPER NUMBER**
2161	9

DATE MAILED: 10/12/01

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

Commissioner of Patents and Trademarks

1- File Copy

6

Office Action Summary	Application No. **09/295,966**	Applicant(s) **Koichiro, Ikudome et al.**
	Examiner **Pierre E. Elisca**	Group Art Unit **2161**

☒ Responsive to communication(s) filed on *Aug 2, 2001*.

☒ This action is **FINAL.**

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

A shortened statutory period for response to this action is set to expire *THREE* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-29* is/are pending in the application.

Of the above, claim(s) *none* is/are withdrawn from consideration.

□ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-29* is/are rejected.

□ Claim(s) ______ is/are objected to.

□ Claims ______ are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The drawing(s) filed on ______ is/are objected to by the Examiner.

□ The proposed drawing correction, filed on ______ is □approved □disapproved.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______.

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______.

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

□ Interview Summary, PTO-413

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

--- *SEE OFFICE ACTION ON THE FOLLOWING PAGES* ---

Examiner Pierre Eddy Elisca

United States Department of Commerce

Patent and Trademark Office

Washington, D. C. 20231

DETAILED ACTION

Response to Amendment

1. This Office action is in response to Applicant's amendment filed on 8/20/2001.

2. Claims 1-29 are remained and claims 1, 8, 15, and 26 are amended.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-29 are rejected under 35 U.S.C. 102 (b) as being anticipated by Shiva Corp. Horowitz et al. (WO 96/05549).

As per claims 1, 8, 15, Horowitz discloses a system/method comprising:

a dial-up network server (or network server) that receives user IDs from user's computers (see., abstract);

a redirection server (a firewall or filter or gateway) to the dial-up network server, an authentication accounting server connected to the database, the dial-up network server and the redirection server (see., figs 1 and 2, col 3, lines 8-34, col 4, lines 1-34);

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server (see.,abstract, col 4, lines 23-34);
8

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the user ID and the temporarily assigned network address to the redirection server (see.,abstract, col 7, lines 1-34, col 9, lines 4-34); and
L/8

wherein data redirected toward the public network from the one of the users' computers are processed by the redirection server according to the individual rule set (see., **this limitation is disclosed by Horowitz, in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string, please note that the process of identifying the remote user is**

seen to read as the step of the users's computers rule set or portion of rule set, and the step of redirecting server is also disclosed in page 4, lines 6-18, specifically wherein it is stated that if the server locates an access filter for a remote user which indicates that the remote user should-not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network, also please note that the fact that the remote user will be able to communicate with other non-restricted parts of the network, thus the remote user in fact has been redirected toward another direction).

As per claims 2-6, 9-13, 16-29 Horowitz discloses the claimed limitation, wherein the redirection server (or filter) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (see., abstract, col 9, lines 13-34).

As per claims 7, 14, Horowitz discloses the claimed limitation, wherein the database entires for a plurality of the plurality of users's IDs are correlated with a common individualized rule set (see., abstract, col 8, lines 28-34, col 9, lines 24-34).

REMARKS

5. In response to claims 1-29, Applicant argues that the prior art of record (Horawitz et al) does not teach or suggest: " user ID for one of the users' computers and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individual rule set or rule set correlated to the temporarily assigned network address". However, these newly added limitations is also disclosed by Horowitz **in the abstract, specifically wherein it is stated that the server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string, please note that the process of identifying the remote user is seen to read as the step of the users's computers rule set or portion of rule set correlated to the temporarily assigned network address (network address or access filter associated with the string), and the step of redirecting server is also disclosed in page 4, lines 6-18, specifically wherein it is stated that if the server locates an access filter for a remote user which indicates that the remote user should-not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network, also please note that the fact that the remote user will be able**

to communicate with other non-restricted parts of the network, thus the remote user in fact has been redirected toward another direction).

Response to Arguments

6. Applicant's arguments filed 8/2/2001 have been fully considered but they are not persuasive.

CONCLUSION

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. The prior art made of record and relied upon is considered to applicant's disclosure.

1. WO 98/26548	Li et al.

This patent relates to an Internet access device uses an automatic configuration process to handle the task of configuring the Internet access device at a consumer site for communication with the Internet (see., abstract).

2. EP 0854621A1 Zenchelsky, Daniel N.

This patent teaches a system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier (see., abstract).

6. Any inquiry concerning this communication from the examiner should be directed to Pierre Eddy Elisca at (703) 305-3987. The examiner can normally be reached on Monday, Tuesday, and Wednesday from 5:30AM. to 6:00PM.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9769.

Any response to this action should be mailed to:

Commissioner of patents and Trademarks
Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

OR:

(703) 305-3718 (for informal or draft communications, pleased label

"PROPOSED" or" DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington. VA., Sixth floor (receptionist)

The Official Fax Numbers for TC-2100 are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Pierre Eddy Elisca

Patent Examiner

October 11, 2001

#8/A
ME
8-1-01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on July 30, 2001.

Signature

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	2161
Examiner	:	P. Elisca
Docket No.	:	34503/WWM/A522

AMENDMENT

Post Office Box 7068
Pasadena, CA 91109-7068
July 30, 2001

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

In response to the Office action of January 30, 2001, please amend the above-identified application as follows:

In the Claims:

Please amend claims 1, 8, 15 and 26 as follows:

1. (Amended) A system comprising:

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

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

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

19

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

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

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

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

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

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

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

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

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

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

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

a2

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

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

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

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

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

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

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

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

a

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

5 ~~15~~. (Amended) A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

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

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address. ; B1

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

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

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

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

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

a

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

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

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

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

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

A4 25 ~~26~~. (Amended) In a system comprising a redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; the method comprising the step of:

A5 B3 modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server ; B2

a

~~27. The method of claim 26, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user access.~~

~~28. The method of claim 26, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user access.~~

~~29. The method of claim 26, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of:.~~

~~receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.~~

REMARKS

Claims 1-29 are pending in this application. Claims 1-29 were rejected under § 102(b) as being anticipated by Shiva Corp. Horowitz et al. (WO 96/05549) (hereinafter "Horowitz").

The claims have been amended to more particularly define the invention originally claimed.

Returning to the rejection, it is noted that Horowitz involves a remote access server for allowing a user to dial up via modem and access a private local area network. Claims 1 and 8 have been amended to make it more clear that the claims are directed toward a system involving dial up network servers and redirection servers that are involved in the connection of a user to a public network, such as the Internet. The claimed system and the system of Horowitz perform various functions that are quite different from each other. For example, the filters used in Horowitz are based upon predetermined resources on the local computer network. In the context of a public network, however, the resources on the public

a

network are virtually limitless, constantly changing, and mostly unknown to firewalls, filters and similar systems. Thus, filtering based only on predetermined resources is not effective.

While not going into all of the patentably distinct features of the various dependent claims, as they all incorporate the clarifications contained herein in the independent claims, applicants would like to highlight some of these features. In particular, applicants do not see where Horowitz discloses redirection of data as a function of the individualized rule set as set forth in claims 5, 6, 12 and 13.

With respect to independent claims 15 and 26, applicants fail to discern a disclosure in Horowitz of allowing modification of a portion of a rule set as set forth in claim 15 and, particularly, allowing the automated modification of at least a portion of a rule set. Also, applicants fail to discern in Horowitz the disclosure of modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server, as set forth in claim 26. It is noted that the Office action fails to indicate where the disclosure of this feature may be found in Horowitz.

Accordingly, applicants respectfully submit the claims are now in condition for allowance and reconsideration of the Office action dated January 30, 2001 is respectfully requested.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "**Version with markings to show changes made**."

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/amb

a

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please amend claims 1, 8, 15 and 26 as follows:

1. (Amended) A system comprising:

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

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

a redirection server connected to the dial-up network server and a public network, and[~~;~~]

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

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

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

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

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

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

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

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

a

15. (Amended) A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

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

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

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

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server.

a

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
AMENDMENT TRANSMITTAL LETTER

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on July 30, 2001.

Signature

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	2766
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
July 30, 2001

Assistant Commissioner for Patents
Washington, D.C. 20231

Enclosed is an amendment to the above-identified application.

CLAIMS AS AMENDED

	Claims Remaining After Amendment	Highest Number Paid For	Number Extra Claims	Small Entity Rate	Large Entity Rate	FEE
Total Claims Fee	29	* 29		x $9.00	x $18.00	
Independent Claims	4	** 4		x $40.00	x $80.00	
Multiple Dependent Claims ***				$135.00	$270.00	
TOTAL FILING FEE						$
NO ADDITIONAL FEE REQUIRED ****	IF NO FEE REQUIRED, INSERT "0"					0
LIST INDEPENDENT CLAIMS: 1, 8, 15 and 26						

* IF HIGHEST NUMBER PREVIOUSLY PAID FOR IS 20 OR LESS, WRITE "20" IN COLUMN 3
** IF HIGHEST NUMBER PREVIOUSLY PAID FOR IS 3 OR LESS, WRITE "3" IN COLUMN 3
*** PAY THIS FEE ONLY WHEN MULTIPLE DEPENDENT CLAIMS ARE ADDED FOR THE FIRST TIME
**** IF NO FEE REQUIRED, ADDRESS ENVELOPE TO "BOX NON-FEE AMENDMENTS"

___ Attached is our check for $ to pay the fees calculated above.
_X_ A Petition for Extension of Time and the required fee are enclosed.
___ Other enclosures:

a

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by or to give effect to this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By

Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/mee

MEE PAS369191.1-*-7/30/01 3:58 PM

#7/Ext. 3
vE
8-11-01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PETITION FOR EXTENSION OF TIME FROM THE OFFICE ACTION

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on July 30, 2001.

Signature

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div	:	2766
Examiner	:	Pierre Eddy Elisca
Docket No.	:	34503/WWM/A522

Post Office Box 7068
Pasadena, CA 91109-7068
July 30, 2001

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

Applicant petitions the Commissioner to extend the time for response to the Office action dated **January 30, 2001** for **three** month(s) from **April 30, 2001** to **July 30, 2001**.

The fee for extension of time required by 37 CFR § 1.17 is calculated below.

CALCULATION OF FEE			
LENGTH OF EXTENSION	SMALL ENTITY	LARGE ENTITY	FEE
WITHIN FIRST MONTH	$ 55	$110	$
WITHIN SECOND MONTH	$195	$390	$
WITHIN THIRD MONTH	$445	$890	$445
WITHIN FOURTH MONTH	$695	$1390	$
WITHIN FIFTH MONTH	$945	$1890	$

Submitted herewith is a check for $ **445** to cover the cost of the extension.

The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed**.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/lll
LLL PAS369152.1-*-7/30/01 3:16 PM

NW

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/295,966	04/21/99	IKUDOME K	34503/WWM/A5

WM02/0130

CHRISTIE PARKER & HALE
P O BOX 7068
PASADENA CA 91109-7068

EXAMINER	
ELISCA,P	
ART UNIT	PAPER NUMBER
2161	6

DATE MAILED: 01/30/01

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

Commissioner of Patents and Trademarks

PTO-90C (Rev. 2/95)
*U.S. GPO: 2000-473-000/44602

1- File Copy

SM

Office Action Summary	Application No. 09/295,966	Applicant(s) Koichiro, Ikudome et al.	
	Examiner Pierre Eddy Elisca		Group Art Unit 2161

☒ Responsive to communication(s) filed on *Apr 21, 1999* .

☐ This action is **FINAL.**

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

A shortened statutory period for response to this action is set to expire *THREE* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-29* is/are pending in the application.

Of the above, claim(s) *none* is/are withdrawn from consideration.

☐ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-29* is/are rejected.

☐ Claim(s) ______ is/are objected to.

☐ Claims ______ are subject to restriction or election requirement.

Application Papers

☒ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on ______ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on ______ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) ______ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). *4 and 5*

☐ Interview Summary, PTO-413

☒ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Examiner Pierre Eddy Elisca

United States Department of Commerce

Patent and Trademark Office

Washington, D. C 20231

DETAILED ACTION

1. **This office action is in response to application serial number 09/295,966, filed on 04/21/1999 with a provisional application 60/084,014, filed on 05/04/1998.**

2. Claims 1-29 are presented for examination.

Claim Rejections - 35 USC § 102

3 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-29 are rejected under 35 U.S.C. 102 (b) as being anticipated by Shiva Corp. Horowitz et al. (WO 96/05549).

As per claims 1, 8, 15, Horowitz discloses a system/method comprising:

a dial-up network server (or network server) that receives user IDs from user's computers (see., abstract);

a redirection server (a firewall or filter or gateway) to the dial-up network server, an authentication accounting server connected to the database, the dial-up network server and the redirection server (see., figs 1 and 2, col 3, lines 8-34, col 4, lines 1-34);

wherein the dial-up network server communicates a first user ID and a temporarily assigned network address for the first user ID to the authentication accounting server (see.,abstract, col 4, lines 23-34); and

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the user ID and the temporarily assigned network address to the redirection server (see.,abstract, col 7, lines 1-34, col 9, lines 4-34).

As per claims 2-6, 9-13, 16-29Horowitz discloses the claimed limitation, wherein the redirection server (or filter) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (see., abstract, col 9, lines 13-34).

As per claims 7, 14, Horowitz discloses the claimed limitation, wherein the database entires for a plurality of the plurality of users's IDs are correlated with a common individualized rule set (see., abstract, col 8, lines 28-34, col 9, lines 24-34).

CONCLUSION

5. The prior art made of record and relied upon is considered to applicant's disclosure.

1. WO 98/26548 Li et al.

This patent relates to an Internet access device uses an automatic configuration process to handle the task of configuring the Internet access device at a consumer site for communication with the Internet (see., abstract).

2.EP 0854621A1 Zenchelsky, Daniel N.

This patent teaches a system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier (see., abstract)

6. Any inquiry concerning this communication from the examiner should be directed to Pierre Eddy Elisca at (703) 305-3987. The examiner can normally be reached on Monday, Tuesday, and Wednesday from 5:30AM. to 6:00PM.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9769.

Any response to this action should be mailed to:

Commissioner of patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

OR:

(703) 305-3718 (for informal or draft communications, pleased label

"PROPOSED" or" DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington. VA., Sixth floor (receptionist)

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Pierre Eddy Elisca

Patent Examiner

January 22, 2001

Notice of References Cited	Application No. 09/295,966	Applicant Koichiro, Ikudome et al.		
	Examiner Pierre Eddy Elisca		Group Art Unit 2161	Page 1 of 1

U.S. PATENT DOCUMENTS

		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS
	A					
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUBCLASS
	N	EP 0854621A1	7/1998	EP	Zenchelsky, Daniel N.	----	----
	O	WO9826548	6/1998	WO	Li et al.	----	----
	P	WO9605549	2/1996	WO	Horowitz et al.	----	
	Q						
	R						
	S						
	T						

NON-PATENT DOCUMENTS

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
	U		
	V		
	W		
	X		

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 29/06, G06F 9/445

A1

(11) International Publication Number: **WO 98/26548**

(43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/10600

(22) International Filing Date: 18 June 1997 (18.06.97)

(30) Priority Data:
08/762,737 10 December 1996 (10.12.96) US

(71) Applicant *(for all designated States except US)*: WHISTLE COMMUNICATIONS CORPORATION [US/US]; Suite 100, 110 Marsh Drive, Foster City, CA 94404 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LI, Jim, Y. [US/US]; 2946 Polk Street, San Francisco, CA 94117 (US). COBBS, Archie, L. [US/US]; 114 Frederick Street, #17, San Francisco, CA 94117 (US). OZZELLO, Paul, D. [US/US]; 990 Fulton, #506, San Francisco, CA 94117 (US).

(74) Agent: HICKMAN, Paul, L.; Hickman Beyer & Weaver, P.O. Box 61059, Palo Alto, CA 94306 (US).

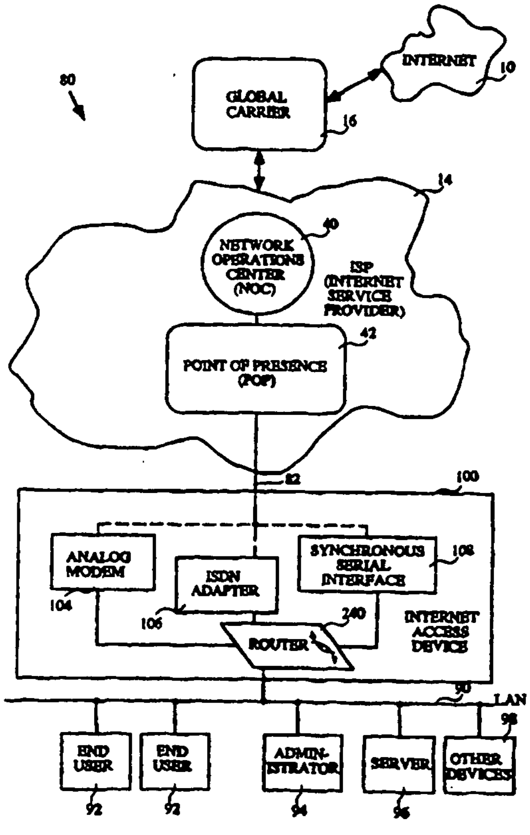
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AUTOMATIC CONFIGURATION FOR INTERNET ACCESS DEVICE

(57) Abstract

An Internet access device (100) uses an automatic configuration process (600) to handle the task of configuring the Internet access device at a customer site for communication with the Internet (10). Once configured, the customer has electronic mail and other access to the Internet from his local area network. A not yet configured Internet access device is shipped directly to a customer without having to be manually configured first. The customer enters a registration identification number (326) and a telephone number onto the Internet access device. The Internet access device then automatically connects to the Internet, downloads configuration data from a configuration server (410) containing customer site specific configuration data, and then automatically configures itself for communication with the Internet. The Internet access device is simple to install for a customer and provides valuable features such as a router (240), firewall, e-mail gateway (212), web server (220), and other servers (222). The Internet access device initially connects to the Internet through an Internet service provider (14) over a standard analog telephone line using a standard modem (52) and using a dynamic IP address. Once automatically configured, the Internet access device may then communicate with the Internet using any suitable connection including an analog telephone line, or a higher-speed line such as an ISDN line or a frame relay circuit and is assigned a static IP address and a range of IP addresses for other devices on its local area network.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

AUTOMATIC CONFIGURATION FOR INTERNET ACCESS DEVICE

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to PCT International Application No. _______________ (Attorney Docket No. WSTLP002.P), entitled "Automatic Setup Of Services For Computer System Users", filed on the same date herewith, which claims priority of U.S. Patent Application Serial No. 08/762,736 filed on December 10, 1996, both of which are incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computing systems and communications networks. More specifically, the present invention relates to automatically configuring a computing system for communication with a communications network.

BACKGROUND OF THE INVENTION

In recent years, the popularity of the Internet has been increasing dramatically. Every day, more and more home users, small business users and large corporations are connecting to the Internet to improve communication. The term "Internet" (upper-case "I") refers to that particular global communications network that is in use around the world and that grew out of a U.S. Department of Defense funded research project named the ARPANet. Currently, most of the Internet is commercially owned and is an extremely complex, highly redundant network of telecommunications circuits that are connected together with routers. The "Internet" refers to a particular network of communications networks, while, in general, any interconnection of networks may be termed an "internet" (lower-case "i"). The "Internet" is one example of an "internet". Currently, the Internet is used for a variety of services including communication, education, news, advertising, reference materials, broadcast like media, financial services, and other.

The Internet may be described in a very simplistic sense as follows. There are six major global telecommunications carriers each of which maintains a global telecommunications network. Examples of these global carriers are companies such as SPRINT or MCI. These global carriers have links between each of their networks to allow communication between the networks. Companies termed Internet service providers (ISPs) lease access to these global networks from one of the global carriers and provide this access to their customers such as businesses, universities and individuals. These ISPs maintain their own IP (Internet protocol) networks that are connected to the Internet. An IP network of an ISP allows an ISP to establish a presence in many different locations around the country, so that customers will have local dial-in access or a short leased-line access to the IP network. Once a customer gains access to the IP network, he or she has access to the Internet. In reality, a hierarchy of local access providers, network service providers, and network access providers provide a link from a customer to the Internet.

In general, it can be said that connecting a computer or computer network to the Internet is not a simple task. Many configuration variables must be taken into account including whether the computer is a single host at a home, or is part of a local area network (LAN) in a corporation, whether a customer desires a dynamic or static IP address, and what type of line connection the customer desires. In general, a customer connects to the Internet using either a dial-up telephone line, or a more permanent leased line connection. Most home or casual use customers connect to the Internet through a dial-up line using a modem, while corporate or heavy use customers often connect with a permanent leased line connection.

Another distinction between customers relates to the type of address on the Internet used by the customer. An IP (Internet protocol) address represents a communications end point. This may or may not correlate to a user. For example, time-sharing or multi-user systems have many users per address. Typically though, each end point will have a unique IP address (or IP number or "dotted quad"). Each IP address has four parts separated by dots, e.g., "101.100.2.2", and is a 32-bit number. A router that directs information to various end hosts has an IP address such as "101.100.2.1", where the last part will be a unique number identifying the end hosts that are attached to the router. For example, for three hosts connected to such a router, these hosts may have IP addresses of 101.100.2.2, 101.100.2.3, and 101.100.2.4.

A home or casual use customer who only dials up to connect to the Internet occasionally, may only need a dynamic or temporary address for that session only. This dynamic IP address is unique for that user for only a particular transaction. Once the user has disconnected from the Internet, the dynamic IP address may be reassigned to another user. However, providers of services or information on the Internet require a permanent or static IP address so that other users may access this information at any time using a known address. Corporate customers having a web site and a domain name may also require one or more static IP addresses. Another configuration variable is that customers may choose between a variety of types of connections to the Internet that are offered by an ISP. For example, a casual use customer may choose to use a modem on a dial-up line to access the Internet, or may choose to use an ISDN (integrated services digital network) adapter in order to access the Internet over a dial-up ISDN line. A corporate or heavy use customer may wish to utilize a permanent leased line connection to the Internet that uses frame relay technology for high-speed access.

Thus, there are complexities and difficulties involved with connecting a computer or LAN to the Internet and configuring the computer or LAN for communication with the Internet. One such difficulty is that routers both at the ISP and in the customer's computer must be configured correctly. At the ISP, a trained network operator is available for entering configuration information into the router such as the IP address of a customer, an account number, etc. Other configuration information that must be entered includes telephone numbers to dial, passwords, packet filter rules, LAN network information, domain name information, e-mail configuration, compression parameters, etc. Once this is done, however, the customer must be told of this information and then must manually enter this same information into his own networking hardware in order to configure a router, for example. This duplicity of entering information is tedious for the customer, and is prone to errors. Also, a configuration will be different depending upon whether a customer wishes to access the Internet using a modem, an ISDN line, a frame relay circuit, or other high-speed line.

Furthermore, connecting a LAN is considerably more difficult than connecting a single host as it requires the correct installation and configuration of a wide variety of interrelated systems. By way of example, routers, firewalls, DNS servers and DHCP servers, etc. must all be configured correctly before the LAN can successfully communicate with the Internet. Connecting a LAN is an all-or-nothing proposition. The minimum equipment necessary includes a firewall, router, and DNS server. Configuring this equipment correctly typically requires an IP networking engineer. This fact represents a significant obstacle to the wide adoption of Internet technologies, particularly amongst the majority of small business organizations. Internet service providers relying on the current state-of-the-art in networking equipment are unable to engage any customers but the technical elite.

Therefore, the automation of the setup of a full-service IP LAN network for communication with the Internet is desirable. It would further be desirable to have an Internet access device and configuration process for configuring a computer system to communicate with the Internet that is not prone to error and that is secure. It would be further desirable for this configuration process to be automatic, and for the configuration process to be able to use the existing infrastructure of the Internet in order to retrieve configuration data from any location. It would further be desirable if a customer need only perform a minimum of tasks and need only enter a minimum of information into such an

Internet access device in order for that device to be automatically configured for communication with the Internet.

SUMMARY OF THE INVENTION

To achieve the foregoing and other objects and in accordance with the purpose of the present invention, an Internet access device is disclosed that uses an automatic configuration process to handle the task of configuring the Internet access device at a customer site. This process allows a not yet configured Internet access device to be shipped directly to a customer without having to be manually configured first. In some embodiments, the customer simply enters a registration identification number and a telephone number onto the front panel of the Internet access device. The Internet access device then automatically connects to the Internet, downloads configuration data from a configuration server containing customer site specific configuration data, and then automatically configures itself for communication with the Internet.

In one embodiment, an Internet access device is a communications apparatus with at least two physical interfaces for connecting a LAN to the Internet over a wide area communications link. In addition to routing network data, an Internet access device may provide one or more related services to the LAN such as a domain name service, a DHCP service, security, electronic mail, etc.

In one embodiment, the Internet access device initially connects to the Internet through an Internet service provider over a standard analog telephone line using a modem that requires no configuration on the part of the customer. Once automatically configured, the Internet access device may then communicate with the Internet using either the analog line or a higher-speed line such as an ISDN line or a frame relay circuit.

In another embodiment, the Internet access device initially connects to the Internet acting as a single host computer, using a dynamic IP address as its address, requiring no configuration on the part of the user. Once automatically configured, the Internet access device may then act as a router, communicating with the Internet using a static IP address and a range of IP addresses for other devices on a local area network.

An Internet access device is as painless and simple to install for a customer as possible, while at the same time providing valuable features such as a router, firewall, e-mail gateway, web server, and other servers. The Internet access device is able to connect to a configuration server using the standard infrastructure of the Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 illustrates an embodiment of a global communications network including an Internet service provider.

FIG. 2 illustrates an embodiment of an IP network of an Internet service provider.

FIG. 3 illustrates an embodiment of a point of presence (POP) for an Internet service provider that has connections for various communications devices used by customers.

FIG. 4 illustrates an embodiment of an Internet access device that allows communication between the Internet and a local area network of a customer site.

FIG. 5 illustrates an embodiment of the hardware architecture of an Internet access device suitable for use in accordance with the present invention.

FIG. 6 illustrates an embodiment of the software architecture of the Internet access device illustrated in FIG. 5.

FIG. 7 illustrates an embodiment of a process by which a registration identification number is formed and then encrypted into decimal digits.

FIG. 8 illustrates how an Internet access device may connect to a configuration server on the Internet using a dynamic IP address.

FIG. 9 illustrates how an Internet access device may be permanently connected to the Internet using a static IP address.

FIG. 10 is a flowchart illustrating a method for automatically configuring an Internet access device for communication with the Internet in accordance with one embodiment of the present invention.

FIGS. 11A and 11B are flowcharts illustrating one method of accomplishing the automatic configuration process step of Figure 10.

FIG. 12 is a flowchart illustrating one method of accomplishing the Internet access device configuration step of Figure 11B.

DETAILED DESCRIPTION OF THE INVENTION

In general, there are at least four components to any internet and to the Internet in particular. These four components include server computers, client computers, networks and routers. These components communicate with each other mainly over leased lines provided by the global carriers. A server is any computer on which information is stored and from which other computers, called clients, can retrieve that information. A client computer is a computer used for accessing the Internet, retrieving information from server computers, entering data, and performing other data processing work. A client computer may be used for word processing, sending e-mail, retrieving information from the Internet, transferring files, and many other tasks. A network is any interconnection of computers using wires, switches, network adapters, etc., that allow these computers to communicate. A network may be a local area network (LAN), for example, or may be a wide area network (WAN). Networks are classified as LANs or as WANs depending upon their geographic reach. Networks are connected to each other via routers or gateways, forming internets.

Figure 1 shows a global communications internet 10 that in one embodiment is the Internet. The Internet has any number of Internet service providers (ISPs) 12 and 14 that connect a communication line 18 to a global carrier 16. Global carriers 16 and 22 may be one of the commercial Internet backbone providers such as SPRINT or MCI. Each global carrier has its own separate communications network 20. Communication lines 18 are typically T-1, T-3 or other high-speed lines. An ISP 14 may connect to a global carrier 16 through a hierarchy of providers. For example, ISP 14 may connect through a network service provider such as Netcom Online, UUNET or ANS, which in turn communicate via a network access provider such as the California Network Access Provider in order to communicate with the global carrier. Each of the global carriers may communicate with each other and with a vBNS 28 (very high speed Backbone Service) through a number of Network Access Points (NAP) 26 and communication lines 24. An ISP 14 includes IP networks 30 and 32 each having their own network of communication lines 34. The global carriers 16 and 22 control the physical portions of the Internet including the wires, fiber-optics and the switching equipment. The global carriers lease access to parts of their network to the ISPs, which in turn sell access to the Internet to their customers.

Figure 2 illustrates in greater detail an IP network 30 as shown in Figure 1. Typically, an Internet service provider offers local access to the Internet to its customers through such an extended IP network 30 that consists of perhaps hundreds of points of presence that are connected by high-speed dedicated lines that are leased from a telecommunications provider. The IP network 30 may be one of many IP networks that are managed by an Internet service provider. IP network 30 contains any number of points of presence (POPs) 42 that are interconnected with each other and to a network operation center (NOC) 40. The network operations center 40 contains hardware, software and systems for managing and monitoring the IP network 30.

IP network 30 connects over one or more high-speed lines 46 to a global carrier 16. Typically, each POP 42 is connected to another POP and eventually to the NOC via a high-speed leased line 44 using a T-1 or T-3 circuit. Each point of presence 42 has any number of feeder lines 48 that connect the POP to a customer 50. The Internet customer 50 may be one of a wide variety of Internet customers. By way of example, customer 50 may be a casual user dialing in from their home with a single computer, a corporate user, a single computer in a corporation, a router which is used to connect any number of other computers in a local area network to the Internet, a computer used for connecting a corporate intranet to the Internet, or other similar connection. Feeder lines 48 may be dial-up or leased lines, or other type. In general, the communication lines shown take a wide variety of forms. By way of example, lines may be traditional telephone copper wire pairs, a permanently installed wire, a cable system coaxial cable, fiber optic cable, a microwave or other electromagnetic transmission device, or other communication line.

Figure 3 illustrates an embodiment of a POP 42 as shown in Figure 2. POP 42 has a connection 44 to either another POP, a NOC of an IP network, or even directly to a global carrier. POP 42 also has feeder lines 48 for connecting to various Internet customers. The type of feeder line 48 may vary depending upon the service desired by the Internet customer. By way of example, a customer may connect to the POP using an analog modem 52 over a switched dial-up telephone line. This line may be a plain old telephone service (POTS) line at up to speeds of 56 Kbps. A customer may also connect to a POP using an ISDN adapter 54 that connects over a switched digital telephone line. A customer may also connect to a POP using a synchronous serial interface 56 utilizing a frame relay standard over a high-speed leased digital line such as a T-1 or T-3 line. Such a customer may be part of a large corporate site that uses a wide area router to communicate information to any number of users at the corporate site. Communication may also take place between a customer and the POP using existing cable television network lines. In this case, a customer may have a cable modem 58 for connecting to the POP. Other types of lines and hardware interfaces for connecting with a POP are possible.

A typical POP contains a distribution router 62 connected to a local area network 64 that distributes information among various servers and various hardware interfaces for outside communication to Internet customers. A wide variety of servers may be present within the POP. By way of example, the POP includes an e-mail server 66, a world wide web server 68 and other servers 70 such as a DNS server, news server, etc. By way of example, the distribution router 62 may take the form of a Cisco 7000 router available from

Cisco Systems, Inc.. A network access server (NAS) 72 is typically used for dial-up accounts. By way of example, the network access server 72 may take the form of a server made by US Robotics Communications or by Livingston Enterprises, Inc. An ISDN router 74 is used for communication over ISDN lines. By way of example, such devices are made by Ascend Communications, Inc. A leased line router 76 is typically used for high speed communications over a leased line using, for example, a frame relay circuit standard. By way of example, leased line routers are currently sold by Cisco Systems, Inc. A cable router 78 may be used to communicate over a cable television network.

Now having described an embodiment of the Internet, Figure 4 illustrates an arrangement 80 in which an Internet access device 100 facilitates communication between end users 92 and the Internet 10. Figures 4, 5, and 6 illustrate an embodiment of an Internet access device while Figures 7 through 12 show and describe a technique by which such an Internet access device may connect to and configure itself for communication with the Internet.

Internet access device 100 connects to a POP 42 of an Internet service provider 14 which in turn connects to a global carrier 16. In this fashion, access is provided to the Internet. In one embodiment, Internet access device 100 connects to a local area network (LAN) 90 at a customer site. By way of example, LAN 90 may take the form of an Ethernet LAN of a corporate or other customer. LAN 90 may connect end users 92, an administrator 94, a server 96, and any number of other devices 98. End users 92 may be a wide variety of users using a wide variety of computing devices. By way of example, end users 92 may use a single personal computer, a network computer, a laptop computer, a workstation, any type of super computer, or any other type of computer used by a user or operating on its own to request, gather, process, send or display information. The administrator 94 is typically a computer used by a system administrator or the like to monitor and administer the LAN 90. Server 96 may be any type of server such as an e-mail server, file server, or other server used for storing information which may be accessed by users on the LAN 90. Other devices 98 may include printers, routers, facsimile machines, gateways, etc.

Internet access device 100 includes an analog modem 104, an ISDN adapter 106, or a synchronous serial interface 108 that are all used to connect through communication line 82 to the POP 42. One or all of these interface devices may be present within the Internet access device 100, although typically only one is in use at a given time for communication with the Internet. Other types of interfaces devices may also be included. By way of example, it is expected that in the near future ADSL and other very high speed modems will be commercially available for use with POTS lines. It is contemplated that such modems can readily be incorporated in the described access device either in place of or in addition to a standard analog modem. Internet access device 100 also includes a router 240 for communicating between one of the interfaces 104, 106 or 108 and the LAN 90.

Figure 5 shows in greater detail an embodiment of the hardware architecture of the Internet access device 100 shown in Figure 4. Internet access device 100 includes a system bus 101 to which are connected various devices such as an analog modem 104, an ISDN adapter 106, a synchronous serial interface 108, an Ethernet LAN adapter 112, a power supply 114, a CPU 116, RAM 118, a hard disk drive 120, a keypad 122, an LCD display 124, and a speaker 126.

Typically, analog modem 104 is present in the Internet access device, while devices 106 and 108 may be present if the customer desires one of these types of connections to the Internet. Analog modem 104 may be any suitable analog modem used for communicating over an analog line. By way of example, analog modem 104 is a V.34 28.8 Kbps modem. ISDN adapter 106 may be any suitable ISDN adapter used for communicating over an ISDN line. Synchronous serial interface 108 may be any suitable device used for communicating via a high-speed serial port, and in one embodiment is arranged for communicating using a frame relay packet based interface standard. In one embodiment, Internet access device 100 acts as a frame relay access device (FRAD) when communication using frame relay technology is desired. It is contemplated that other communications interface devices such as 104, 106 and 108 may be used within the Internet access device 100 in order to communicate over a particular type of communication line and using a particular protocol.

LAN adapter 112 may be any suitable device for providing an interface between the Internet access device 100 and a LAN 90. By way of example, LAN adapter 112 may be based upon a LocalTalk or a token ring standard. In the embodiment shown,, LAN adapter 112 is for an Ethernet LAN with an integral 4-port 10BaseT hub, although of course, a wide variety of other LAN adapters may be used in conjunction with or alternately to the adapter shown. Internet access device 100 also includes a power supply 114 that includes a battery backup. CPU (central processing unit) 116 may be any suitable CPU and in the embodiment shown, is an Intel 80486 CPU. RAM 118 provides random access memory used to store temporary data such as routing tables, packet buffers, program storage, etc. for the Internet access device. Hard disk drive 120 may be any suitable hard disk, and in one embodiment is a 1.2GB IDE hard disk drive used for storing user information such as accounts, electronic mail, web pages, etc. Of course, it is expected that each of the described components may be upgraded as more powerful components become available and cost effective.

Keypad 122 may be any suitable keypad for entering numbers and information by a user to the Internet access device. By way of example, keypad 122 may take the form of an 18 key keypad including a numeric keypad similar to that found on a push button telephone, and other keys for inputting information to the Internet access device. LCD display 124 is provided for presenting information to the user, along with status lights indicating the status of the Internet access device. The status lights include information such as power, system activity, disk activity, LAN activity, and WAN activity. In the described embodiment, the LCD display 124 takes the form of a 128x 64 pixel LCD display, although other displays are possible. Speaker 126 is any suitable speaker for presenting audible information to a user.

Figure 6 illustrates an embodiment of the software architecture 200 of the Internet access device 100 of Figure 5. The software architecture 200 includes an operating system 210 that communicates with each of an e-mail server 212, an FTP daemon 214, a LAN Manager/AppleTalk file server 216, an automatic configuration engine 218, a web server 220, and other servers 222. These elements 212-222 are each in communication with a system administration module 228 that uses a graphical user interface.

Operating system 210 may be any suitable operating system. By way of example, in the described embodiment, operating system 210 is the BSD UNIX operating system. This operating system 210 includes an Ethernet driver 230, PPP (Point to Point Protocol) software 232, and a frame relay driver 234 in communication with an IP Routing/address translation module 240. Ethernet driver 230 communicates over line 231 to an Ethernet card. PPP software communicates over line 233 to either a modem or an ISDN adapter. Frame relay driver 234 communicates over line 235 to a synchronous serial interface card. The address translation module 234 allows for both host (1-N) and network (N-N) address translation. The module 240 is also in communication with a domain name server (DNS) and a dynamic host configuration protocol (DHCP) server 238 which supply appropriate connectivity protocols to the Internet. The IP routing may be performed by any suitable routing software used for receiving information over the Internet and routing it to the appropriate device on LAN 90. By way of example, a GateD router with support for OSPF, RIP and BGP routing protocols may be used.

E-mail server 212 provides e-mail service both internally to users of a LAN 90 of a company, and also externally to the world via the Internet. Every user on the LAN 90 is provided with their own unique e-mail address. FTP (file transfer protocol) daemon 214 is used for both internal and external file storage and transfer using industry standard Internet file transfer protocols. LAN Manager/AppleTalk file server 216 is a file server providing a central location by which users may exchange files. Automatic configuration engine 218 provides for the automatic configuration of the Internet access device 100 for communication with the Internet. An embodiment of how this automatic configuration engine configures the Internet access device will be discussed in more detail below with reference to the flow charts of Figures 10, 11 and 12.

Web server 220 may be any suitable web server for providing both internal and public web pages for not only a company, but also for each user on the LAN 90. In one embodiment, web server 220 is an Apache HTTP web server. Other servers 222 include such servers as directory servers, news servers, catalog servers, search engines, proxy servers, authentication servers, etc.

System administration module 228 provides a graphical user interface by which a system administrator and/or individual users may access the Internet access device in order to manage e-mail and web pages, perform system administration, allow access by individual users, and in general monitor and support the functioning of the Internet access device by users on the LAN 90. In one embodiment, system administration module 222 uses an HTML-based animated user interface for use with either Netscape NAVIGATOR or Microsoft INTERNET EXPLORER that allows all-in-one administration from any desktop and from any platform. System administration module 228 also provides for self-maintenance via an agent based metaphor, automated backups of any user data to any workstation on the LAN 90 or to the ISP, automated software management for software updates, and automated log and audit management. An aspect of system administration module 228 is disclosed in greater detail in U.S. Patent Application entitled "Automatic Setup Of Services For Computer System Users" referenced above.

Now that an embodiment of an Internet access device has been described, a method of advantageously using such a device will be described. The Internet access device is advantageous because, once installed at a customer site it is able to automatically connect itself to an appropriate location on the Internet, download configuration information and configure itself for a level of service desired by the customer. Figures 10, 11 and 12 illustrate one embodiment of a method of automatically configuring the Internet access device. Before the Internet access device configures itself, the customer and an Internet service provider communicate in order to determine an appropriate level of service for that customer and corresponding configuration information for the Internet access device. This interaction will now be described.

When a customer first determines that he or she desires a connection to the Internet the customer contacts an Internet service provider to request a particular level of service. This desired level of service includes many different variables. For example, the customer must first determine if they wish to connect a LAN to the ISP or simply a single machine to the ISP. Also, the type of connection must be determined. A customer may be connecting to the ISP over a dial-up line or over a permanent leased line. Also, the customer may desire an analog line using a conventional or high speed modem, an ISDN line using an ISDN adapter, or a leased line that may be a T-1 or a T-3 line using frame relay technology. Other types of lines and levels of service may also be specified by the customer. The customer may also determine a desired domain name, and a range of IP addresses that it requires. A customer with only a single host computer may need only a dynamic IP address, while a customer such as a corporation or provider of information may require not only a static IP address but also a range of addresses for various computers connected to a LAN. Other information from the customer may also be required by the ISP such as the number of users on the LAN, geographic location (used to determine which POP to connect to), anticipated storage needed for a web site, etc.

.Once the customer has specified his needs, the ISP assembles all of this customer information and inputs it into an ISP database. Some of this customer information comes from the customer itself (e.g., a desired domain name), while some information is generated by the ISP itself (e.g., the IP address block). Using the information in this database, the ISP is then able to generate a configuration file for future use by the customer. The configuration file contains all of the configuration needed by the customer to configure his Internet access device for the customer's desired level of service. Any suitable form and language for a configuration file may be used. By way of example, one such suitable configuration language for representing customer configuration information may be found in the Appendix.

If the configuration file is stored on the configuration server as a flat text file it is possible to create this file manually using any text editor. It is also possible that a configuration file may be automatically generated from the ISP customer database once all of the customer information has been entered, or the configuration file may be generated on the fly from the customer database when a request is made from an Internet access device to download a particular configuration file from a configuration server.

Once a configuration file has been generated, this configuration file is stored by the ISP onto a configuration server. In one embodiment, the configuration file is stored as a configuration record of a database on a dedicated configuration server. This configuration server may be located on an IP network within the ISP itself, or the configuration server may be located at any appropriate location on the Internet that is accessible by an address. In other embodiments, the configuration server may be located outside of the Internet or an internet, in a location that is accessible by a customer desiring access to a configuration file.

A more detailed description of the types of information contained within this configuration file is explained below with reference to Figure 12. Once the ISP has determined an IP address for the configuration server that holds the customer's configuration file, the ISP generates a registration identification number for that customer. Generation of this registration identification number will now be explained in more detail with reference to Figure 7.

Figure 7 illustrates a method 300 by which a registration identification number (registration ID) may be generated. Initially, a registration ID 302 includes a 32-bit IP address 304 for the configuration server on which the customer's configuration record resides, a 32-bit account identifier (account ID) 306, and an 8-bit check sum 308. The 32-bit IP address 304 uniquely identifies the configuration server on the Internet. The 32-bit account ID 306 is an arbitrary 32-bit number that uniquely identifies the Internet access device for a particular customer. This account ID 306 will be used to access that customer's unique configuration record on the configuration server identified by the IP address 304. The 8-bit check sum 308 is used for detecting erroneous customer keypad entries on the Internet access device. Without the check sum 308, the Internet access device would have to dial-up and connect to the configuration server before being able to alert the customer that an entered registration ID was invalid.

Next, a series of six "0" bits 314 are concatenated onto the registration ID 302 to produce a registration ID 312. Of course, the size of the various fields may be widely varied and additional or alternative fields may be used as well. After the registration ID has been concatenated, it is encrypted to produce an encrypted registration ID. In the described embodiment,, the 78-bit registration ID 312 is encrypted to produce a new 78-bit encrypted registration ID 318. As will be appreciated by one of skill in the art, any suitable encryption technique may be used. Next, the encrypted registration ID 312 is divided into groups of multi-digit numbers to create a decimal digit registration ID 326. When a 78-bit encrypted registration ID is used, the encrypted 78 bits are divided into groups of 13 bits each as shown at 322. Finally, each group of 13 bits is transformed into its corresponding four digit decimal numeral resulting in a 24 decimal digit registration ID 326. It is this registration ID 326 which is delivered to the customer from the ISP. Thus, the registration ID 326 contains information allowing a customer to access a configuration server on the Internet and to download a specific configuration file unique to that customer's requirements.

Once the registration ID has been generated, the ISP then ships to the customer an Internet access device, the registration ID, and a telephone number for accessing the ISP. Typically, this telephone number is a local telephone number or a toll-free "800" telephone number that the customer may use to dial into a network access server 72 of a local point of presence 42 for that Internet service provider. However, this telephone number may be any suitable number that allows the customer to gain access to the Internet and thereby begin the process of retrieving its configuration file from the configuration server. Once the customer receives the Internet access device, the registration ID and the telephone number, the customer is then able to install the Internet access device, connect it to his computer system or LAN and begin the process of automatic configuration. This process of automatic configuration will be discussed in more detail below with reference to the flow charts of Figures 10, 11 and 12, and with reference to the illustrations of Figures 8 and 9.

Figure 8 shows an arrangement 400 in which an Internet access device 100 is connected to a local point of presence 42 through a network access server. In this arrangement, Internet access device 100 has connected to the POP 42 using a dynamic IP address of "200.100.1.1" (for example) and has requested access to configuration server 410 which contains a database 420 of customer configuration records. Figure 8 will be discussed in greater detail below with reference to steps 714 through step 724 of Figure 11.

Figure 9 illustrates an arrangement 500 in which an Internet access device 100 has downloaded its configuration record, has automatically configured itself, and is now connected to the Internet at its desired level of service. Figure 9 shows an Internet access device 100 that is connected to a leased line router 76 of a local POP 42 using a leased line and frame relay technology. Through this line the Internet access device now has access to the Internet 10 through communications line 46. The Internet access device 100, already having been configured, routes to the LAN having (for example) address 207.76.205.X (where "X" represents one of a range of IP addresses, such as from "2" to "5"), and has a LAN 90 with attached computers 99 having IP addresses of 207.76.205.2, 207.76.205.3, 207.76.205.4 and 207.76.205.5. The Internet access device itself occupies an address at 207.76.205.1. It should be noted that these addresses are for example only. Each customer will receive a globally unique range of addresses. Figure 9 will be discussed in greater detail below with reference to Figure 12.

Once a customer has received a registration ID and a local telephone number from the ISP, the customer may begin the automatic configuration process for the Internet access device. Figure 10 is a flowchart showing the overall automatic configuration steps 600. As preparation, the customer first installs the Internet access device by supplying power, connecting the Internet access device to a telephone line and to the customer's computer system or LAN.

In step 602 the customer enters the encrypted registration ID supplied by the ISP onto the Internet access device 100 by way of keypad 122. Next, in step 604 the user enters the local telephone number of a network access server located on the ISP's network. This number may be the number of a local point of presence (POP) for the Internet service provider. This telephone number is a number for a basic analog dial-up telephone line by which the Internet access device may dial into and connect with a corresponding modem of the network access server of the ISP. In this fashion, the Internet access device may connect to the ISP (and to the Internet) with a minimum of configuration. During this phase, the Internet access device emulates a simple single address host. This allows it to utilize existing configuration protocols such as LCP and IPCP to gain an initial temporary connection. This is a "bootstrapping" technique in which a simple mechanism is employed to load and initiate a more complex one. The Internet access device comes ready to connect to an ISP over a standard dial-up analog telephone line (i.e. a POTS line); the customer is not required to perform any setup, configuration or entering of information in order to access the ISP.

In step 606 the user inputs a start command using keypad 122. In step 608 the Internet access device determines whether the entered registration ID is valid by using the 8-bit check sum. If the registration ID is not valid then in step 610 the Internet access device provides error feedback by way of the LCD display 124. If the registration ID is valid, then in step 612 the Internet access device begins execution of an automatic configuration process which will configure the Internet access device for communication with the Internet at a customer desired level of service. For example, the Internet access device will be configured for using an ISDN line or a frame relay circuit, and may be configured with a static IP address and a range of IP addresses for use by various computers connected to the Internet access device. This type of configuration typically requires extensive manual effort on the part of the customer at the customer site; the present invention is advantageous because it performs this type of configuration automatically. Step 612 will be explained in greater detail below with reference to Figure 11.

If automatic configuration has been successful, then in step 614 the program ends. However, if automatic configuration was not successful, then in step 610 error feedback related to this condition is provided to the user and control returns to step 602 where the user is able to enter the registration ID and telephone number once again. In step 614 the automatic configuration process may fail due to a problem with the modem, a hardware failure, an incorrect configuration server IP address, an incorrect account ID for the user, or other error.

Figures 11A and 11B illustrate in greater detail one method suitable for carrying out the automatic configuration process step 612 of Figure 10. This step allows the Internet access device to automatically dial into an Internet service provider without any configuration needing to be performed by the user. Once connected to an ISP, the Internet access device is then able to automatically locate a configuration server, request a unique configuration record for that Internet access device, download that configuration record, and then automatically configure itself for communication with the Internet using the configuration record.

In step 702 the analog modem 104 of Internet access device 100 automatically dials the local telephone number provided by the ISP and entered by the customer to contact a network access server (NAS) 72 of a local point of presence 42 of the ISP. This connection is made over a basic analog, dial-up telephone line that is straightforward to use and requires no configuration or input from the user of the Internet access device. Step 704 determines whether a successful connection has been made from the Internet access device to the network access server of the ISP. If no connection was made, then control returns to step 702 and the NAS is dialed again, unless in step 706 it is determined that the redial count has already been exceeded, in which case control moves to step 708. In step 708 the Internet access device displays an error message, terminates the calling procedure and then returns to step 614 of Figure 10 with a negative result.

If the connection is successful, then in step 710 a Point to Point Protocol (PPP) connection is established between the Internet access device and the NAS of the ISP. Establishing a PPP connection is known to those of skill in the art and involves password negotiations, exchange of addresses, and other standard handshaking. If this PPP connection is not successful, then step 712 moves control to step 708, an error message is displayed, and a negative result is returned to step 614 of Figure 10. Reasons why a connection may not be successful include an invalid password used by the Internet access device, an incorrect telephone number, malfunctioning equipment, busy signal, or other.

If the connection is successful, then in step 714 the registration ID entered by the user is decoded into an IP address of the configuration server and a customer account ID. It should be appreciated that an encoded registration ID may be decoded into its various parts in a wide variety of fashions. By way of example, a registration ID may be decoded with reference to Figure 7 in a reverse fashion to the procedure previously described for encoding a registration ID. First, a 24 decimal digit registration ID 326 is divided up into six groups of four digit decimal numbers and then each four digit numeral is transformed into its representative 13 binary digits to form a registration ID 322. These six groups of 13 bits each form a registration ID 318 of 78 bits. Next, the 78-bit encrypted registration ID 318 is decrypted to form a 78-bit registration ID 312. The first 32 bits are the IP address of the configuration server 304, the second 32 bits are a unique customer account ID 306, the next 8 bits are a check sum, and the last six bits are all zeros.

Using the decoded IP address 304 of the configuration server, in step 716 a connection is opened to this configuration server via the network access server over the Internet. Any standard technique may be used to open a connection to a configuration server located on the Internet using its IP address. By way of example, an HTTP protocol may be used, although it is contemplated that an LDAP (light weight directory access protocol) may also be used. Figure 8 illustrates a connection from an Internet access device 100 to a network access server of a POP 42 of an ISP, which in turn is connected to a configuration server 410. The Internet access device has connected to the ISP using a dynamic IP address of "200.100.1.1". Connecting in this fashion using an analog modem and a dynamic IP address is a simpler technique and requires no configuration of the Internet access device on the part of the customer. In the embodiment shown, the configuration server 410 is located within the Internet service provider, although the configuration server may be present at any location on the Internet and accessed via its IP address.

If this connection is not successful, then in step 708 an appropriate error message is displayed, the call is terminated, and a negative result is returned to step 614 of Figure 10. In step 718 a connection may be unsuccessful because of an incorrect registration ID, an incorrect configuration server, trouble on the Internet, the configuration server being down, or other communications difficulties. However, if the connection is successful, then step 718 transfers control to step 720 of Figure 11B.

In step 720 the Internet access device asks the configuration server 410 for the configuration record stored in database 420 that is identified by the customer account ID. This is typically done using an HTTP "get" request. The configuration record may be stored in a database 420 using a wide variety of techniques. By way of example, a configuration record may be stored in any typical database. In other embodiments, the configuration record takes the form of a configuration file on the configuration server. For example, a configuration file may be stored as a flat text file in a directory on the configuration server 410. In a second embodiment, the URL requested from the server resolves to a CGI (Common Gateway Interface) script, which takes the registration ID as extra path information. This extra path information is passed to the CGI script which then accesses the ISP database as required and outputs the configuration file corresponding to the customer account ID. In this second embodiment, the "get" request also sends two field values to be stored on the server, namely the Internet access device's Ethernet address, and the registration ID.

If the configuration record does not exist, then in step 734 an appropriate error message is displayed, the call is terminated, and a negative result is returned to step 614 of Figure 10. A record may not exist due to an incorrect customer account ID, an unknown customer account ID, a record not being present, or other discrepancy or problem with the database.

If however, the record does exist, then in step 724 this configuration record is downloaded from the configuration server 410 via the Internet and the ISP to the Internet access device 100 at its temporary IP address. Figure 8 illustrates a database 420 containing a configuration record that may be downloaded to the Internet access device in this fashion. This configuration record may store the configuration information needed by the Internet access device in any suitable format. By way of example, a configuration language such as may be found in the Appendix may be used. Next, in step 726 the Internet access device automatically configures itself using the information from the configuration record. This step will be explained in greater detail below with reference to Figure 12.

If the configuration is unsuccessful, then in step 734 an appropriate error message is displayed, the call is terminated, and a negative result is returned to step 614 of Figure 10. If the configuration was successful, then in step 730 the call is terminated and in step 732 a "configuration successful" message is displayed to the user, a positive result is returned to step 614 of Figure 10 and the procedure ends. Once the Internet access device has been successfully configured, the customer is then able to communicate with the Internet using a more complex, or higher speed method such as an ISDN line or a frame relay circuit. The IP routing configuration is then performed, followed by the configuration of various network services such as electronic mail and a web publishing. This configuration has occurred automatically, without intervention on the part of the customer.

Figure 12 describes in more detail the configuration step 726 of Figure 11B. Before Figure 12 is described in detail, the types of information that may be present in the configuration record are first described. The Internet access device is able to automatically configure itself for communication with the Internet using information contained in the configuration record. The configuration record contains information such as the customer domain name, the customer LAN network IP address, the Internet access device IP address, the DHCP range, time zone and NTP servers for time configuration, IP addresses for forwarding name servers, PPP account log in and password information, web mirroring configuration information, and mail configuration information. Other information may be added to the configuration record such as IP multicast router information, secondary DNS server information, etc.

It should be appreciated that the configuration record may contain any other information needed by the Internet access device to automatically configure itself for communication with a wide variety of communication lines in order to connect to the Internet. In this fashion, a customer is not required to manually enter information into the Internet access device at the customer site, nor is the customer required to modify or configure the Internet access device in any way. Configuration occurs automatically once a registration ID and a telephone number have been entered into the Internet access device. This allows for a very quick, simple, and error-proof configuration process. In addition, if the customer seeks a different configuration, or desires a different level of service in order to connect using a different type of communication line, this automatic configuration process may be invoked by the customer at any time in order to automatically download a new configuration file in order to configure their Internet access device again.

A wide variety of configuration information is contained within the configuration record. By way of example, the configuration record contains link information related to the actual hardware that will connect the Internet access device to the ISP. There is also IP network information that relates to Internet protocols, and DNS naming information relating to the process of using the Internet. Additional application information relates to configuration data that allows optional software applications to be configured correctly on the Internet access device. Examples of specific types of information for each of these categories will now be given. Further examples of information available in a configuration record may be found in the Appendix.

The link information includes configuration parameters related to a particular type of line service desired by a customer in addition to PPP link layer information. For example, if a customer desires a connection over a dial-up line using a modem, then POTS parameters (plain old telephone service) are supplied. These parameters include a local telephone number for the ISP, speaker on, dial-on-demand, idle time-out, permissible connect hours, etc. Alternatively, if the customer desires an ISDN line, then additional parameters are supplied. These parameters include a dial-up telephone number, a directory number for the customer, an SPID (service profile identifier), an ISP telephone number, a switch type, etc. A reference of ISDN connection parameters may be found in the document "NI-1 Standard" available from ANSI or ITU. On the other hand, if a frame relay circuit is desired, then parameters supplied in the configuration record would include DLCI (data link communication interface) information, LMI (link management interface) information, etc. Other parameters useful for configuring a frame relay connection may be found in the reference "UNI Specification", available from Frame Relay Forum. In addition to either of the sets of link parameters for a desired service specified above, the configuration record also includes PPP link layer information such as a login id, a password, authentication method, compression type, etc.

The configuration record also includes configuration information related to the IP network of the Internet service provider. This information includes an IP network address and an IP network mask. Also, an address translation parameter indicates whether the Internet access device will appear to the ISP as a single user or as multiple users on a LAN. A remote host parameter sets an IP address for the remote end of the link, such as a router at an ISP. A set of DHCP parameters allow other computers on a LAN attached to the Internet access device to be configured either with dynamic IP addresses, or with static IP addresses that are used for such servers as web servers, e-mail servers, printers, etc.. Other parameters useful for IP network configuration are routing protocols desired (e.g. BGP,. RIP), etc. The configuration record also includes information relating to DNS naming protocols. These parameters include domain name, list of DNS forwarders, etc.

The configuration record also includes application configuration information that allows various applications and services to be automatically configured. Time service parameters such as time zone, NTP servers, current GMT time, etc. allow the Internet access device to retrieve an accurate time over the Internet. Web mirroring service parameters allow the contents of the web site on the Internet access device to be automatically copied up to a location on the ISP for faster access by outside users. E-mail service parameters direct the Internet access device on where and how to connect for e-mail over the Internet. Upgrade service parameters allow the Internet access device to automatically receive software upgrades over the Internet. Backup services parameters allow the Internet access device to backup files to a secure location located on the Internet.

The configuration record may also include parameters related to a wide variety of other types of services. By way of example, parameters for configuring an electronic news service, an electronic banking service, an authentication service, or other services may also be included in the configuration record. In general, the configuration record may contain any parameters relating to a desired service that may be downloaded to configure the Internet access device automatically to enable it to use that service.

The flowchart of Figure 12 demonstrates one possible embodiment by which the information in the configuration record may be used to automatically configure the Internet access device. In step 802 the link information is used to configure either the analog modem, the ISDN adapter, or the synchronous serial interface, depending upon which level of service the user has chosen. In step 804 the PPP information is used to configure the Internet access device for Point to Point Protocol. In step 806 the IP router 240 of the Internet access device is configured using the IP network information. In step 808 the domain name server 236 is configured using the DNS naming information. In step 810 the DHCP server is configured using the IP network information. In step 812 the time server is configured using the appropriate time application information.

In step 814 any subscriber information from the configuration record is stored to the hard disk drive 120. In step 816 the mail server is configured using appropriate mail service parameters. Next in step 818, any other additional applications that are present are configured using the appropriate application information from the configuration record.

Once the above devices have been configured, then the Internet access device is ready to be enabled.

In step 820 the router 240, the domain name server 236, and the DHCP server 238 are enabled. Next, in step 822 the analog modem 104, the ISDN adapter 106, the synchronous serial interface 108, and the PPP connection 232 are all enabled. In step 824 the mail, web, time and other additional servers are all enabled. Finally customer information and a confirmation of enablement are sent to the ISP. After this step, the automatic configuration process is over.

Embodiments of the present invention as described above employs various process steps involving data stored in computer systems. These steps are those requiring physical manipulation of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It is sometimes convenient, principally for reasons of common usage, to refer to these signals as bits, values, elements, variables, characters, data structures, or the like. It should be remembered, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

Further, the manipulations performed are often referred to in terms such as identifying, running, or comparing. In any of the operations described herein that form part of the present invention these operations are machine operations. Useful machines for performing the operations of embodiments of the present invention include general purpose digital computers or other similar devices. In all cases, there should be borne in mind the distinction between the method of operations in operating a computer and the method of computation itself. Embodiments of the present invention relate to method steps for operating a computer in processing electrical or other physical signals to generate other desired physical signals.

Embodiments of the present invention also relate to an apparatus for performing these operations. This apparatus may be specially constructed for the required purposes, or it may be a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. The processes presented herein are not inherently related to any particular computer or other apparatus. In particular, various general purpose machines may be used with programs written in accordance with the teachings herein, or it may be more convenient to construct a more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given above.

In addition, embodiments of the present invention further relate to computer readable media that include program instructions for performing various computer-implemented operations. The media and program instructions may be those specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts. Examples of computer-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM) and random access memory (RAM). Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Examples of input/output devices usable by the present invention include those described above as well as video monitors, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, or other well-known input devices such as, of course, other computers.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, the present invention is useful not only in the context of the Internet, but also with any type of internet or network. Also, in addition to the specific types of communications lines and protocols described, the present invention would be useful in configuring other lines as well. The present invention is advantageous for configuring a single host site, as well as local or wide area networks. In addition, the initial accessing and retrieval of configuration information from a configuration record may be performed by a device separate from the Internet access device which is finally configured for communication. Also, the configuration server may be located on the Internet, an internet, at the ISP, or in an isolated location that is not connected to the Internet. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein but should be defined by the following claims and their full scope of equivalents.

APPENDIX

1. Language Overview and Example

```
# Set the domain name and forwarding DNS servers
  domain "customer.isp.com";
   forwarders 207.76.204.2 207.76.204.9;
  enable host-addr-xlate;

  time-zone "America/Los_Angeles";
  ntp-servers "tick.usno.navy.mil" "tock.usno.navy.mil";

# Configure customer's modem port for PPP dialup
# Enable dial-on-demand with a 20 minute timeout
  port "Mod0"
  {
     type modem
     {
           telno "456-7890";
           ppp
           {
              login "ppp-login";
              password "ppp-password";
           };
           dial-on-demand  {      timeout 1200;  };      };  };

# Customer uses a fake IP address with host address translation
# They also want to turn on DHCP from 192.168.1.100 -- 192.168.1.200
  local network "client"
  {
     address 192.168.1.0/24;
     enable dhcp;
     dhcp min-host 100;
     dhcp max-host 200;
  };

# Set IP addresses on customer WAN network (uses modem port)
  local network "wan"
  {
     port "Mod0";
     address 207.76.204.65/0;
     remote host 207.76.204.4;
  };
 web-mirror
  {
     server "webfarm1.isp.com";
     login "cust-login";
     password "cust-password";
     path "/customer/webdocs";
     enable update "05:00";
  };
  {
     enable finger "m38742@mailserv.isp.com";
     check-interval "1:00";
     disable stay-connected;
  };
```

2. Top Level Commands

```
domain "domain-name" ;
forwarders [ ip-address ... ] ;
workgroup "workgroup-name" ;
[ enable | disable ] host-addr-xlate ;
gateway network "network-name" host host-number ;
port "port-name" { port-commands };
[ local | remote ] network "network-name" { network-commands };
machine "machine-name" { machine-commands };
ref "machine-name" ip-address { ref-commands };
time-zone "zone-name" ;
ntp-servers [ "server-name" ... ] ;
current-time-gmt [ "date-string" | seconds ] ;
web-mirror { mirror-commands };
mail-config { mail-commands };
organization { org-commands };
upgrade { upgrade-commands };
isp-agent { isp-agent-commands };
```

3. Port Commands

```
description "string" ;
interface "if-name" ;
device "dev-name" ;
external [ yes | true | no | false ] ;
enabled [ yes | true | no | false ] ;
type [ ethernet | loopback | modem | raw-sync | frame-relay | cisco-hdlc | isdn-bri ]
{ port-type-commands } ;
```

4. Port Type Commands

```
lmi-type [ ansi | itu | group-of-four ] ;
telephone "number" ;
prefix "number" ;
port-speed value ;
speaker [ on | off ] ;
bitrate value ;
dial-on-demand { dod-commands } ;
idle-timeout value ;
ppp { ppp-commands } ;
login "string" ;
password "string" ;
[ enable | disable ] proxy-arp ;
[ enable | disable ] ppp ;
```

5. Network Commands

```
description "string" ;
address ip-address/width ;
```

For point-to-point networks, the address is the address of the local end of the link and the width MUST be zero. Otherwise, the host part of the address (as determined by the netmask width) MUST be zero. If the width is omitted, the natural class A, B, or C width is assumed.

For PPP links, the address is used as a starting point for IPCP negotiation; if negotiated differenly, this address will be overridden. If the address is 255.255.255.255, then PPP will use the IP address of the Internet access device on the LAN network as a starting point.

```
remote host ip-address ;
[ enable | disable ] dhcp ;
dhcp min-host host-number ;
dhcp max-host host-number ;
dhcp max-lease value-in-seconds ;
dhcp default-lease value-in-seconds ;
dlci value ;
```

6. Machine Commands

```
description "string" ;
hardware [ ether-address ... ] ;
names [ "dns-name" ... ] ;
```

7. Reference Commands

```
start [ "date-string"     | seconds ] ;
expiry [ "date-string"  | seconds ] ;
timestamp [ "date-string"       | seconds ] ;
unconfirmed [ yes | true | no | false ] ;
names [ "dns-name" ... ] ;
```

8. Web Mirroring Commands

```
server          "host-or-ip" ;
login           "string" ;
password        "string" ;
path            "directory" ;
[ enable | disable ] update   [ "time" ] ;
```

9. Mail Configuration Commands

```
[ enable | disable ] stay-connected   [ minutes ] ;
[ enable | disable ] finger   [ "account" ] ;
check-interval   [ "time" ] ;
```

10. Organization Commands

```
name          “string” ;
email         “string” ;
address       “string” ;
city          “string” ;
state         “string” ;
zip           “string” ;
country       “string” ;
telno         “string” ;
fax           “string” ;
note          “string” ;
```

11. Upgrade Commands

```
server        “string” ;
path          “string” ;
```

12. ISP Agent Commands

```
name          “string” ;
account-url   “string” ;
support-url   “string” ;
```

13. Special Names

```
port "Eth0"
port "Mod0"
port "Loop"
network "client"
machine "wg"
```

We Claim:

1. A computer-implemented method of automatically configuring an access device for communication with a communications network, said access device being associated with a customer account identifier said method comprising the steps of:

connecting said access device with a configuration server over a communications line;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device;

downloading said configuration record from said configuration server to said access device; and

configuring said access device for communication with said communications network using said configuration information of said configuration record.

2. A method as recited in claim 1 wherein said configuration server is located within a point of presence of an Internet service provider.

3. A method as recited in any of claims 1 or 2 wherein said step of configuring said access device includes the sub-steps of:

configuring one selected from the group of a modem, an ISDN adapter, and a synchronous serial interface; and

configuring a router of said access device.

4. A method as recited in any of claims 1, 2 or 3 wherein said access device is connected to a local area network (LAN) and said step of configuring said access device includes the sub-step of configuring said LAN for communication with said communications network.

5. A computer-implemented method of automatically configuring an access device for communication with a communications network, said access device being associated with a customer account identifier said method comprising the steps of:

accessing said communications network using said access device;

connecting said access device with a configuration server located on said communications network;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device;

downloading said configuration record from said configuration server to said access device; and

configuring said access device for communication with said communications network using said configuration information of said configuration record.

6. A method as recited in claim 5 wherein said step of accessing said communications network is performed by way of an Internet service provider and said communications network includes the Internet.

7. A method as recited in any of claims 5 or 6 wherein said access device connects to a local area network (LAN) and said step of configuring said access device includes the sub-steps of:

assigning a static address to a router included in said access device; and

assigning a static address to each of a plurality of end hosts present on said LAN.

8. A method as recited in any of claims 5, 6 or 7 wherein said step of accessing said communications network is performed using a modem over an analog communications line.

9. A method as recited in any of claims 5, 6, 7 or 8 wherein said step of configuring said access device configures said access device for communication over a line selected from the group consisting of a high-speed leased telephone line and a digital communications line.

10. A method as recited in any of claims 5, 6, 7, 8 or 9 wherein said access device is assigned a temporary dynamic address during said step of accessing said communications network.

11. A method as recited in any of claims 5, 6, 7, 8, 9 or 10 wherein said step of configuring said access device assigns a static address to said access device.

12. A method as recited in any of claims 5, 6, 7, 8, 9, 10 or 11 further including the step of receiving said customer account identifier and an identifying address by said access

device, said identifying address being arranged to identify said configuration server on said communications network.

13. A method as recited in any of claims 5, 6, 7, 8, 9, 10, 11 or 12 further including the step of receiving a telephone number for accessing a service provider of said communications network and wherein the telephone number is utilized by the access device to automatically access the communications network.

14. A method as recited in claim 12 wherein said customer account identifier and said identifying address are received by said access device in a concatenated and encrypted form via an input means of said access device.

15. A method as recited in any of claims 5, 6, 7, 8, 9, 10, 11, 12, 13 or 14 wherein said access device is connected to a local area network (LAN) and said step of configuring said access device includes the sub-step of configuring said LAN for communication with said communications network.

16. A computer-implemented method of automatically configuring an access device for use as a router in a communications network, said access device being associated with a unique customer account identifier, said method comprising the steps of:

accessing said communications network using said access device using a temporary dynamic address for said access device;

connecting said access device with a configuration server located on said communications network;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device, said configuration information including a static address for said access device;

downloading said configuration record from said configuration server to said access device at said temporary dynamic address; and

configuring said access device for communication with said communications network using said configuration information of said configuration record, including assigning said static address to said access device.

17. A method as recited in claim 16 wherein said step of accessing said communications network is performed using a modem over an analog communications line.

18. A method as recited in any of claims 16 or 17 wherein said step of configuring said access device configures said access device for communication over a line selected from the group consisting of an analog communication line, a high-speed leased telephone line and a digital communications line.

19. A method as recited in any of claims 16, 17 or 18 further including the step of receiving by said access device a registration identification number that includes said customer account identifier and an identifying address for said configuration server.

20. A method as recited in claim 19 further including the steps of:

verifying that said received registration identification number is valid; and

wherein when it is determined that said received registration identification number is valid, initiating said step of accessing said communications network.

21. A method as recited in any of claims 19 or 20 further including the step of decoding said received registration identification number into said customer account identifier and said identifying address.

22. A method as recited in any of claims 19, 20 or 21 wherein said registration identification number further includes a check sum for verifying that said registration identification number is valid.

23. A method as recited in any of claims 16, 17, 18, 19, 20, 21 or 22 wherein said configuration record includes a range of static addresses for use by a local area network (LAN) connected to said access device.

24. A method as recited in any of claims 16, 17, 18, 19, 20, 21, 22 or 23 wherein said access device is connected to a local area network (LAN) and said step of configuring said access device includes the sub-step of configuring said LAN for communication with said communications network.

25. A computer program product comprising a computer-usable medium having computer-readable program code embodied thereon for automatically configuring an access device for communication with a communications network, said access device being associated with a customer account identifier, said computer program product comprising computer-readable program code for effecting the following steps within a computer system:

connecting said access device with a configuration server over a communications line;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device;

downloading said configuration record from said configuration server to said access device; and

configuring said access device for communication with said communications network using said configuration information of said configuration record.

26. A computer program product comprising a computer-usable medium having computer-readable program code embodied thereon for automatically configuring an access device for communication with a communications network, said access device being associated with a customer account identifier, said computer program product comprising computer-readable program code for effecting the following steps within a computer system:

accessing said communications network using said access device;

connecting said access device with a configuration server located on said communications network;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device;

downloading said configuration record from said configuration server to said access device; and

configuring said access device for communication with said communications network using said configuration information of said configuration record.

27. A computer program product comprising a computer-usable medium having computer-readable program code embodied thereon for automatically configuring an access device for use as a router in a communications network, said access device being associated with a unique customer account identifier, said computer program product comprising computer-readable program code for effecting the following steps within a computer system:

accessing said communications network using said access device using a temporary dynamic address for said access device;

connecting said access device with a configuration server located on said communications network;

requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device, said configuration information including a static address for said access device;

downloading said configuration record from said configuration server to said access device at said temporary dynamic address; and

configuring said Internet access device for communication with said communications network using said configuration information of said configuration record, including assigning said static address to said access device.

28. An access device for communication with a communications network, said access device being associated with a customer account identifier, said access device comprising:

means for connecting said access device with a configuration server over a communications line;

means for requesting that said configuration server return a configuration record identified by said customer account identifier, said configuration record containing configuration information for said access device;

means for downloading said configuration record from said configuration server to said access device; and

means for configuring said access device for communication with said communications network using said configuration information of said configuration record.

29. An access device for use in communicating with an internet, said access device comprising:

a central processing unit;

a memory device coupled to said central processing unit;

input means coupled to said central processing unit for inputting information from a user;

output means coupled to said central processing unit for presenting information to a user;

a communication means for communicating with said internet using a dynamic address of said access device, said communication means able to access and communicate with said internet without receiving configuration information from said internet; and

automatic configuration means for providing a configuration server address and a customer account identifier and for automatically retrieving configuration information associated with said customer account identifier from a configuration server located on said internet at said configuration server address, said automatic configuration means being arranged to configure said access device using said configuration information such that said access device is configured using a static address included in said configuration information and said communication means is then arranged to access and communicate with said internet using said static address as an address of said access device.

30. An access device as recited in claim 29 further comprising a router for routing information received from said internet to a local area network (LAN) connected to said access device, said router initially configured as having a temporary dynamic address and being arranged to be configured as having a static address.

31. An access device as recited in any of claims 29 or 30 wherein said communication means includes an analog modem and one of an ISDN adapter and a synchronous serial interface.

32. An access device as recited in claim 31 wherein said automatic configuration means is arranged to configure one of said ISDN adapter and said synchronous serial interface for communication with said internet.

33. An access device for use in communicating with an internet, said access device comprising:

a central processing unit;

a memory device coupled to said central processing unit;

an input mechanism coupled to said central processing unit for inputting information from a user;

a display coupled to said central processing unit for presenting information to a user;

a modem for communicating with said internet using an analog communications line, said modem being configured to access and communicate with said internet over said analog communications line without receiving configuration information from said internet; and

a configutor for providing a configuration server address and a customer account identifier and for automatically retrieving configuration information associated with said customer account identifier from a configuration server located on said internet at said configuration server address, said configutor being arranged to configure said access device using said configuration information such said access device is then arranged to access and communicate with said internet.

34. An access device as recited in claim 33 further comprising a router for routing information received from said internet to a local area network (LAN) connected to said access device, said router initially being configured as having a temporary dynamic address and being arranged to be configured by the configutor to have a static address.

35. An access device as recited in any of claims 33 or 34 wherein said access device further includes at least one high speed communication device selected from the group consisting of an ISDN adapter and a synchronous serial interface, and wherein the configutor is arranged to configure the high speed communications device.

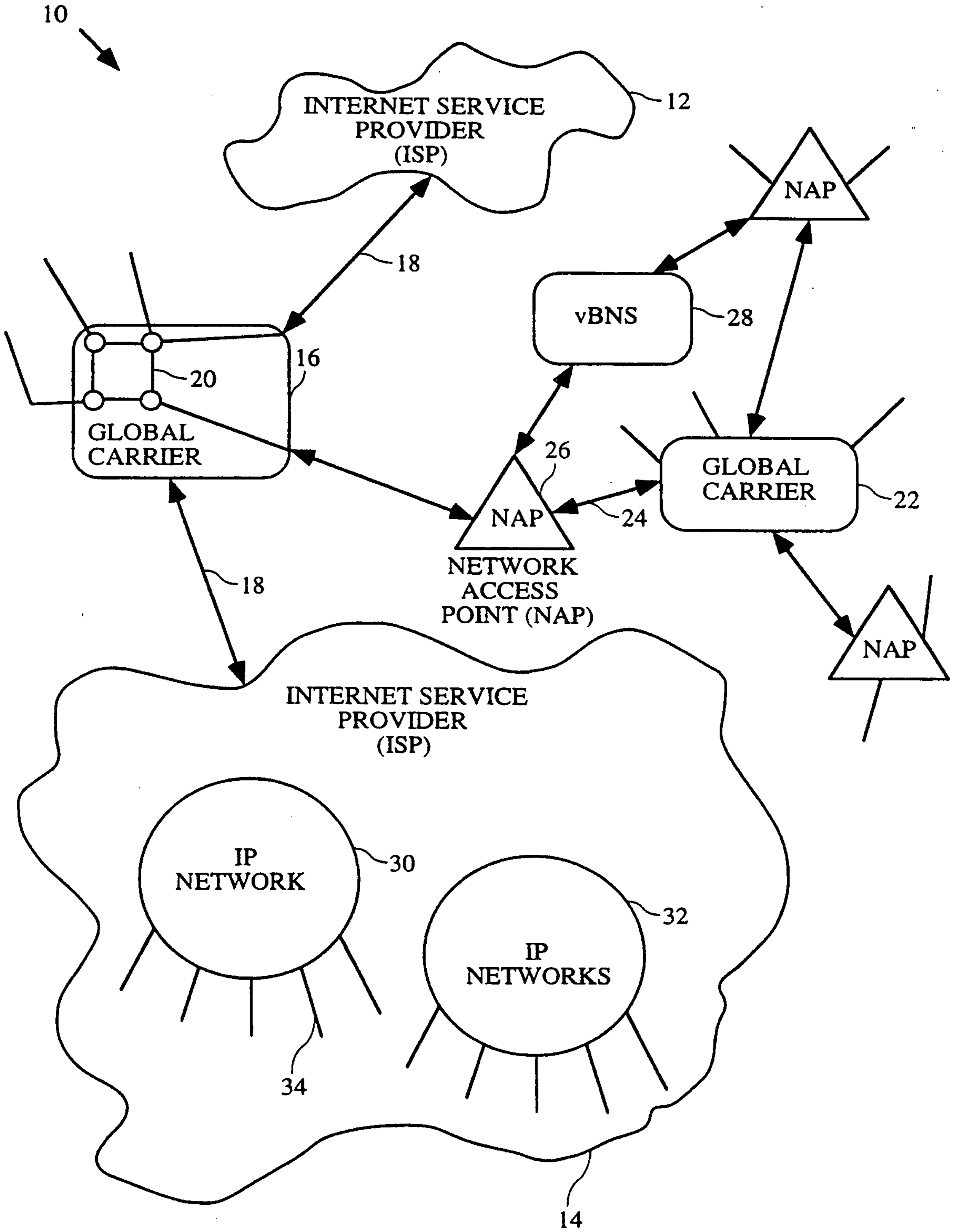

10
INTERNET SERVICE PROVIDER (ISP)
12
18
GLOBAL CARRIER
20
16
NAP
vBNS
28
GLOBAL CARRIER
22
26
NAP
24
NETWORK ACCESS POINT (NAP)
NAP
18
INTERNET SERVICE PROVIDER (ISP)
IP NETWORK
30
IP NETWORKS
32
34
14

FIG. 1

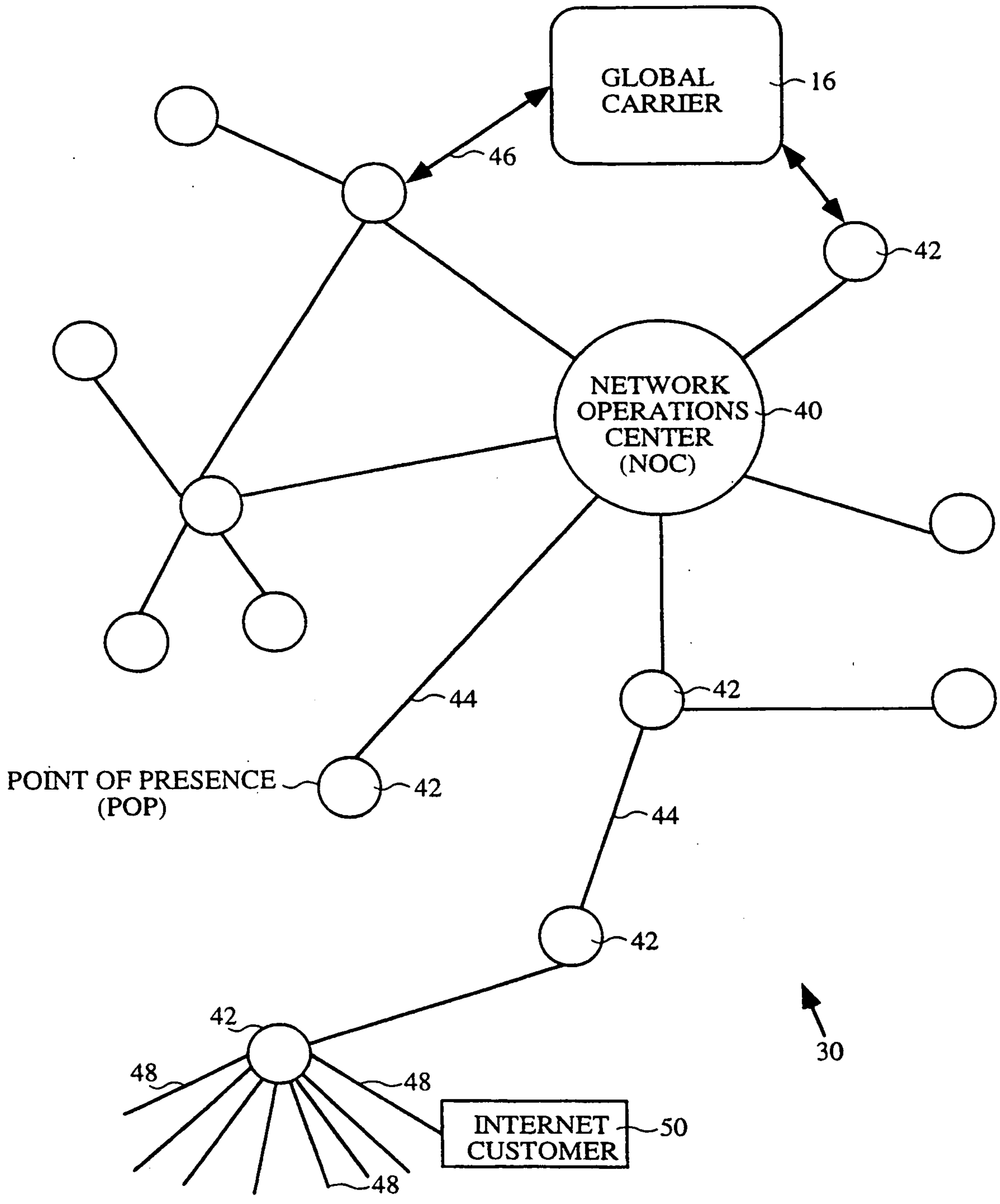

GLOBAL CARRIER
16
46
42
NETWORK OPERATIONS CENTER (NOC)
40
44
42
POINT OF PRESENCE (POP)
42
44
42
42
48
48
INTERNET CUSTOMER
50
48
30

FIG. 2

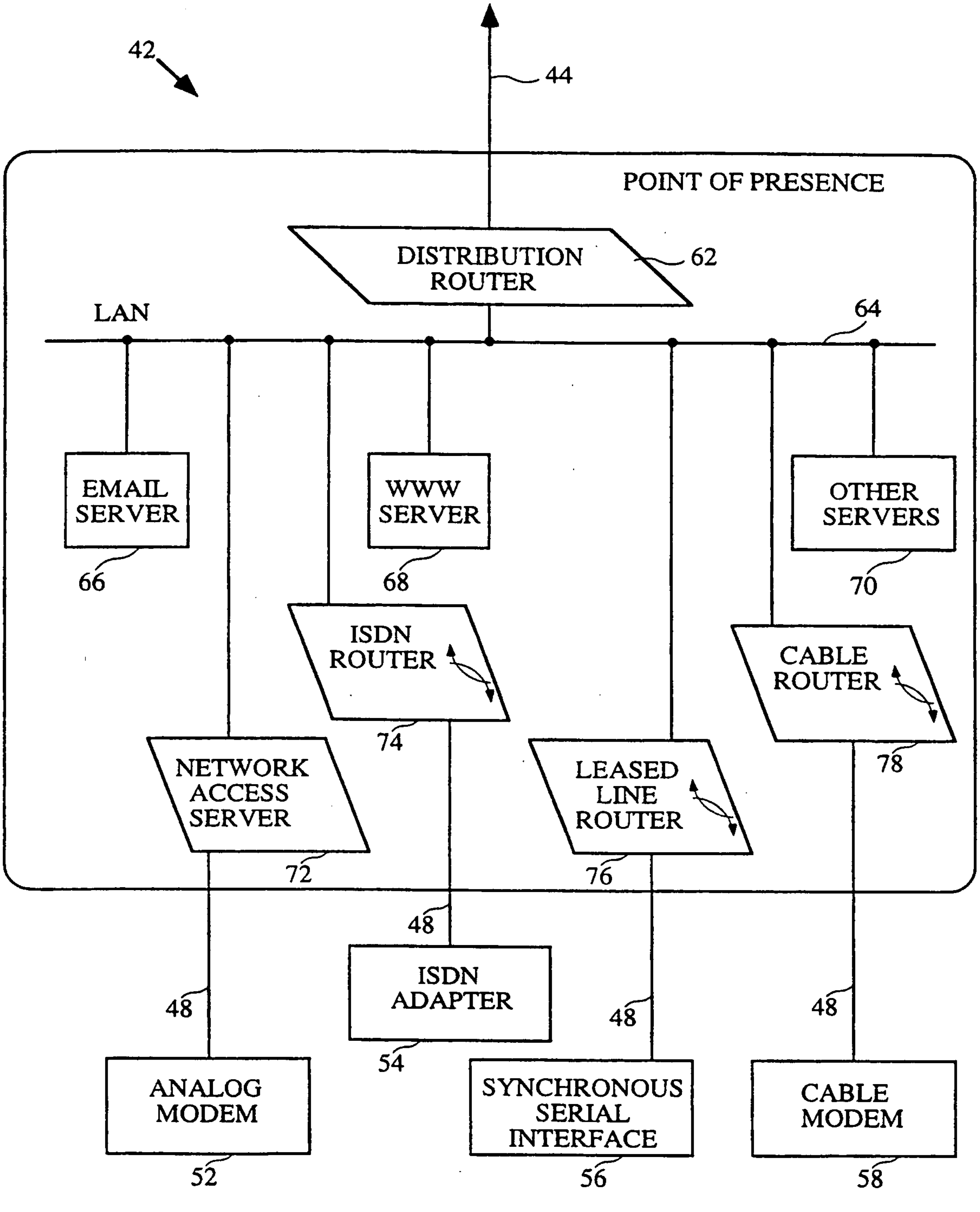
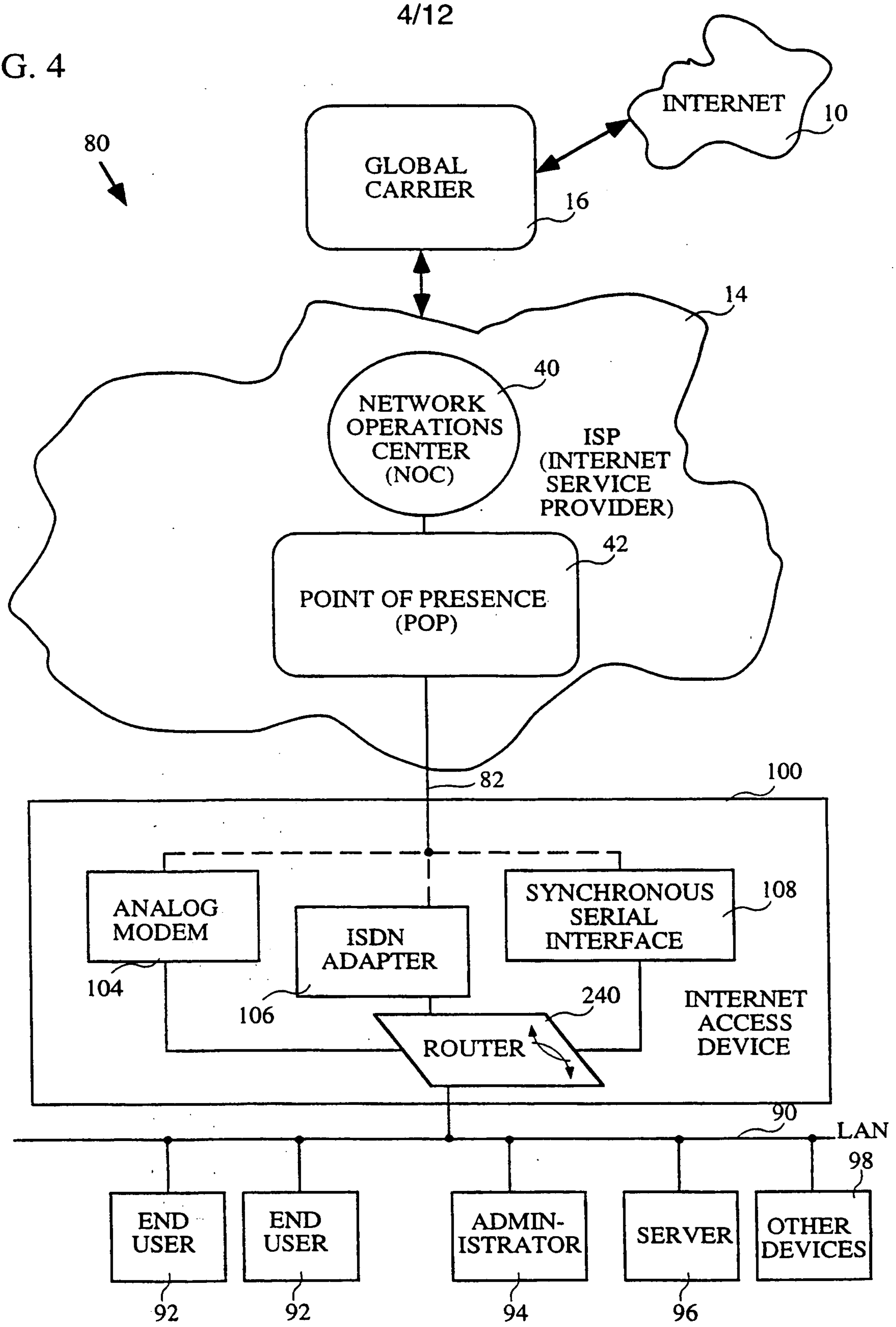

42
44
POINT OF PRESENCE
DISTRIBUTION ROUTER
62
LAN
64
EMAIL SERVER
66
WWW SERVER
68
OTHER SERVERS
70
ISDN ROUTER
74
CABLE ROUTER
78
NETWORK ACCESS SERVER
72
LEASED LINE ROUTER
76
48
48
ISDN ADAPTER
54
48
48
ANALOG MODEM
52
SYNCHRONOUS SERIAL INTERFACE
56
CABLE MODEM
58

FIG. 3

FIG. 4


80
INTERNET
10
GLOBAL CARRIER
16
14
NETWORK OPERATIONS CENTER (NOC)
40
ISP (INTERNET SERVICE PROVIDER)
POINT OF PRESENCE (POP)
42
82
100
ANALOG MODEM
104
ISDN ADAPTER
106
SYNCHRONOUS SERIAL INTERFACE
108
240
ROUTER
INTERNET ACCESS DEVICE
90
LAN
98
END USER
END USER
ADMIN-ISTRATOR
SERVER
OTHER DEVICES
92
92
94
96

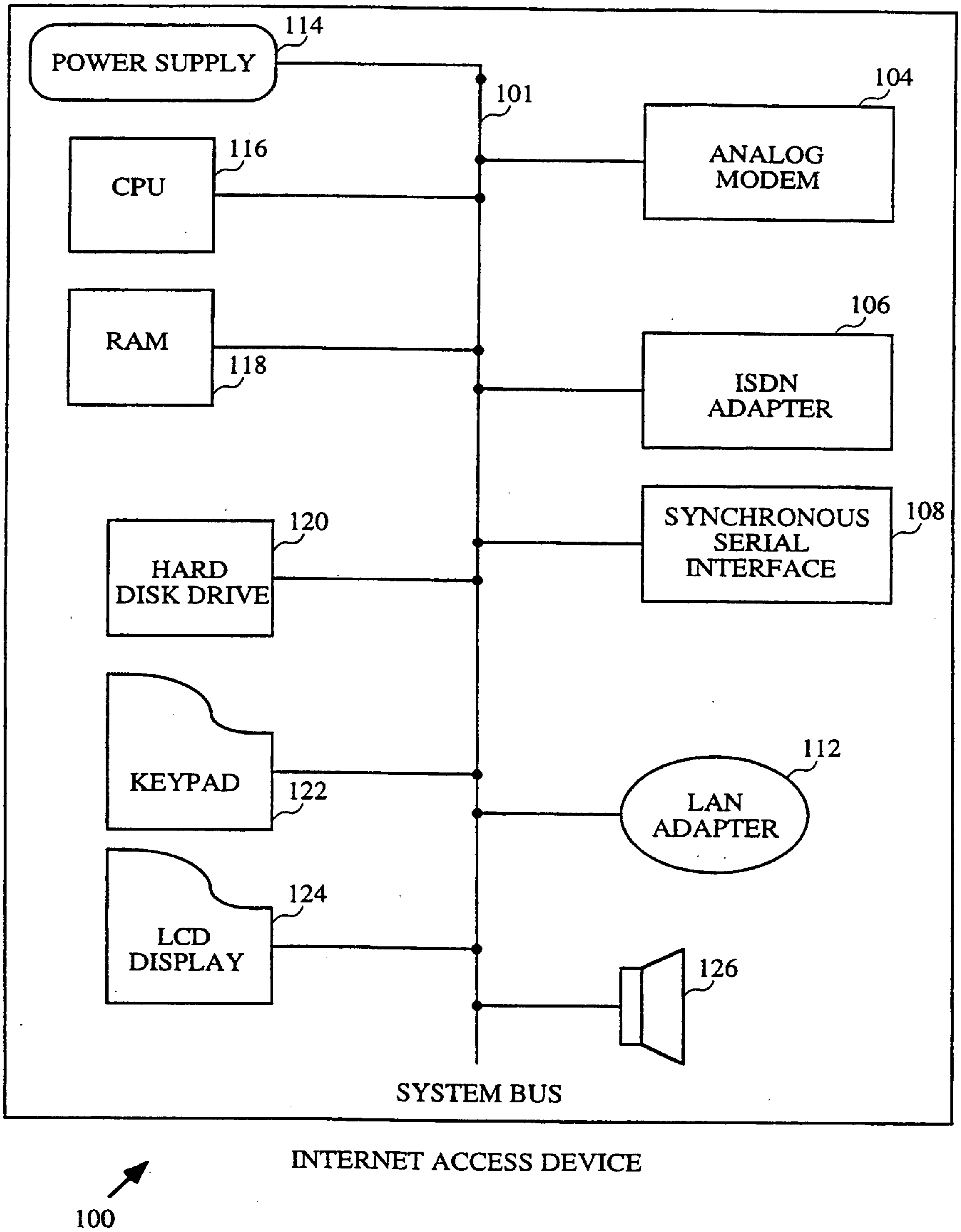

POWER SUPPLY
114
101
104
ANALOG MODEM
CPU
116
RAM
118
106
ISDN ADAPTER
SYNCHRONOUS SERIAL INTERFACE
108
HARD DISK DRIVE
120
KEYPAD
122
112
LAN ADAPTER
LCD DISPLAY
124
126
SYSTEM BUS
INTERNET ACCESS DEVICE
100

FIG. 5

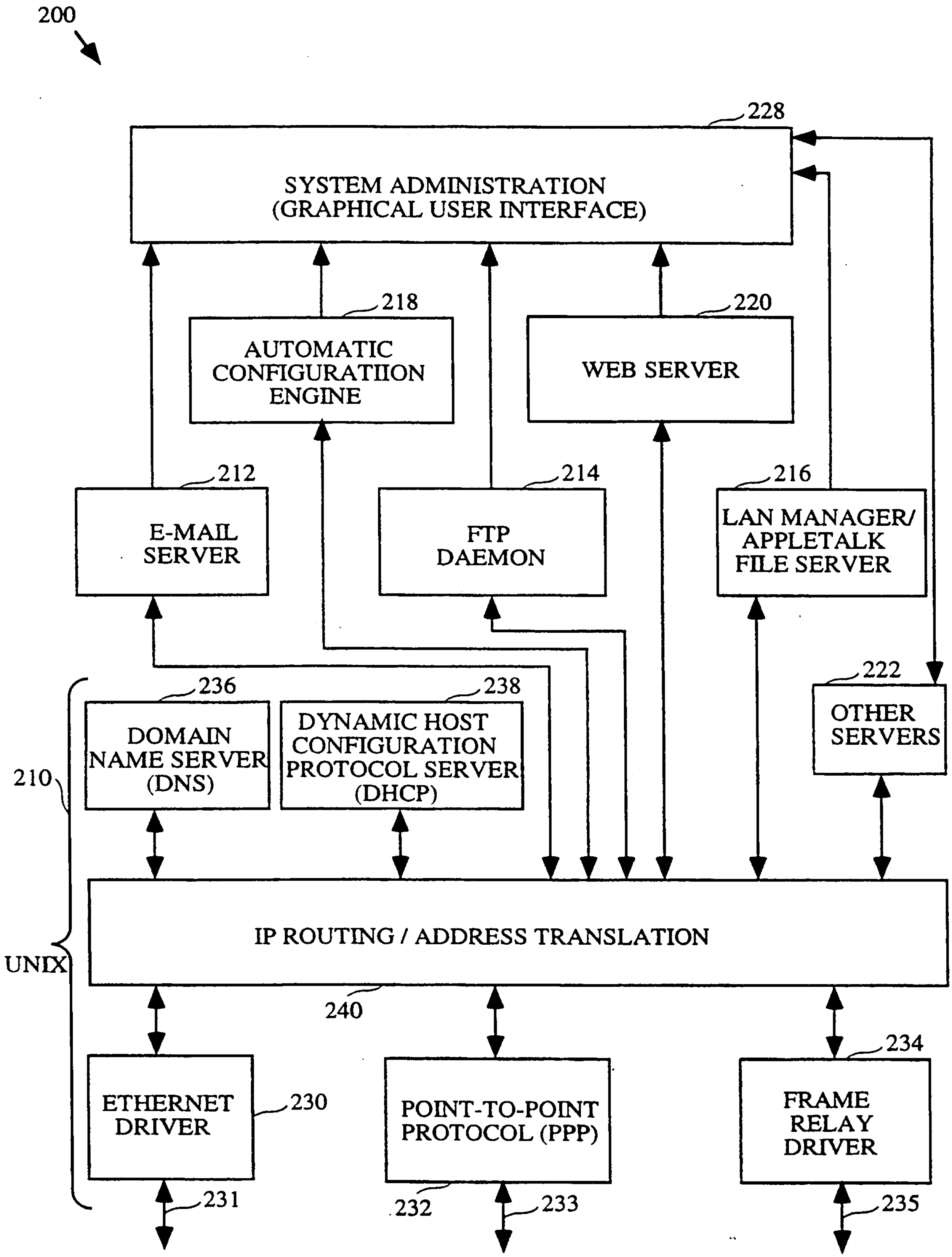
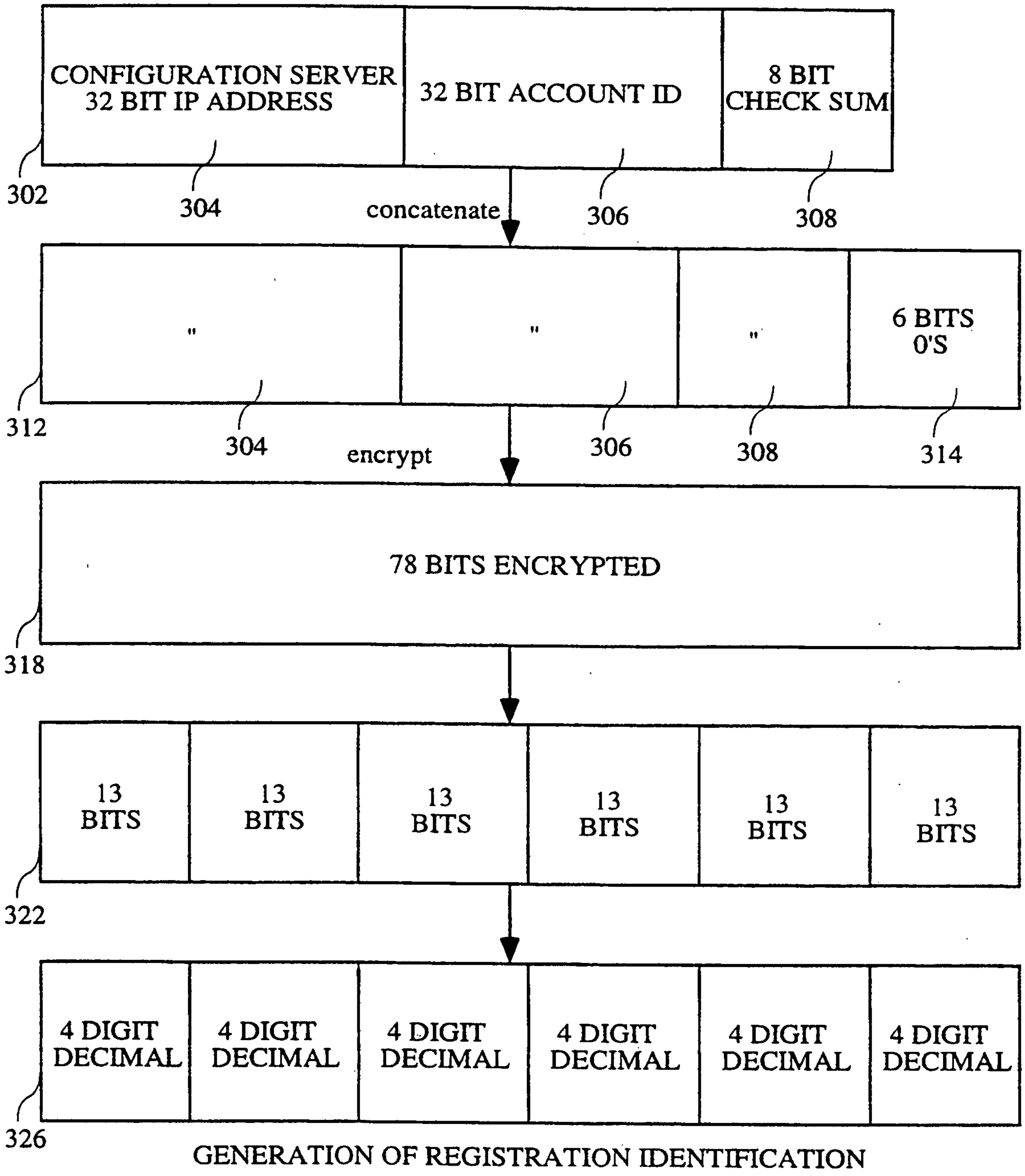

200
228
SYSTEM ADMINISTRATION
(GRAPHICAL USER INTERFACE)
218
AUTOMATIC
CONFIGURATIION
ENGINE
220
WEB SERVER
212
E-MAIL
SERVER
214
FTP
DAEMON
216
LAN MANAGER/
APPLETALK
FILE SERVER
222
OTHER
SERVERS
236
DOMAIN
NAME SERVER
(DNS)
238
DYNAMIC HOST
CONFIGURATION
PROTOCOL SERVER
(DHCP)
210
UNIX
IP ROUTING / ADDRESS TRANSLATION
240
ETHERNET
DRIVER
230
POINT-TO-POINT
PROTOCOL (PPP)
234
FRAME
RELAY
DRIVER
231
232
233
235

FIG. 6



GENERATION OF REGISTRATION IDENTIFICATION

300

FIG. 7

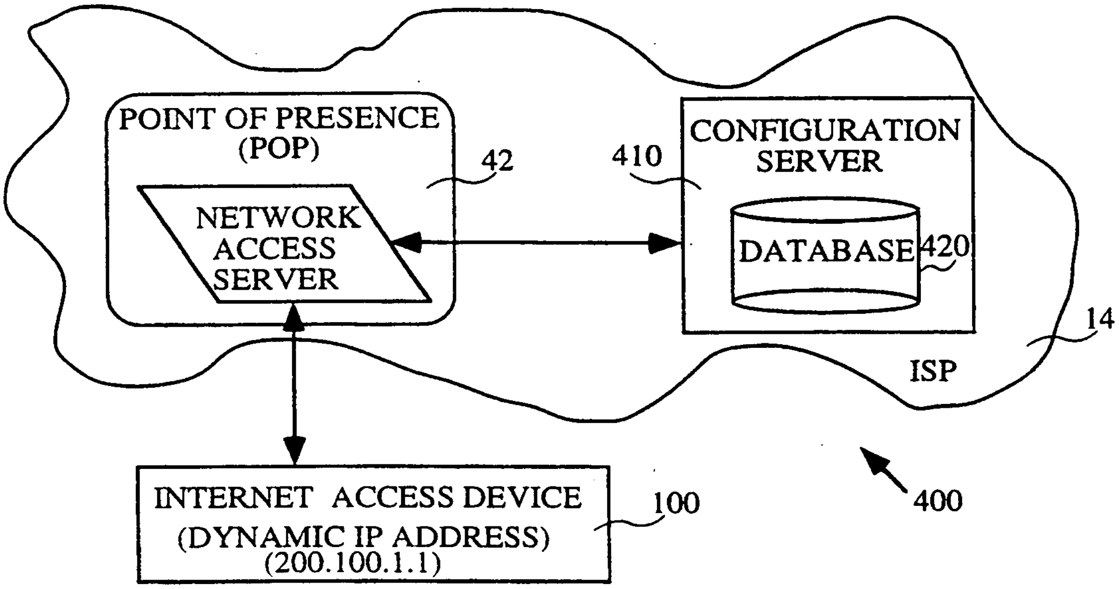

POINT OF PRESENCE
(POP)
42
NETWORK
ACCESS
SERVER
410
CONFIGURATION
SERVER
DATABASE
420
14
ISP
INTERNET ACCESS DEVICE
(DYNAMIC IP ADDRESS)
(200.100.1.1)
100
400

FIG. 8

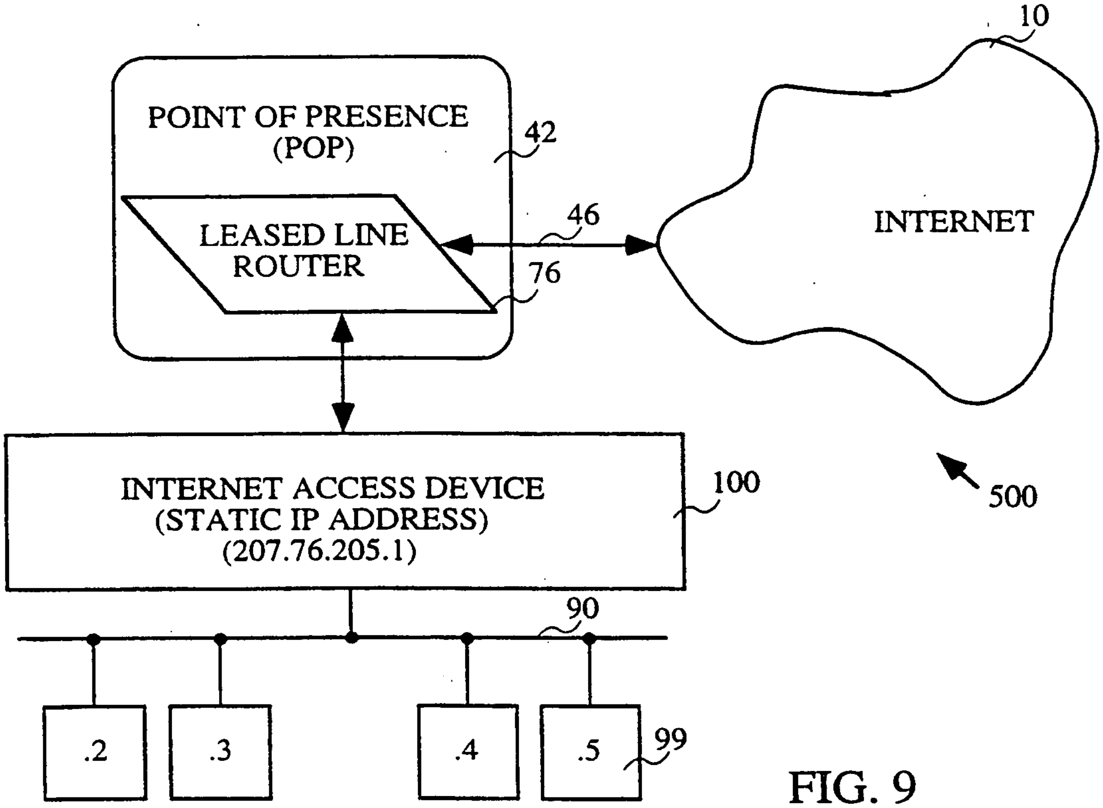

10
POINT OF PRESENCE
(POP)
42
LEASED LINE
ROUTER
46
76
INTERNET
INTERNET ACCESS DEVICE
(STATIC IP ADDRESS)
(207.76.205.1)
100
500
90
.2
.3
.4
.5
99

FIG. 9

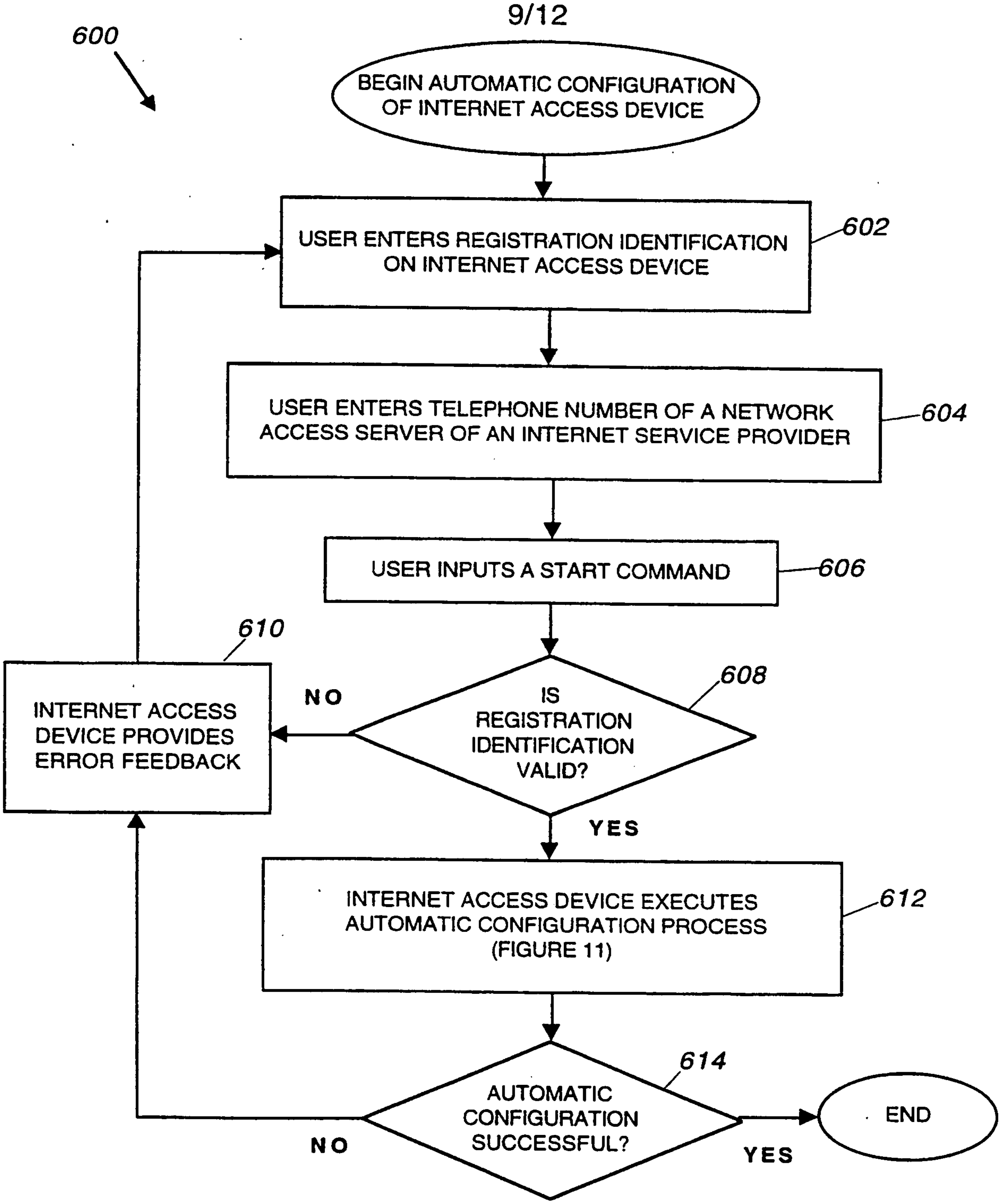
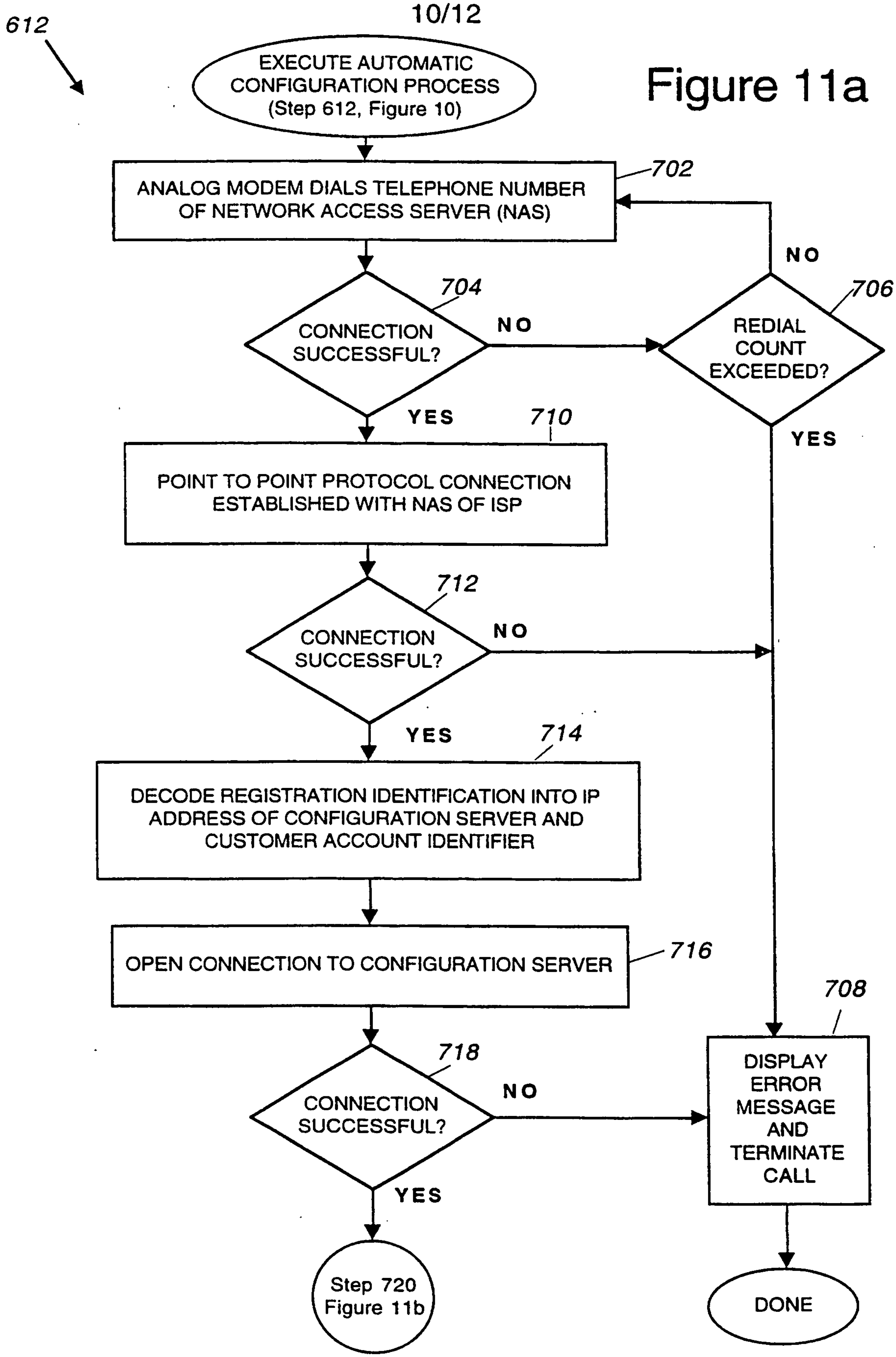

600
BEGIN AUTOMATIC CONFIGURATION OF INTERNET ACCESS DEVICE
USER ENTERS REGISTRATION IDENTIFICATION ON INTERNET ACCESS DEVICE
602
USER ENTERS TELEPHONE NUMBER OF A NETWORK ACCESS SERVER OF AN INTERNET SERVICE PROVIDER
604
USER INPUTS A START COMMAND
606
610
INTERNET ACCESS DEVICE PROVIDES ERROR FEEDBACK
NO
IS REGISTRATION IDENTIFICATION VALID?
608
YES
INTERNET ACCESS DEVICE EXECUTES AUTOMATIC CONFIGURATION PROCESS (FIGURE 11)
612
AUTOMATIC CONFIGURATION SUCCESSFUL?
614
NO
YES
END

Figure 10

Figure 11a


612
EXECUTE AUTOMATIC CONFIGURATION PROCESS (Step 612, Figure 10)
ANALOG MODEM DIALS TELEPHONE NUMBER OF NETWORK ACCESS SERVER (NAS)
702
CONNECTION SUCCESSFUL?
704
NO
YES
REDIAL COUNT EXCEEDED?
706
NO
YES
POINT TO POINT PROTOCOL CONNECTION ESTABLISHED WITH NAS OF ISP
710
CONNECTION SUCCESSFUL?
712
NO
YES
DECODE REGISTRATION IDENTIFICATION INTO IP ADDRESS OF CONFIGURATION SERVER AND CUSTOMER ACCOUNT IDENTIFIER
714
OPEN CONNECTION TO CONFIGURATION SERVER
716
CONNECTION SUCCESSFUL?
718
NO
YES
DISPLAY ERROR MESSAGE AND TERMINATE CALL
708
Step 720 Figure 11b
DONE

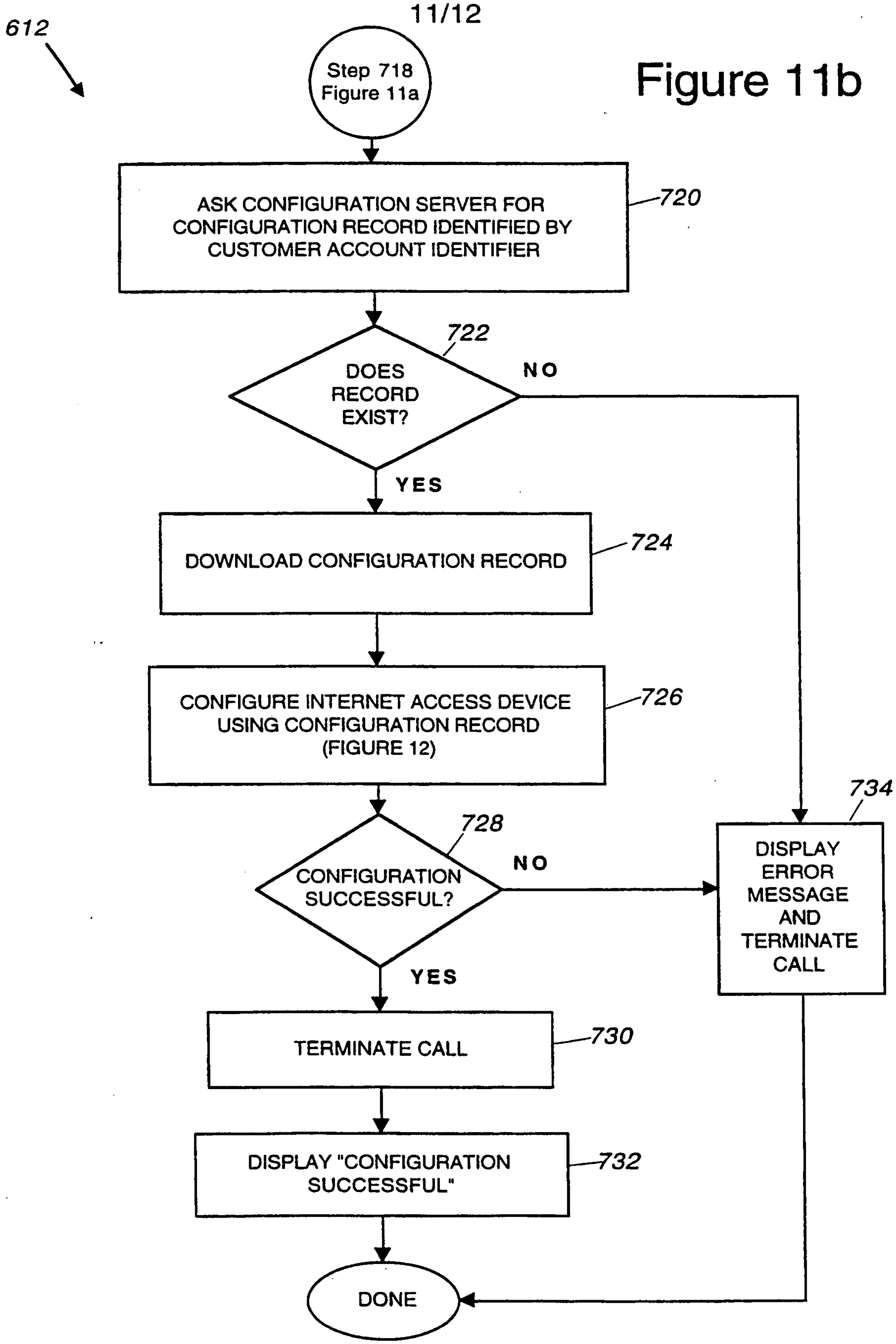

612
Step 718
Figure 11a
ASK CONFIGURATION SERVER FOR CONFIGURATION RECORD IDENTIFIED BY CUSTOMER ACCOUNT IDENTIFIER
720
DOES RECORD EXIST?
722
NO
YES
DOWNLOAD CONFIGURATION RECORD
724
CONFIGURE INTERNET ACCESS DEVICE USING CONFIGURATION RECORD (FIGURE 12)
726
CONFIGURATION SUCCESSFUL?
728
NO
YES
734
DISPLAY ERROR MESSAGE AND TERMINATE CALL
TERMINATE CALL
730
DISPLAY "CONFIGURATION SUCCESSFUL"
732
DONE

Figure 11b

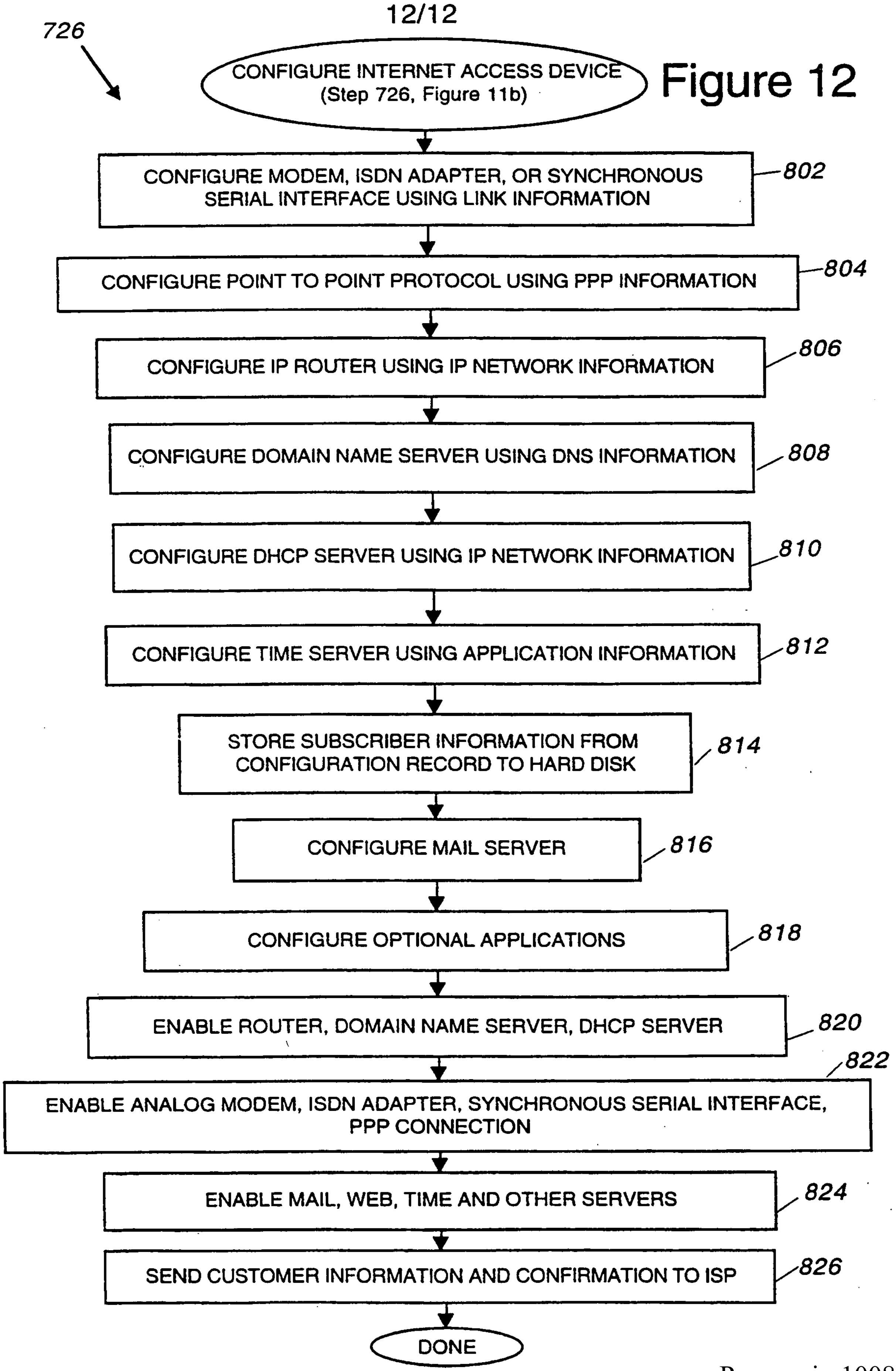

726
CONFIGURE INTERNET ACCESS DEVICE (Step 726, Figure 11b)
CONFIGURE MODEM, ISDN ADAPTER, OR SYNCHRONOUS SERIAL INTERFACE USING LINK INFORMATION
802
CONFIGURE POINT TO POINT PROTOCOL USING PPP INFORMATION
804
CONFIGURE IP ROUTER USING IP NETWORK INFORMATION
806
CONFIGURE DOMAIN NAME SERVER USING DNS INFORMATION
808
CONFIGURE DHCP SERVER USING IP NETWORK INFORMATION
810
CONFIGURE TIME SERVER USING APPLICATION INFORMATION
812
STORE SUBSCRIBER INFORMATION FROM CONFIGURATION RECORD TO HARD DISK
814
CONFIGURE MAIL SERVER
816
CONFIGURE OPTIONAL APPLICATIONS
818
ENABLE ROUTER, DOMAIN NAME SERVER, DHCP SERVER
820
822
ENABLE ANALOG MODEM, ISDN ADAPTER, SYNCHRONOUS SERIAL INTERFACE, PPP CONNECTION
ENABLE MAIL, WEB, TIME AND OTHER SERVERS
824
SEND CUSTOMER INFORMATION AND CONFIRMATION TO ISP
826
DONE

Figure 12

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 97/10600

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 G06F9/445

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	EP 0 793 170 A (SUN MICROSYSTEMS INC) 3 September 1997 see abstract see figure 3 see page 4, column 6, line 15 - page 5, column 8, line 48 ---	1,2,5, 12,25, 26,28, 29,33
E	EP 0 791 881 A (COMPAQ COMPUTER CORP) 27 August 1997 see abstract see page 2, line 46 - line 57 see page 3, line 26 - line 37 --- -/--	1,2,5, 25,26,28

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

1

Date of the actual completion of the international search 4 March 1998	Date of mailing of the international search report 12/03/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Adkhis, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 97/10600

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 321 840 A (AHLIN LEO ET AL) 14 June 1994 see abstract see column 4, line 59 - column 5, line 34 -----	1-35

1

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/US 97/10600

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0793170 A	03-09-97	NONE	
EP 0791881 A	27-08-97	NONE	
US 5321840 A	14-06-94	US 4991199 A	05-02-91
		US 5008927 A	16-04-91
		US 5485370 A	16-01-96
		US 5572572 A	05-11-96
		AT 115807 T	15-12-94
		AU 619861 B	06-02-92
		AU 3689089 A	29-11-89
		CA 1306318 A	11-08-92
		CN 1038182 A	20-12-89
		DE 68920041 D	26-01-95
		DK 263490 A	02-11-90
		EP 0418288 A	27-03-91
		GR 1000586 B	26-08-92
		JP 3505509 T	28-11-91
		MX 167633 B	30-03-93
		PT 90443 B	09-08-95
		WO 8911195 A	16-11-89
		US 5195130 A	16-03-93
		AT 163119 T	15-02-98
		AU 6758290 A	13-06-91
		CA 2068336 A,C	10-05-91
		CN 1054164 A,B	28-08-91
		CN 1093475 A	12-10-94
		EP 0499620 A	26-08-92
		EP 0666681 A	09-08-95
		JP 7170341 A	04-07-95
		JP 5501645 T	25-03-93
		WO 9107839 A	30-05-91

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

(11) EP 0 854 621 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.07.1998 Bulletin 1998/30

(51) Int. Cl.^{6}: **H04L 29/06**, G06F 1/00

(21) Application number: 98100283.5

(22) Date of filing: 09.01.1998

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 17.01.1997 US 785501

(71) Applicant: AT&T Corp.
New York, NY 10013-2412 (US)

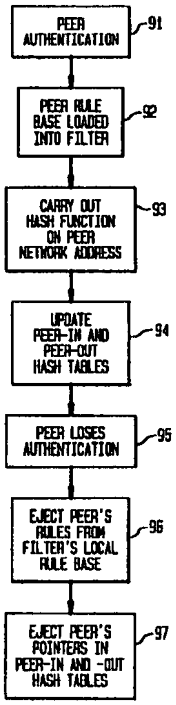
(72) Inventors:
- Zenchelsky, Daniel N.
San Jose, CA 95123 (US)
- Dutta, Partha P.
San Jose, CA 95129 (US)
- London, Thomas B.
Mountain View, CA 94040 (US)
- Vrsalovic, Dalibor F.
Sunnyvale, CA 94087 (US)
- Sül, Karl Andres
Princeton, New Jersey 08540 (US)

(74) Representative:
Modiano, Guido, Dr.-Ing. et al
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
80469 München (DE)

(54) System and method for providing peer level access control on a network

(57) A system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier. The local rule base of a peer is dynamically loaded into a filter when the peer is authenticated, and ejected when the peer is loses authentication. The local rule base is efficiently searched through the use of hash tables wherein a hashed peer network address serves as a pointer the peer's local rules. Each rule comprises a 5-tuple and an action. The action of a rule is carried out on a packet when the 5-tuple of the rule corresponds to the 5-tuple of the packet.

FIG. 9


PEER AUTHENTICATION
91
PEER RULE BASE LOADED INTO FILTER
92
CARRY OUT HASH FUNCTION ON PEER NETWORK ADDRESS
93
UPDATE PEER-IN AND PEER-OUT HASH TABLES
94
PEER LOSES AUTHENTICATION
95
EJECT PEER'S RULES FROM FILTER'S LOCAL RULE BASE
96
EJECT PEER'S POINTERS IN PEER-IN AND -OUT HASH TABLES
97

Printed by Xerox (UK) Business Services
2.16.3/3.4

Description

Field of the Invention

This invention relates to information systems security, in particular to providing access control between one set of automated information systems and another.

Background of the Invention

known methods for implementing access control for a specific computer on a network are cumbersome and inflexible because access rules must be coded and entered by hand by a system administrator. This is impractical for networks whose members change frequently, or whose members' security needs change frequently.

Effective information systems security prevents the unauthorized disclosure, modification or execution of an automated information system's (AIS) data and processes. As used here, the term AIS refers to a computer, network of computers, internetwork of computers, or any subset thereof. The term "data" refers to any information resident on an AIS, including files and programs. The term "processes" refers to programs in any stage of execution on an AIS.

A "host" is a computer with an assigned network address, e.g., an Internet Protocol (IP) address. A "user" is a computer that does not have a fixed, assigned network address. To obtain connectivity to the Internet, for example, a user must commonly obtain a temporary IP address from a host with a pool of such addresses. Such a temporary IP address is retained by the user only for the duration of a single session of connectivity with the Internet.

Information flows in certain networks in packets. A "packet" is a quantum of information that that has a header containing a source and a destination address. An example of a packet is an IP packet. Packets such as IP packets have a network protocol identifier ("protocol") as a part of packet header. The protocol identifies the version number of the protocol used to route the packet. An example of a network protocol identifier is the IP protocol field in an IP packet header.

Packets on a network are directed to and from ports. A "port" is a logical address within a computer through which a process executing on the computer communicates with other executing processes. These other processes may reside on the same computer, or on other networked computers.

Information systems security is implemented by means of a security policy, which comprises rules directed towards regulating the flow of information in an AIS. The rules of a security policy are embodied in a "rule base," a set of rules that specify whether a packet should be passed to the intended recipient or dropped based upon the packet's identifier. A packet identifier is data generally carried in the packet header that serves to identify the packet. An example of a packet identifier is a circuit number, which occurs in the headers of packets flowing in connection-oriented (i.e., circuit-switched) packet switched networks. Another example of a packet identifier is a packet 5-tuple, which is the packet's source and destination address, source and destination port, and protocol. Packets with 5-tuples flow in connectionless packet switched networks.

A rule base may be global or local. A global rule base is a uniform set of rules ("global rules") that apply to a group of users, hosts, or both. A local rule base is a set of rules ("local rules") that apply to a single user with a temporary network address or a host. A single user with a temporary network address or a host that has its own rule base is called a "peer."

Another means for implementing security policy is to restrict access to a network to a predetermined set of users and hosts. When a user or host requests access, its identity must be established and verified before access is granted. This process implicates two steps: identification and authentication.

FIG 1 shows one method of identification and authentication in the form of a flow chart with each step designated by a reference numeral. A first step requires a source of information to identify itself by name by supplying a string of data called a user id 10. To prevent an imposter from obtaining the privileges associated with a given user id, the user behind the user id is verified by requiring it to provide a password 11 that is normally kept confidential. Such verification is called "authentication." The AIS checks the combination of source id and password against a list of valid users, 12. When the AIS recognizes a valid user id and corresponding password, a user or host is said to have been identified and authenticated 14. Otherwise, the request for access is denied 13. Hereinafter, a source that has been identified and authenticated will be said to have been "authenticated" for purposes of brevity.

A security policy rule base is implemented on a network using a device called a filter comprising hardware and software. The rule base is loaded into the filter, which receives packets en route (between their source and destination) and checks the identifier of each packet against the identifier contained in each rule of the rule base for a match, i.e., if the packet corresponds to the rule. A packet corresponds to a rule if the rule applies to the packet. Hence, a rule that is meant to apply to packets with a circuit number of 3254, for example, "corresponds" to all packets with a packet identifier that indicates circuit number 3254. If the network packet identifier corresponds to a rule identifier, the filter carries out the PASS or DROP action prescribed by the rule on the packet. If the PASS action is carried out, the packet is allowed to pass through the filter. If the DROP action is carried out, the packet is eliminated.

A filter is often combined with other hardware and software that helps manage the flow of information through the filter. The combination of hardware and software that carries out and supports packet filtering is called a firewall. A firewall is often positioned between a first network that "owns" the firewall and a second network. The purpose of the firewall is to regulate the flow of information into and out of the first network from the second network by implementing the rule base belonging to the first network for all such information.

A typical application of a firewall is shown in FIG 2. A corporate network 20 may wish to provide access to Internet hosts 21 to its subscribers, but may wish to limit the access that the Internet hosts 21 have to the corporate network 20, which may contain trade secrets and proprietary information. The corporate network 20 would develop a security policy implemented by a firewall 22 placed at the interface between the corporate network 20 and the Internet hosts 21. The firewall 22 comprises a filter 23 that would PASS or DROP packets from Internet hosts 21 to corporate network subscribers 20 and vice versa based upon the packets' source and destination addresses. The firewall is said to belong to the corporate network, and enforces rules that "protect" hosts within the corporate network that have IP addresses. Such hosts are said to be "behind" the corporate network firewall.

An example of a rule base for corporate network 20 having hosts A 24, B 25 and C 26, connected through a firewall 22 to the Internet having hosts G 27, H 28 and I 29 is as follows:

SOURCE Address, Port	DESTINATION Address, Port	VERSION	ACTION
A,21	G,32	4	PASS
A,22	H,19	3	DROP
G,11	A,64	4	DROP
C,9	I,23	4	PASS

Every rule base must also have a default action for transactions that are not explicitly specified in the rule base, which is usually the DROP action. Thus, packets from system A,21 to system G,33 will be dropped because the above rule base does not expressly include a rule for such a transfer.

A typical architecture for providing users access to the Internet is shown in FIG 3. Users 31 and 32 do not have fixed IP addresses. Rather, a user is assigned temporary IP addresses by an Internet Service Provider (ISP) Point of Presence (POP) 33 from a pool of such addresses kept by the POP 33 for this purpose. A POP comprises at least one host (not shown). When a user 31 terminates his session of access to the Internet 35, the IP address is returned to the POP 33. Thus, over successive access sessions, a user 31 is likely to have several different IP addesses.

Known filters are not well suited to providing appropriate access control for networks such as a POP. This is because a known filter is only able to load and store rules through the intervention of a system administrator, a slow and cumbersome process. Indeed, the system administrator generally must hand-code rules in a format specific to the filter platform. With known filters, it is impractical to implement the access rules of a specific user (known as the user's "local rules") who is accessing and leaving the network with changing network addresses.

This problem is illustrated in FIGs 5a and 5b. FIG 5a shows a first session where a first user 51 has requested Internet access and been authenticated by a POP and been assigned IP address B from the POP IP address pool 52. Likewise, a second user 53 has been authenticated and been assigned IP address E from the pool 52. A rule base 53 is loaded into a filter to regulate the flow of information between users 51 and 53 and the hosts P, U, V and W on the Internet. The rule base shown in FIGs 5a and 5b show only the source and destination addresses for each rule, and omit source and destination ports and protocol for simplicity.

Both users stop accessing the Internet and then later request access again and are authenticated for a second session, shown in FIG 5b. This time, the first user 51 is assigned IP address E from the pool 52, and the second user is assigned IP address A. With the newly assigned network addresses, the rule base in the filter is now out of date, containing no rules for the second user, and the wrong rules for the first user, which has been assigned the IP address assigned to the second user during the first session. Even if both users had fortuitously been reassigned the same IP addresses for their second sessions, if either user's security needs had changed between sessions, a new rule base would have had to be loaded into the filter. As discussed above, loading rules into known filters is tedious. Loading and dropping such rules with the frequency that users access and leave a POP is impractical for known filters.

The inflexibility of known filters often necessitates the implementation of rule bases that are too broad for a given application. Without the possibility of easy updates, it is simpler to mandate global rules that apply to all AIS behind a filter rather than to load rules that apply to specific hosts. In such a case, all AIS behind the filter must conform to the most restrictive security requirements of any such AIS, resulting in overly restrictive filtering.

The shortcomings of known filters are illustrated by some of the architectures presently used to provide information systems security for a POP. The architecture shown in FIG 3 provides a minimal level of security through an authentication system 34 which limits access to a predetermined list of authenticated users. But the list of users must generally be entered by hand by the system administrator, and so cannot be easily changed. Further, once access is granted, the access is unlimited. Information may flow to and from users 31 and 32 from the Internet 35 without regulation, providing no security past the initial authentication process. This exposes users 31 and 32 to the risk of hacker attacks from users and hosts on the Internet, possibly resulting in the theft or unauthorized manipulation of user data.

The architecture illustrated in FIG 4 shows another known solution to providing information systems security on a POP. The known filter 46 implements a security policy for packets flowing between the Internet 45 and hosts 41 and 42. However, the rule base in the filter 46 must still be formulated and loaded by the system administrator. Further, the network addresses of the users 31 and 32 are likely to change on a session by session basis. This means that it is only practical to load general, "global" rules into the filter that are valid for all of the users. Thus, for example, if user A does not wish to receive packets from a particular host on the Internet, the filter rule base must drop all such packets, thus cutting off user B from receiving packets from that Internet host as well. In this way, the global rule base necessitated by the limited capabilities of known filtering systems is almost always too broad. Another disadvantage is that it is difficult to change the filter rule base to accommodate changing security needs of either user 41 or 42.

Another architecture that provides security on for each peer is shown in FIG 6. Here, filters 66 and 67 are placed between users 61 and 62, respectively, and the POP. Requiring every user to have its own filter is an expensive solution that is impractical to implement.

What is needed is a filtering system and method that accurately and efficiently implements local rule bases on a network whose configuration and security needs are constantly changing. Such an invention would provide peer-level security flexibly and inexpensively, with little intervention required from a system administrator.

Summary of the Invention

The present invention comprises a filter that efficiently stores, implements and maintains access rules specific to an individual computer on a network with rapidly changing configurations and security needs. This advantageously allows an individual computer (a peer) to implement its security policy on a filter shared by many such computers on a network.

When a local rule base is no longer valid because the peer is no longer authenticated to the filter in accordance with the present invention, the peer's local rule base is "ejected," i.e., a logical operation is carried out at the filter whereby the local rule base is deleted from the filter. This logical operation of stored data in a computer is well known in the art. This effectively regulates the flow of information on session-by-session basis, which is especially advantageous in AIS where individual users and hosts have different security needs that change from time to time. For example, the present invention is useful for implementing a parental control system wherein a parent is able to regulate the access to certain types of licentious material on the Internet for household Internet access accounts.

The present invention allows a single device to flexibly and efficiently regulate the flow of information in accordance with security policies that are specifically tailored to the individual user or host. Advantageously, no intervention on the part of the system administrator is ordinarily required in the ordinary functioning of the present invention. Unlike known filters, the present invention is able to accommodate users with temporary network addresses as easily as hosts with fixed network addresses.

In accordance with the present invention, each individual peer is authenticated upon requesting network access. The peer's local rule base is then loaded into the filter of the present invention, either from the peer itself, or from another user, host or peer. When the peer is no longer authenticated to the POP (e.g., the peer loses connectivity or logs off from the POP), the peer's local rule base is ejected (deleted)from the filter.

Brief Description of the Drawings

FIG 1	shows the process of identification and authentication.
FIG 2	shows a firewall interposed between a corporate network and the Internet.
FIG 3	shows users connected to the Internet through a Point of Presence (POP) having an authentication system.
FIG 4	shows a POP with an authentication system and a filter.
FIG 5a	shows a first Internet access session for two users through a POP having a filter.
FIG 5b	shows a second Internet access session for two users through a POP having a filter.
FIG 6	shows a known method of providing user level access control to the Internet.
FIG 7a	shows a rule base architecture in accordance with an embodiment of the present invention.

FIG 7b	shows an implementation of the rule base architecture shown in FIG 7a.
FIG 8a	shows a POP with a filter and an authentication system that provides access to the Internet to three peers.
FIG 8b	shows a simplified depiction of the rule bases belonging to the peers shown in FIG 8a.
FIG 8c	shows a hash function applied to the network addresses of the three peers shown in FIG 8a, and the local-in and local-out rule bases.
FIG 8d	shows a detailed representation of the box "Check Local Rule Base" shown in FIG 7b.
FIG 9	shows an implementation of the present invention.

Detailed Description

In accordance with the present invention, FIG 7a shows an embodiment of a rule architecture that incorporates the functionality of known filters by including a global pre-rule base 701, a local rule base 702 and a global post-rule base 703.

The global pre-rule base 701 usually comprises general rules that apply to all hosts behind the firewall, and are most efficiently applied before any local rules. An example of a global pre-rule is that no telnet (remote login) requests are allowed past the firewall.

The local rule base 702 comprises the set of peer rule bases loaded into the filter for authenticated peers. These rule pertain to specific hosts. An example of a local rule is that host A may not receive e-mail from beyond of the firewall.

The global post-rule base 703 comprises general rules that are most efficiently applied after the global pre-rule base and local rule base is searched. A rule applied in the global post-rule base need not have the same effect as if it were applied in the global pre-rule base. Consider the above example prohibiting the reception of certain telnet requests. If this rule is placed in the global post-rule base, the local rule base is searched first, and may contain a rule allowing a telnet request through for a particular peer. If such a rule is found in the local rule base, the global post-rule base is not subsequently searched, and the telnet request is allowed to pass. Consider the different effect of the same rule when it occurs in the global pre-rule base, which is to block all telnet requests for all hosts behind the firewall. The importance of the order of applying rules is evident from a more thorough consideration of the method of the present invention.

FIG 7b illustrates a flow chart of packet processing or filtering in accordance with the present invention. As shown therein, a packet entering the filter is first checked against a global pre-rule base 711 containing rules for all hosts and users having network addresses behind the firewall.

If a corresponding rule is found and the prescribed action is DROP, the packet is dropped 712. If a corresponding rule is found and the action is PASS, the packet is passed 720. If no corresponding rule is found, then the local rule base is checked 713.

The local rule base 702 is the set of all per user rule bases that are dynamically loaded upon authentication and ejected upon loss of authentication in accordance with the present invention.

If a corresponding rule is found in the local rule base and the action is DROP, the packet is dropped 714. If a corresponding rule is found and the action is PASS, the packet is passed 721. If no corresponding rule is found, then the global post-rule base is checked 715.

If a corresponding rule is found in the global post-rule base and the action is DROP, the packet is dropped 716. If the action is PASS, the packet is passed 722. If no corresponding rule was found in any of the rule bases, then the packet is checked against the default rule 717, whose action is generally to DROP the packet. If the packet corresponds to the default rule, then the default action is carried out 723. If the packet does not match the default rule, then an error condition occurs 724.

This rule base architecture advantageously retains the functionality of known filters. For example, if there are rules in the global pre- or post-rule base only, the filter behaves the same as known filters. If there are only rules in the local rule base, the filter has all of the new and innovative features of the present invention without having global rules.

It is advantageous to implement the present invention with a system for efficiently searching the local rule base for corresponding rules for a given packet. A system that provides such efficiencies uses a hash function to generate an index for the rules. A hash function maps a string of characters to an integer. As is known in the art, a character string is represented as binary numbers inside a computer. An example of a hash function would be to take the third, fourth and fifth bytes of a character string as it is stored in a computer as the first, second and third digits of an integer to be associated with the string. A string on which a hash function has been carried out is said to be "hashed," and the resulting integer is referred to as the "hash" of the string.

This is carried out by logically dividing the local rules into local-in rules and local-out rules. A local-in rule is any rule that applies to a packet whose destination address corresponds to a network address behind the firewall. For example, suppose a host with network address A is behind the firewall, and hosts B, C and D are outside the firewall. The following are examples of local-in rules for host A, following the format SOURCE ADDRESS, SOURCE PORT--> DESTINATION ADDRESS, DESTINATION PORT: Protocol: ACTION:

B,31-->A,33:4:DROP
C,64-->A,45:4:PASS
D,11-->A,17:4:PASS

A local-out rule is any rule that applies to a packet whose source corresponds to a network address behind the firewall. Local out-rules for the above example are:

A,44-->B,70:4:PASS
A,13-->C,64:4:DROP
A,12-->D,17:4:DROP

In accordance with the present invention, a hash function h is carried out on the network address of the owner of a local rule base. A hash function associates an integer with a string. For the above example in which a host with network address A ("host A") has a local rule base, a hash function would be carried out on A: h(A)=N , where N is an integer An example of such a hash function is to take the last decimal digit in each octet of an IP address and compose an integer for the hash number. Thus, for example, the IP address 123.4.46.135 would have a hash value of 3465.

After the hash function is carried out, a local-in and a local-out hash table is generated. These tables are essentially indexes searchable on hash numbers derived from network addresses of peers, where each hashed peer network address points to that peer's local-in and local-out rules. Thus, if A is the network address of peer A, and if h(A)=32, then 32 would point to peer A's local-in and local-out rules in the local rule base.

The advantages of this indexing system in accordance with the present invention may be demonstrated with the aid of FIGs 8a, 8b, 8c and 8d. FIG 8a shows an example architecture where peers A 801, B 802, and C 803 are behind a firewall 804 having a filter 805 connected to a network 806 having hosts G 807, H 808 and I 809. These letters represent network addresses. FIG 8b shows the local rule base associated with each host. For simplicity, each rule in the rule bases is shown only as a network source and destination address; the source and destination ports and protocol numbers are not shown. The asterisk represents a wildcard indicating any host. For example, this feature may be advantageously implemented in accordance with the present invention by including wildcards in one or more of the four octets that constitute an IP address. The following IP address specifications are all valid for use in rule bases in accordance with the present invention:

123.*.233.2
34.*.*.155
..*.32
..*.*

The wildcard feature may also be used in accordance with the present invention in a similar fashion in any other component in the 5-tuple, i.e., the source and destination ports and the protocol.

FIG 8c shows the peer-in hash table 821 and peer-out hash table 822 derived from the local rules shown in FIG 8b and hash function h carried out on network addresses A, B and C 823. When a packet is received by the filter 805, the filter carries out the same hash function h on the packet's source and destination address 824.

FIG 8d shows the method by which the hash tables are searched in accordance with the present invention. FIG 8d represents a detailed view of the box "Check Local Rule Base" 713 in FIG 7b.

In accordance with the present invention, if there was no corresponding rule found in the global pre-rule base 711 (FIG 7b), then the local-in hash table is efficiently searched for a rule that corresponds to the packet 841. If a corresponding rule is found and the action is DROP, the packet is dropped 842. If the action is PASS or there is no corresponding rule, the peer-out hash table is checked 843. If a corresponding rule in the hash-out table is found and the action is DROP, the packet is dropped 844. If the action is PASS or there is no corresponding rule, and if at least one of the hash tables contained a corresponding rule, the packet is passed 845. If there were no corresponding rules in either hash table 846, then the post-rule base is checked 715 as shown in FIG 7b.

Were it not for the peer-in and peer-out hash tables, the rules would have to be searched far less efficiently by searching the entire rule base for rule identifiers (e.g., 5-tuples) that match the packet identifier (e.g., 5-tuple.) The part of the rule that identifies the packet to which the rule applies (the rule identifier) is also called the rule "key." Using hash tables eliminates the need to search the keys of all rules, pointing instead to the relevant subset of possibly applicable rules through a speedier search. Thus, the scope and computational time needed to carry out the search is substantially and advantageously reduced, reducing the delay in packet transit time caused by the interposition of a filter between the packet source and destination.

As shown in FIG 9, a peer is first authenticated 91 in accordance with the present invention. Upon authentication, the peer's local rule base is loaded into the filter 92. A hash function is carried out on the peer's network address 93, and the filter's peer-in and peer-out hash tables are updated 94 with pointers to the peer's peer-in and peer-out rules. When the peer is no longer authenticated 95, the peer's local rules are ejected from the filter local rule base 96, and the pointers to the peer's peer-in and peer-out rules are ejected from filter's peer-in and peer-out hash tables 97.

The present invention provides new security functionality on a per user basis to filters and firewalls, while maintaining the functionality of known filters. The present invention allows for the dynamic adjustment of local rule bases that can be dynamically tailored to meet the changing needs of the individual user.

Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A filter for providing peer level access control on a network having a peer with a local rule base, wherein said filter comprises:

   a. means for accessing a peer's local rule base; and
   b. means for receiving a packet having a packet identifier, identifying a corresponding local rule, and carrying out the action of the corresponding local rule on the packet while said filter is filtering packets for the peer. on the packet.

2. The filter of claim 1, further comprising:

   c. means for ejecting said local rule base from said filter.

3. The filter of claim 1, wherein the packet identifier comprises a source and destination address, a source and destination port, and a protocol identifier.

4. The filter of claim 1, wherein said means for accessing the local rule base comprises receiving and storing the local rule base.

5. The filter of claim 1, further comprising means for authenticating the peer.

6. The filter of claim 1, further comprising a global pre-rule base having a global pre-rule, wherein upon receiving the packet, said filter first searches said global pre-rule base for a rule that corresponds to the packet and carries out the action of the corresponding global pre-rule on the packet, and wherein if no corresponding global pre-rule is identified, the filter searches the local rule base for a rule that corresponds to the packet and carries out the action of the corresponding local rule on the packet.

7. The filter of claim 1, further comprising a global post-rule base, wherein the global post-rule base is searched for a rule that corresponds to the packet, and the action of a global post-rule is carried out if it corresponds to the packet only if no corresponding rule in said global pre-rule base and no corresponding rule in said local rule base are identified.

8. The filter of claim 1, further comprising a default rule, wherein if no corresponding pre-global rule and no corresponding local rule and no corresponding post-global rule are identified, said filter carries out the action of said default rule if said default rule corresponds to the packet, and generates an error condition if said default rule does not correspond to the packet.

9. The filter of claim 1, wherein the peer has a network address, and wherein the packet identifier comprises a packet source address and a packet destination address, and wherein a local rule comprises a rule source address, a rule destination address and an action, further comprising a local-in hash table having an in-pointer derived by applying a hash function to the network address of the peer, said in-pointer pointing to a peer's local rule whose rule destination address corresponds to the network address of said peer.

10. The filter of claim 1, wherein the peer has a network address, and wherein the packet identifier comprises a packet source address and a packet destination address, and wherein a local rule comprises a rule source address, a rule destination address and an action, further comprising a local-out hash table having an out-pointer derived by applying a hash function to the network address of the peer, said out-pointer pointing to a peer's local rule whose rule

source address corresponds to the network address of said peer.

11. A method for providing peer-level access control on a network, said method comprising:

a. accessing a local rule base of a peer;
b. receiving a packet having a packet identifier; and
c. searching the local rule base, identifying a local rule that corresponds to the packet identifier, and carrying out the action of a local rule if the local rule corresponds to the packet.

12. The method of claim 11, further comprising the step of:

d. ejecting the local rule base.

13. The method of claim 11, wherein the packet identifier comprises a source and destination address, a source and destination port, and a protocol identifier.

14. The method of claim 11, wherein accessing a local rule base comprises the steps of receiving and storing the local rule base.

15. The method of claim 11, further comprising step of authenticating a peer before accessing the peer's local rule base.

16. A method for providing peer-level access control on a network with a peer, said method comprising:

a. receiving a packet having a packet identifier;
b. searching a global pre-rule base and identifying a global pre-rule that corresponds to the packet;
c. carrying out the action of a global pre-rule if the global pre-rule corresponds to the packet;
d. accessing a local rule base of a peer;
e. if no corresponding global pre-rule is found in the global pre-rule base, searching the local rule base, identifying a local rule that corresponds to the packet, and carrying out the action of a local rule if the local rule corresponds to the packet.

17. The method of claim 16, further comprising the step of:

f. ejecting the local rule base from the filter.

18. The method of claim 17, further comprising the steps of:

g. if no corresponding global pre-rule is found in said global pre-rule base and no corresponding local rule is found in said local rule base, searching a global post-rule base for a global post-rule that corresponds to the packet; and
h. carrying out the action of a global post-rule if the global post-rule corresponds to the packet.

19. The method of claim 18, further comprising the steps of:

i. if no corresponding rule is found in the global pre-rule base and no corresponding rule is found in the local rule base, and no corresponding rule is found in the global poet-rule base, determining if the packet corresponds to a default rule; and
j. carrying out the action of the default rule if the default rule corresponds to the packet, and generating an error condition if the default rule does not correspond to the packet.

20. The method of claim 16, wherein the peer has a network address, and wherein the packet identifier comprises a packet source address and a packet destination address, and wherein a local rule comprises a rule source address, a rule destination address and an action, and wherein the local rule base having a local rule whose rule destination address corresponds to the network address of the peer is searched for a local rule that corresponds to the packet, and the action of a local rule is carried out if the local rule corresponds to the packet; comprising the steps of:

a. deriving an in-pointer by applying a hash function to the network address of the peer;

b. storing the in-pointer in a peer-in hash table such that the in-pointer points to a local rule whose rule destination address corresponds to the network destination address of the peer;

c. receiving a packet;

d. applying the hash function to the network destination address of the packet;

e. searching the local rules to which the in-pointer corresponding to the hashed packet network destination address points for a rule that corresponds to the packet; and

f. carrying out the action of a rule if the rule corresponds to the packet.

21. The method of claim 20, further comprising the step of:

g. deleting the peer's in-pointers in said local-in hash table.

22. The method of claim 16, wherein the peer has a network address, and wherein the packet identifier comprises a packet source address and a packet destination address, and wherein a local rule comprises a rule source address, a rule destination address and an action, and wherein the local rule base having a local rule whose rule source address corresponds to the network address of the peer is searched for a local rule that corresponds to the packet, and the action of a local rule is carried out if the local rule corresponds to the packet, comprising the steps of:

a. deriving an out-pointer by applying a hash function to the network address of the peer;

b. storing the out-pointer in a peer-out hash table such that the out-pointer points to a local rule whose rule source address corresponds to the network source address of the peer;

c. receiving a packet;

d. applying the hash function to the network source address of the packet;

e. searching the local rules to which the out-pointer corresponding to the hashed packet network source address points for a rule that corresponds to the packet; and

f. carrying out the action of a rule if the rule corresponds to the packet.

23. The method of claim 22, further comprising the step of:

g. deleting the peer's out-pointers in said local-out hash table.

24. A filter for providing peer-level access control on a network with a peer, said filter comprising:

a. means for authenticating a peer;

b. means for accessing rules from a peer that prescribe a PASS or DROP action to be carried out on a packet;

c. means for receiving a packet;

d. means for searching for and identifying rules that match the packet; and

e. means for carrying out the PASS or DROP action of a rule that corresponds to the packet.

25. The filter of claim 23, further comprising:

f. means for ejecting the rules of a peer.

26. The filter of claim 24, further comprising:

g. means for authenticating a peer.

FIG. 1
(PRIOR ART)

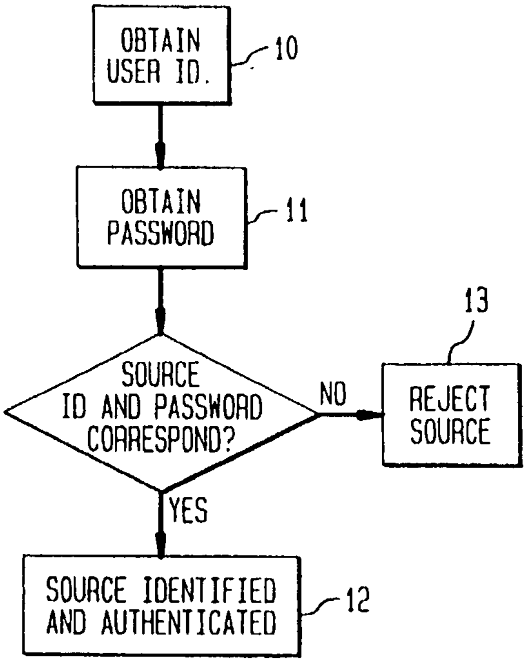

OBTAIN USER ID.
10
OBTAIN PASSWORD
11
SOURCE ID AND PASSWORD CORRESPOND?
NO
13
REJECT SOURCE
YES
SOURCE IDENTIFIED AND AUTHENTICATED
12

FIG. 2
(PRIOR ART)

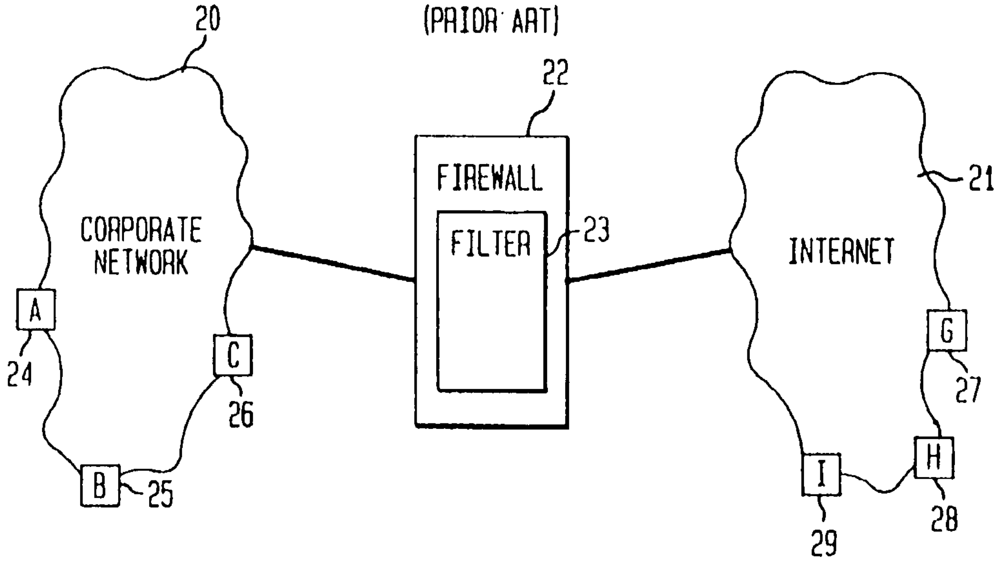


FIG. 3
(PRIOR ART)

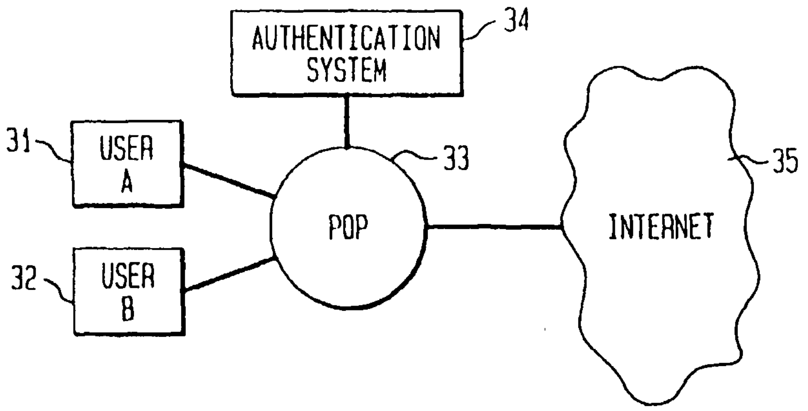


FIG. 4
(PRIOR ART)

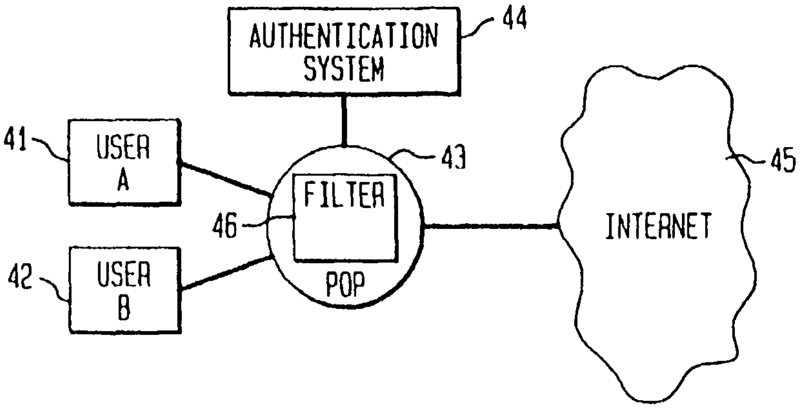


FIG. 5A
(PRIOR ART)

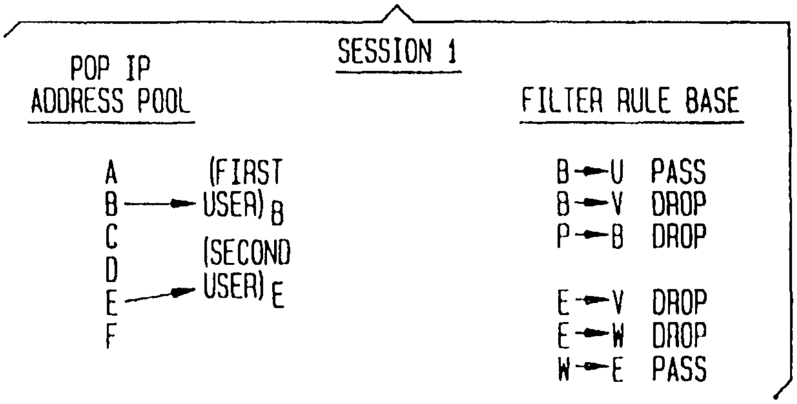


FIG. 5B
(PRIOR ART)

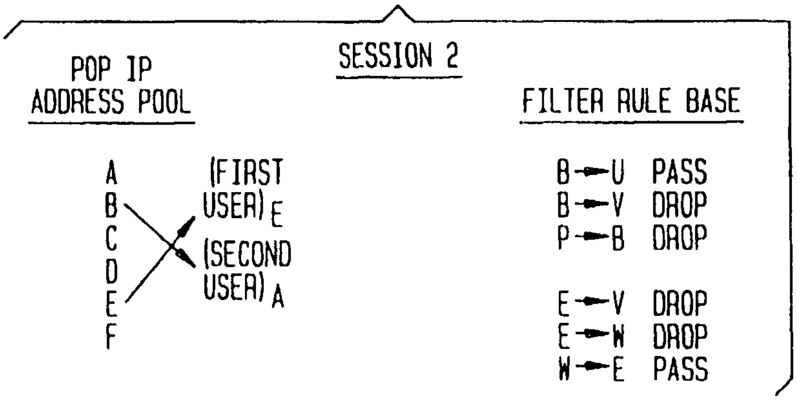


FIG. 6
(PRIOR ART)

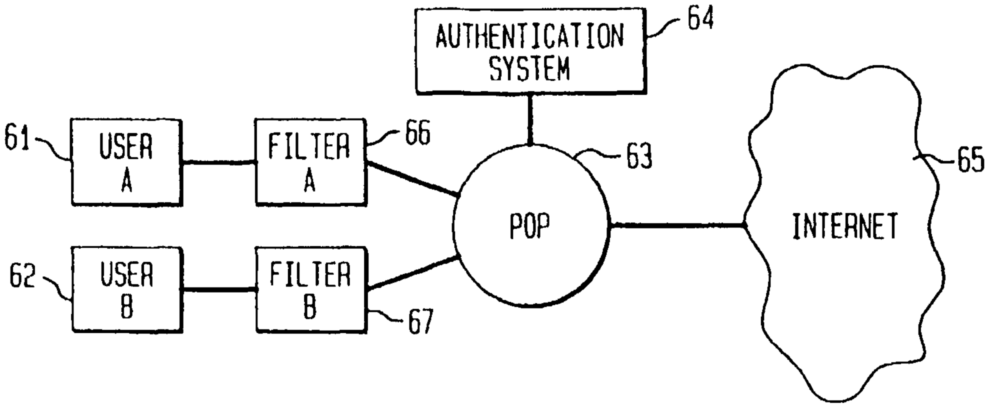


FIG. 7A

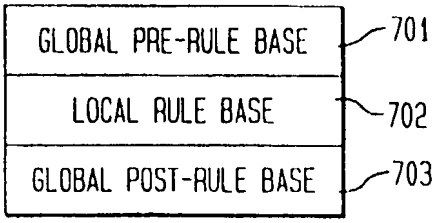

GLOBAL PRE-RULE BASE
701
LOCAL RULE BASE
702
GLOBAL POST-RULE BASE
703

FIG. 7B

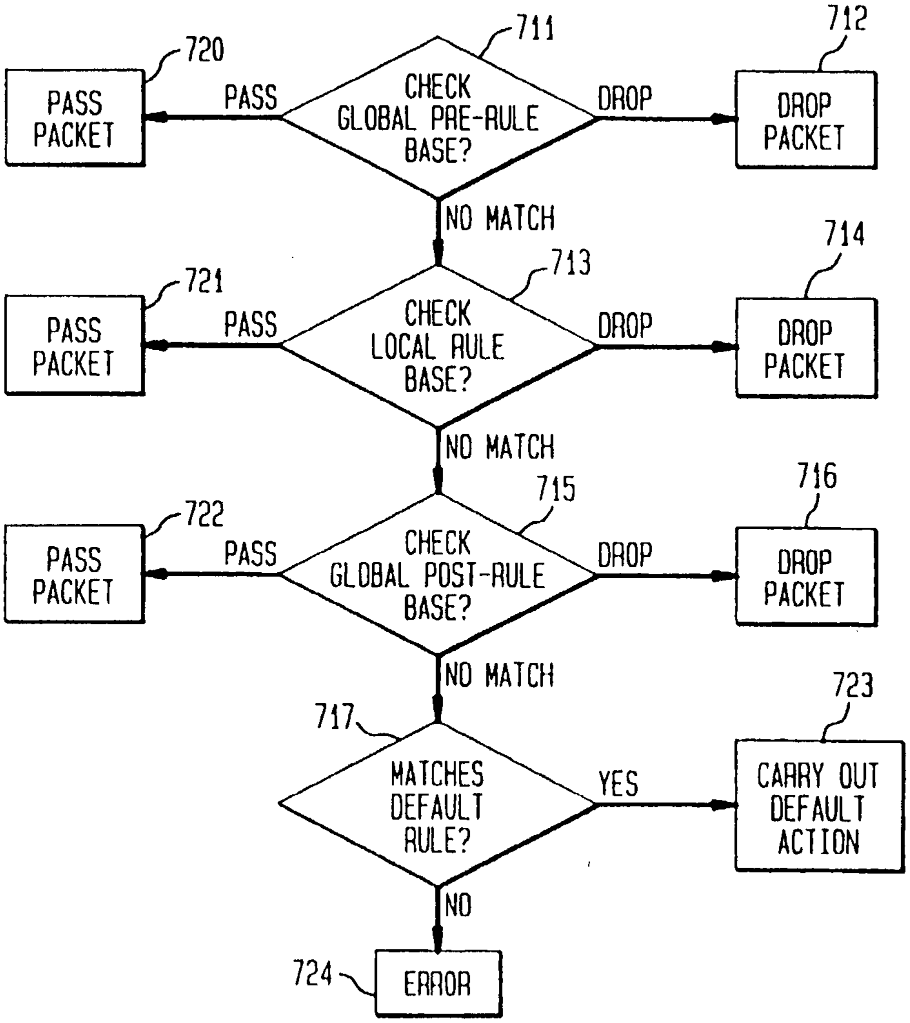

711
CHECK GLOBAL PRE-RULE BASE?
PASS
720
PASS PACKET
DROP
712
DROP PACKET
NO MATCH
713
CHECK LOCAL RULE BASE?
PASS
721
PASS PACKET
DROP
714
DROP PACKET
NO MATCH
715
CHECK GLOBAL POST-RULE BASE?
PASS
722
PASS PACKET
DROP
716
DROP PACKET
NO MATCH
717
MATCHES DEFAULT RULE?
YES
723
CARRY OUT DEFAULT ACTION
NO
724
ERROR

FIG. 8A

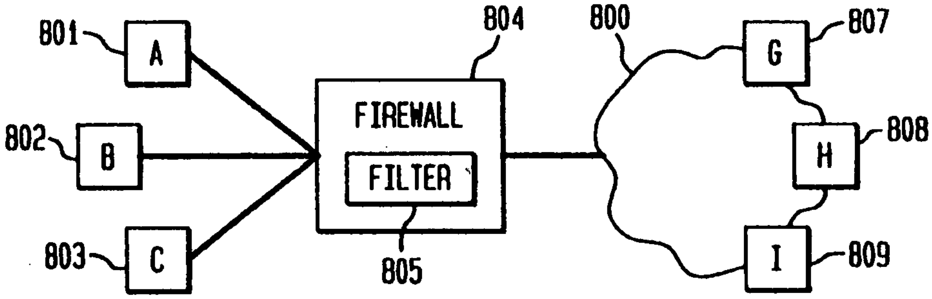


FIG. 8B

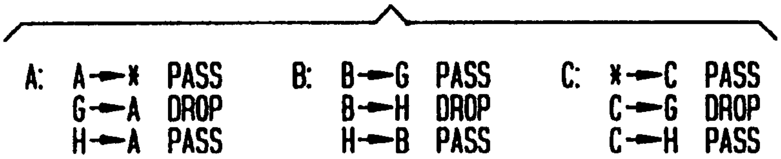


FIG. 8C

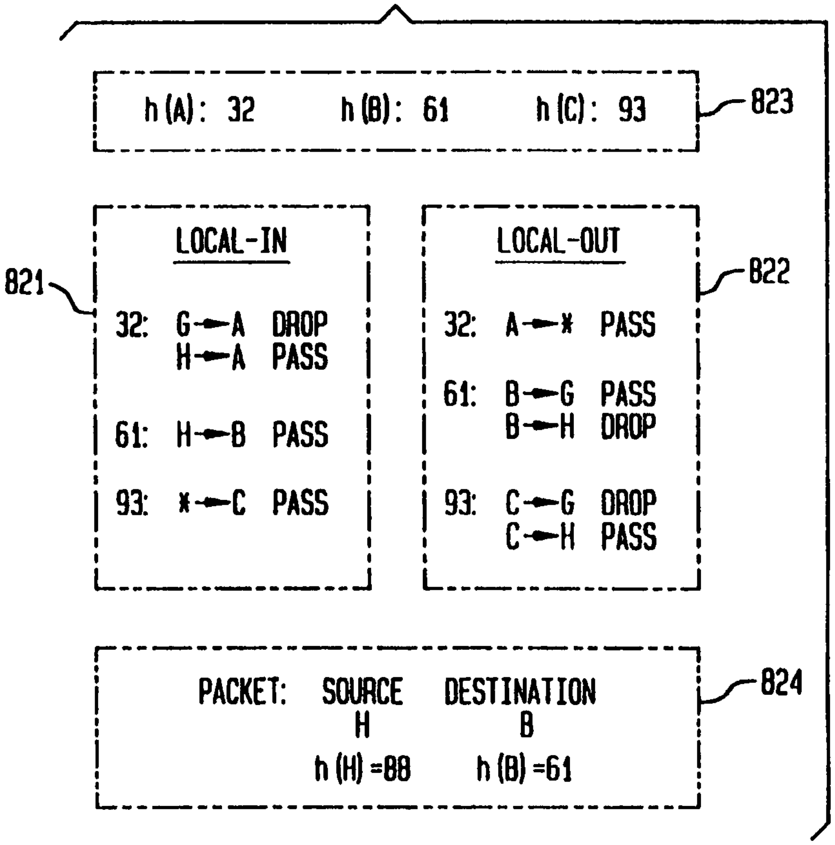


FIG. 8D

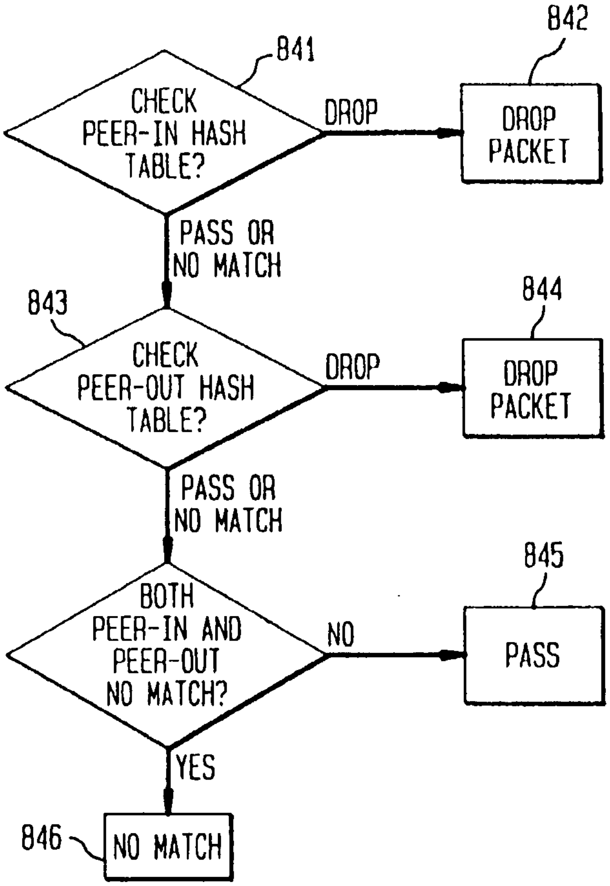
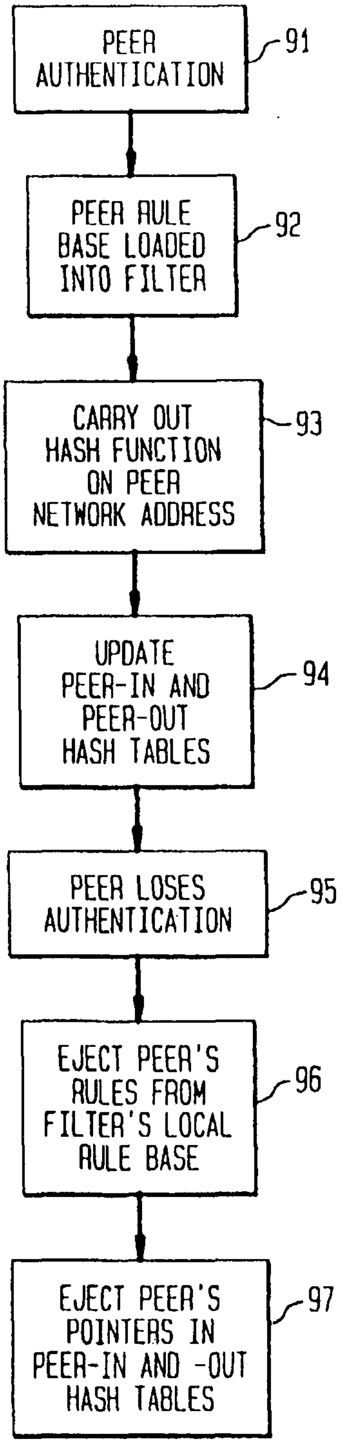

841
CHECK PEER-IN HASH TABLE?
DROP
842
DROP PACKET
PASS OR NO MATCH
843
CHECK PEER-OUT HASH TABLE?
DROP
844
DROP PACKET
PASS OR NO MATCH
BOTH PEER-IN AND PEER-OUT NO MATCH?
NO
845
PASS
YES
846
NO MATCH

FIG. 9


PEER AUTHENTICATION
91
PEER RULE BASE LOADED INTO FILTER
92
CARRY OUT HASH FUNCTION ON PEER NETWORK ADDRESS
93
UPDATE PEER-IN AND PEER-OUT HASH TABLES
94
PEER LOSES AUTHENTICATION
95
EJECT PEER'S RULES FROM FILTER'S LOCAL RULE BASE
96
EJECT PEER'S POINTERS IN PEER-IN AND -OUT HASH TABLES
97

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 0283

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 96 05549 A (SHIVA CORP)	1,4,5, 11,14, 15,24,26	H04L29/06 G06F1/00
	* page 3, line 8 - page 5, line 7 * * page 8, line 9 - page 9, line 32 *		
Y	* page 10, line 23 - page 11, line 2 * * page 12, line 28 - page 13, line 24 * * page 14, line 31 - page 15, line 21 * ---	3,13	
Y	BELLOVIN S M ET AL: "NETWORK FIREWALLS" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 50-57, XP000476555	3,13	
A	* page 52, column 1, line 60 - page 54, column 2, line 30 * ---	7,9,10, 12, 18-20,22	
A	US 5 473 607 A (HAUSMAN RICHARD J ET AL) * page 1, line 33 - line 45 * * column 2, line 47 - line 66 * * column 5, line 23 - line 40 * * column 9, line 35 - line 46 * ---	9,10,20, 22	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G06F
P,X	EP 0 762 707 A (TELIA AB) * page 2, column 1, line 34 - page 3, column 3, line 52 * -----	1-5, 11-15, 24,26	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 April 1998	Karavassilis, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

#5
7-24-00
cl

FORM PTO-1449

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Attorney Docket Number	34503/WWM
Application Number	09/295,966
Filing Date	April 21, 1999
Applicant(s)	Koichiro Ikudome, et al.
Group Art Unit	~~2766~~ 2161
Examiner Name	Not Assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	DOCUMENT NUMBER	ISSUE DATE	PATENTEE	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	COUNTRY OR PATENT OFFICE	CLASS	SUBCLASS	TRANSLATION	
						YES	NO
P.E.	WO 99/57660	11/1999	WIPO	—	—		
P.E.	WO 00/16529	3/2000	WIPO	—	—		

OTHER DOCUMENTS

EXAMINER INITIALS	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	PCT International Search Report for PCT/US99/09362

EXAMINER SIGNATURE		DATE CONSIDERED	01/22/01

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

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Sheet 1 of 1

WWM/sl
SL PAS262646.1-*-7/19/00 3:17 PM

FORM PTO-1449

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Attorney Docket Number	34503/WWM
Application Number	09/295,966
Filing Date	April 21, 1999
Applicant(s)	Koichiro Ikudome, et al.
Group Art Unit	~~2766~~ 2161
Examiner Name	Not Assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIALS	DOCUMENT NUMBER	ISSUE DATE	PATENTEE	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
P.E	5,696,898	12/1997	Baker et al.	395	187.01	

FOREIGN PATENT DOCUMENTS

EXAMINER INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	COUNTRY OR PATENT OFFICE	CLASS	SUBCLASS	TRANSLATION	
						YES	NO
P.E	WO 96/05549	02/1996	WIPO	—	—		
↓	WO 98/26548	06/1998	WIPO	—	—		
↓	EP 0 854 621	07/1998	European Patent Office	—	—		

OTHER DOCUMENTS

EXAMINER INITIALS	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

EXAMINER SIGNATURE		DATE CONSIDERED	01/22/01

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

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Sheet 1 of 1

WWM/amb
AMB PAS213840.1-*-10/22/99 2:27 PM

Form PTO 948 (Rev. 8-98) U.S. DEPARTMENT OF COMMERCE - Patent and Trademark Office Application No. 09/295966

NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

The drawing(s) filed (insert date) 4/21/99 are:
A. ☒ approved by the Draftsperson under 37 CFR 1.84 or 1.152.
B. ☐ objected to by the Draftsperson under 37 CFR 1.84 or 1.152 for the reasons indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawing must be sumitted according to the instructions on the back of this notice.

1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings: Black ink. Color.
____ Color drawings are not acceptable until petiton is granted. Fig(s) ____
____ Pencil and non black ink not permitted. Fig(s) ____
2. PHOTOGRAPHS. 37 CFR 1.84 (b)
____ 1 full-tone set is required. Fig(s) ____
____ Photographs not properly mounted (must use brystol board or photographic double-weight paper). Fig(s) ____
____ Foor quality (half-tone). Fig(s) ____
3. TYPE OF PAPER. 37 CFR 1.84(e)
____ Paper not flexible, strong, white, and durable. Fig(s) ____
____ Erasures, alterations, overwritings, interlineations, folds, copy machine marks not accepted. Fig(s) ____
____ Mylar, velum paper is not acceptable (too thin). Fig(s) ____
4. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable sizes:
____ 21.0 cm by 29.7 cm (DIN size A4)
____ 21.6 cm by 27.9 cm (8 1/2 x 11 inches)
____ All drawing sheets not the same size. Sheet(s) ____
____ Drawings sheets not an acceptable size. Fig(s) ____
5. MARGINS. 37 CFR 1.84(g): Acceptable margins:

Top 2.5 cm Left 2.5cm Right 1.5 cm Bottom 1.0 cm
SIZE: A4 Size
Top 2.5 cm Left 2.5 cm Right 1.5 cm Bottom 1.0 cm
SIZE: 8 1/2 x 11
Margins not acceptable. Fig(s) ____
____ Top (T) ____ Left (L)
____ Right (R) ____ Bottom (B)
6. VIEWS. 37 CFR 1.84(h)
REMINDER: Specification may require revision to correspond to drawing changes.
Partial views. 37 CFR 1.84(h)(2)
____ Brackets needed to show figure as one entity. Fig(s) ____
____ Views not labeled separately or properly. Fig(s) ____
____ Enlarged view not labeled separetely or properly. Fig(s) ____
7. SECTIONAL VIEWS. 37 CFR 1.84 (h)(3)
____ Hatching not indicated for sectional portions of an object. Fig(s) ____
____ Sectional designation should be noted with Arabic or Roman numbers. Fig(s) ____
8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)
____ Words do not appear on a horizontal, left-to-right fashion when page is either upright or turned so that the top becomes the right side, except for graphs. Fig(s) ____
9. SCALE. 37 CFR 1.84(k).
____ Scale not large enough to show mechanism without crowding when drawing is reduced in size to two-thirds in reproduction. Fig(s) ____
10. CHARACTER OF LINES, NUMBERS, & LETTERS. 37 CFR 1.84(l)
____ Lines, numbers & letters not uniformly thick and well defined, clean, durable, and black (poor line quality). Fig(s) ____
11. SHADING. 37 CFR 1.84(m)
____ Solid black areas pale. Fig(s) ____
____ Solid black shading not permitted. Fig(s) ____
____ Shade lines, pale, rough and blurred. Fig(s) ____
12. NUMBERS, LETTERS, & REFERENCE CHARACTERS. 37 CFR 1.84(p)
____ Numbers and reference characters not plain and legible. Fig(s) ____
____ Figure legends are poor. Fig(s) ____
____ Numbers and reference characters not oriented in the same direction as the view. 37 CFR 1.84(p)(1) Fig(s) ____
____ English alphabet not used. 37 CFR 1.84(p)(2) Figs ____
____ Numbers, letters and reference characters must be at least .32 cm (1/8 inch) in height. 37 CFR 1.84(p)(3) Fig(s) ____
13. LEAD LINES. 37 CFR 1.84(q)
____ Lead lines cross each other. Fig(s) ____
____ Lead lines missing. Fig(s) ____
14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)
____ Sheets not numbered consecutively, and in Arabic numerals beginning with number 1. Sheet(s) ____
15. NUMBERING OF VIEWS. 37 CFR 1.84(u)
____ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig(s) ____
16. CORRECTIONS. 37 CFR 1.84(w)
____ Corrections not made from prior PTO-948 dated ____
17. DESIGN DRAWINGS. 37 CFR 1.152
____ Surface shading shown not appropriate. Fig(s) ____
____ Solid black shading not used for color contrast. Fig(s) ____

COMMENTS

REVIEWER AD DATE 8/9/99 TELEPHONE NO. ____

ATTACHMENT TO PAPER NO. 6

CONTINUED PROSECUTION APPLICATION (CPA) REQUEST TRANSMITTAL

Submit an original, and a duplicate for fee processing
(Only for Continuation or Divisional applications under 37 CFR 1.53(d))

Docket No.	: 34503/WWM/A522
Inventor(s)	: Koichiro Ikudome and Moon Tai Yeung
Title	: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Express Mail Label No.	: EL366428305US Check if applicable: ___ DUPLICATE

ADDRESS TO: Assistant Commissioner for Patents
Box CPA
Washington, D.C. 20231

Date: July 19, 2000

This is a request for a continuation application under 37 CFR 1.53(d), (continued prosecution application (CPA) of prior application number 09/295.966, filed on April 21, 1999, entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM.

1. _____ Enter the unentered amendment previously filed on , under 37 CFR 1.116 in the prior nonprovisional application.

2. _____ A preliminary amendment is enclosed.

3. This application is filed by fewer than all the inventors named in the prior application, 37 CFR 1.53(d)(4).

   a. _____ DELETE the following inventor(s) named in the prior nonprovisional application:

   b. _____ The inventor(s) to be deleted are set forth on a separate sheet attached hereto.

4. Information Disclosure Statement (IDS) is enclosed:
   a. _X_ PTO-1449
   b. _X_ Copies of IDS Citations

5. Small entity status:
   a. _____ A small entity statement is enclosed.
   b. _X_ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.
   c. _____ Is no longer claimed.

6. _____ Other

CONTINUED PROSECUTION APPLICATION (CPA) REQUEST TRANSMITTAL

Submit an original, and a duplicate for fee processing

(Only for Continuation or Divisional applications under 37 CFR 1.53(d))

Docket No.: 34503/WWM/A522

FEE CALCULATIONS					
	CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	CALCULATIONS
A	TOTAL CLAIMS	29 - 20 =	9	9 x $9.00	$81.00
B	INDEPENDENT CLAIMS	4 - 3 =	1	1 x $39.00	$39.00
C	SUBTOTAL			SMALL ENTITY FEE = A + B LARGE ENTITY FEE = 2 X (A + B)	$120
D	BASIC FEE			SMALL ENTITY FEE = $345.00 LARGE ENTITY FEE = $690.00	$345
E	MULTIPLE-DEPENDENT CLAIMS FEE			SMALL ENTITY FEE = $130.00 LARGE ENTITY FEE = $260.00	
F	TOTAL FILING FEE (ADD LINES C, D, AND E)				$465
List Independent Claims: 1, 8, 15 and 26					

7. _____ A Petition for Extension of Time for the parent application and the required fee are enclosed as separate papers.

8. X Payment Enclosed: Check for $465

9. X The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required during the **entire pendency** of the application to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A duplicate copy of this sheet is enclosed.**

NOTE: The prior application's **correspondence address** will carry over to this CPA **UNLESS** a new correspondence address is provided.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By

Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/sl

#5
7-24-00
ed

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

This paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" under 37 CFR Section 1.10 Mailing Label No. EL 366428305US.

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	2766
Examiner	:	Not Assigned
Docket No.	:	34503/WWM/A522

INFORMATION DISCLOSURE STATEMENT
37 CFR § 1.97(b)

Post Office Box 7068
Pasadena, CA 91109-7068
July 19, 2000

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

In compliance with the duty of disclosure under 37 CFR §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the Manual of Patent Examining Procedure §§ 609 and 707.05(b), enclosed is FORM PTO-1449 listing the references that are known to applicant. Copies of each of the listed references are enclosed. This filing is timely because it is made during one of the periods described in 37 CFR § 1.97(b).

It is respectfully requested that the listed references be considered in the examination of this application and identified on the list of references cited on the patent issuing for this application. Applicant also requests that an initialed copy of FORM PTO-1449 be entered in the application file and returned to applicant with the next communication from the Office in accordance with MPEP § 609.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/sl
Enclosures: PTO-1449, w/references
SL PAS262596.1-*-7/19/00 3:32 PM

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 29/06, G06F 17/30

A1

(11) International Publication Number: WO 00/16529

(43) International Publication Date: 23 March 2000 (23.03.00)

(21) International Application Number: PCT/IB99/01493

(22) International Filing Date: 2 September 1999 (02.09.99)

(30) Priority Data:
60/100,114 14 September 1998 (14.09.98) US

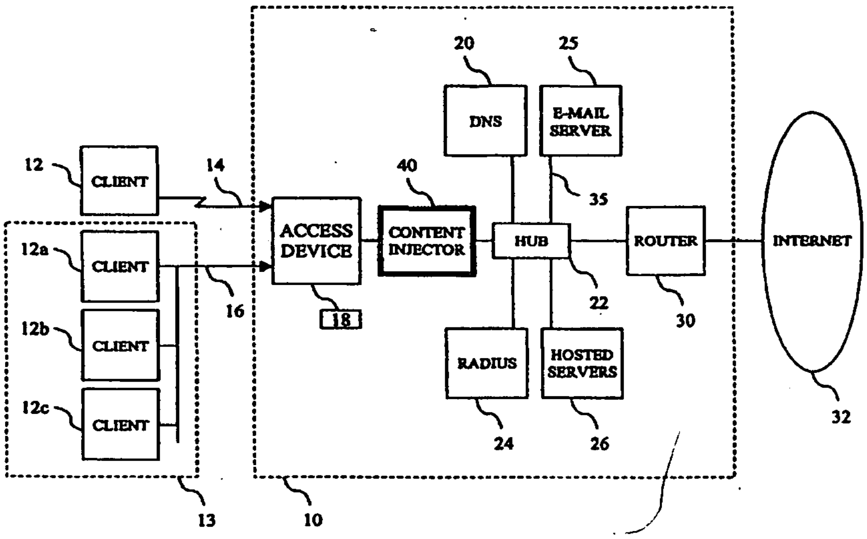
(71) Applicant: ADWISE LTD. [IL/IL]; Shaul Hamelech Boulevard 39 #B–305, 64928 Tel Aviv (IL).

(72) Inventors: YEDIDIA, Meir; Brener Street 23, 55201 Kirat Ono (IL). BOZNACH, Yaron; Dafna Street 24, 64929 Tel Aviv (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR INJECTING EXTERNAL CONTENT INTO COMPUTER NETWORK INTERACTIVE SESSIONS



(57) Abstract

A method and system for injecting external content to a user's client computer engaged in an interactive computer network session. A request for selected content from a user is intercepted and a decision is made whether to deliver external content to the user's client computer in addition to the requested content. The method and system allows for local service providers such as ISPs to add their own content to sessions involving remote content suppliers.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD AND SYSTEM FOR INJECTING EXTERNAL CONTENT INTO COMPUTER NETWORK INTERACTIVE SESSIONS

CROSS REFERENCE TO RELATED APPLICATION

This application is based on and claims priority to provisional patent application serial No. 60/100,114, filed on September 14, 1998.

BACKGROUND OF THE INVENTION

The present invention is directed generally to a system and method for injecting external customized content into an interactive computer network session, and, in particular, to such a system and method which provides the display of additional content on a user's Internet web browser other than that content actually requested by the user during an interactive session.

Presently, it is acceptable that Internet web servers contain web pages with content to be requested by a user. The requested content is generally of interest to the user, such as home pages or the like, and may often include other content, such as for example, advertisements and messages, on the same web page. Users who wish to obtain content on their client computer from a remote server through a global computer communication network such as the Internet, generally must connect through an Internet Service Provider (ISP) who serves as a connection point to the global network, such as the Internet, and provides the routers to direct the user's request to the appropriate web page server. A glossary of relevant communication and Internet terms as used herein is provided at the end of the present specification.

Currently, the ISP does not control client requests from a user, nor remote server content. Such a client request merely passes through the ISP's communication junction. Nevertheless, the ISP may have a business interest to attract its customers' attention by providing or injecting its own content during a user interactive session.

Generally, the ISP forwards client requests and remote server content in a transparent way. The ISP can encourage its customers to use its portal or ISP home page, or can use "push technology" in order to attract the client's attention and deliver content to them. Push technology implements a method in which the ISP or a third party can send special content to a user who preinstalls push client software or who preconfigures their computer/network device to receive that special content. Whether using the portal or push method, the ISP or the third party relies upon the user's full consent and cooperation in using the push client software to view the pushed content. An exemplary push product is available, for example, from Backweb Ltd. of Tel-Aviv, Israel.

Communication between devices over a network is conducted using a communication protocol. For example, communication over the Internet uses Transport Control Protocol/Internet Protocol (TCP/IP). A protocol is charted by layers as per the open system interconnection (OSI) communication layer model. Various network devices use different layers of the OSI. Certain Internet based systems extract data from a limited number of layers. Shwed U.S. Patent No. 5,606,668, for example, describes a "firewall" system based on data from two of the communication layers. A router, for example, by Cisco Inc, USA uses data from only one layer.

Typically, when a user requests content by entering an Internet address such as a Uniform Resource Location (URL) or domain name to receive a web page, there is some delay in delivering and displaying the web page on the user's web browser. The same is true when a hyperlink on a web page is activated. Judson U.S. Patent No. 5,572,643 recognizes such retrieval delay and deals with it by providing the display of information, pre-loaded or stored on the user's computer. In particular, the patent uses information embedded in the hyperlink itself to display during the delay period.

Accordingly, it would be desirable to provide content to the user when the request for a web page is made, but content provided from a source other than the web server from which the client's request for content is made.

The system and method presented herein allows for external information to be added in a controlled manner to interactive sessions conducted by local users such as an Internet user, with a remote server, without any client or servers/special setup or configuration.

SUMMARY OF THE INVENTION

Generally speaking, in accordance with the present invention, a system and method of delivering localized or external content to a user's client computer, is provided. The client computer is adapted to transmit requests for selected content and to allow downloading of requested selected content from a selected location. The request for selected content is intercepted upon delivery to the selected location. The local or external content is delivered to the user's client computer in addition to delivery of the selected content.

In a preferred embodiment, the user's client computer includes an Internet web browser for browsing the Internet by requesting selected content from a specified address location. Upon such request being received at an ISP, a decision is made based on predefined criteria whether to deliver additional content to the user's client computer. The additional content is supplied from a source other than the specified address location.

Accordingly, it is an object of the present invention to provide a system and method for inserting customized content into an interactive communication session, without changing content provided by remote sites and without having any noticeable effect on performance as it is perceived by the end-user/client.

A further object of the present invention is to provide a generic, intelligent point of intervention into interactive sessions that allows applying various intervention schemes according to end-user communications attributes and to particular activity attributes.

Another object of the present invention is to provide a method for monitoring client and server interaction, using all ISO model communication layers and acting accordingly.

Yet another object of the present invention is to provide to an ISP a method for adding content to a user's browser while processing a client request without depending on any pre-configuration/installation on the client or remote server side.

Still other objects and advantages of the invention will in part be obvious and will in part be apparent from the specification.

The invention accordingly comprises the several steps and the relation of one or more of such steps with respect to each of the others, and the system embodying features of construction, combination of elements and arrangement of parts which are adapted to effect such steps, all as exemplified in the following detailed disclosure, and the scope of the invention will be indicated in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the invention, reference is had to the following description taken in connection with the accompanying drawings, in which:

Fig. 1 is a flowchart representation of a typical global communications network in accordance with the prior art;

Fig. 2 is a flowchart representation of a global communications network in accordance with a preferred embodiment of the present invention;

Fig. 3 is a detailed flowchart representation of the content injector of Fig. 2 constructed in accordance with the present invention;

Fig. 4A depicts one manner of operation of the content injector of the present invention;

Fig. 4B depicts the various header formats for several Internet protocols;

Figs. 5 through 7 are flowchart representations depicting the steps performed by the method and system of the present invention;

Figs. 8A and 8B are flowchart representations depicting the steps performed in a sample application of the present invention;

Fig. 9A through 9C depict views which may be seen on a web browser in connection with the present invention; and,

Figs. 10A through 10C are timing charts depicting the manner in which the present invention may be used in conjunction with network idle time.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference is first made to FIG. 1 of the drawings which depicts a typical ISP junction in accordance with the prior art. In such a typical ISP junction, the main ISP site, generally indicated at 10 includes an ISP access device 18 which allows, for example, a dial-in access through a modem or the like, direct access through a router or any other communication means, thereby enabling a client 12, or a network 13 of clients 12a, 12b, 12c to connect to ISP junction 10. The site also includes a hub 22, a domain name server (DNS) 20, client access control such as a Radius 24, an e-mail server 25, hosted servers 26, and a router 30 which connects the ISP junction to global computer networks such as Internet 32. Generally, the identified named ISP devices are connected together via network such as a local area network (LAN). It is noted that the particular configuration is shown as an example only and other ISP network configurations can be used with the present invention. The arrangement and set up of such configurations are well know to those skilled in the art. The present invention, as described below in detail can be used in conjunction with any of these possible configurations.

Each client 12 is generally a computer such as a PC or laptop with video and audio capabilities, having a processor and programs or applications associated therewith. Internet

32 is a networked collection of clients and servers which are adapted through software and communication links to communicate with one another. The clients, typically through a browser program, can send a request message to a server and await a response. The response is displayed or presented by the browser. For a more detailed description of the Internet, browsers, Internet communication and protocols, reference is made to Ruvolo U.S. Patent No. 5,928,363, the description therein being incorporated by reference herein as though fully set forth.

FIG. 2 depicts the network configuration of FIG. 1 in which a content injector system, generally indicated at 40, and constructed in accordance with the present invention, has been installed. Like elements in FIG. 2 as shown in FIG. 1 have the same reference numbers. It is noted that content injector 40 is provided in ISP junction 10 in this embodiment, however, content injector 40 may also be provided in other places, such as between network 13 and ISP junction 10 or between client 12 and ISP junction 10. The present invention may be used with any of these configurations.

FIG. 3 depicts a detailed configuration of content injector 40 of FIG. 2. As shown, content injector 40 contains a gateway 42, a controller 66, two storage devices 54 and 58, a content supplier 64, which is responsible for assigning external content to the original request when needed, and a system administrator 42. Information flows on the network in the form of packets, as is well known to those skilled in the art. The location of content injector 40 in FIG. 2 is chosen so that data flow to or from a particular device of the network, such as a workstation, client access device or a router, appropriately can be controlled. Thus, packets, which flow to/from clients 12 can be controlled. The unit of the content injector 40 can be realized, for example, on a PC computer having an Intel Pentium II processor, with a 10GB hard disk and 64MB of RAM. Content injection 40 may also be an embedded CPU.

Content injector 40 operates using an "addition policy" (as hereinafter explained in detail), which is determined by system administrator 42. The addition policy determines whether to add external content to a client's content request or to pass the request transparently. The addition of the external content is accomplished without changing the original request or the requested content. The system administration configures the addition policy via a graphical interface and stores it on controller 66. An example of such a policy rule might be to add content every 10-seconds to a client request.

Another method of configuring the addition policy is by using a central policy controller which transmits a specific customized addition policy and external content to a specified ISP. The central policy controller can be located anywhere on the network, for example on a server remote from the ISP. Such a server can communicate with the content injector 40 of the ISP via the Internet connection, through a dial-up connection or any other appropriate communication system.

Communication protocols are layered, which is also referred to as a protocol stack. The ISO (International Standardization Organization) has defined a general model which provides a framework for design of communication protocol layers. This model serves as a basic reference for understanding the functionality of existing communication protocols. Different communication protocols employ different layers of the ISO model, e.g. IP protocol. A full detailed explanation of ISO model and IP protocol can be found in the book entitled: "TCP/IP Illustrated, Volume1: The Protocols" by W. Richard Stevens (Addison-Wesley Professional Computing Series 1994). A detailed explanation of TCP/IP protocol and protocols under IP can be found in the book entitled: "Internet Protocols Handbook" by Dave Roberts.

TABLE 1: ISO MODEL via IP protocol and IP protocol suite

Layer	ISO layer Functionality	IP protocol layers	IP protocol suite
7	Application	Application	HTTP, FTP, TELNET, SNMP, SMTP, NNTP
6	Presentation		
5	Session	Session	TCP,UDP
4	Transport		
3	Network	Network	IP
2	Data link		
1	Physical		

Referring to Table 1 above, layer 1 provides the physical electrical connection to a transmission medium. This layer may be the wire connection used to connect several network devices together. Layer 2 creates and controls the physical data link of communication between two end points. Layer 3 addresses network packets, e.g. Internet Protocol (IP) packets, and routes them to provide end-to-end communication between two network hosts, through intermediate hosts. Layer 4 transfers data reliably or unreliably, e.g. Transport Control Protocol (TCP) for reliable transfer or User Datagram Protocol (UDP) for unreliable transfer. Reliable transfer involves creation of a connection (a "virtual circuit") and then termination of the connection on completion of the session.

Layer 5 opens a session (a "virtual connection") between two hosts, controls the session between the two end points, and then closes the session. Layer 6 formats data to preserve its meaning. Layer 7 provides the user interface and implements the services to complete the application's purpose, e.g. File Transfer Protocol (FTP), E-MAIL, HTTP (browsing), TELNET, etc.

Content injector 40 of the present invention operates on a client request for content. A user is a person who operates a client computer/network device which is connected to the Internet Service Provider (ISP), or a computer/network device, which is connected to the above network and can interact with the network automatically or through programming. A client request for content from a remote server can be accomplished using a connected protocol, e.g. TCP, an unconnected protocol e.g. UDP, or any other protocol.

The exchanged information between server and client flows through the network in IP packets that contain higher layer protocols, which contain the client request for information or the desirable content. The process in which client and server exchange information is referred to as an "interactive session". The interactive session is characterized by an initial phase where the client initiates a content request, an information exchange phase where the client sends/receives content to/from a server, and a termination phase where the interactive session is terminated. Content can be any form of electronic information, including but not limited to text, web pages, pictures or graphics of any known format audio, computer applications or software component, files, videos, etc.

FIG. 4A depicts the manner in which content injector module 40 using a content injector module generally indicated at 220 is utilized within the ISO model. This figure shows which ISO communication layers (marked 210, 212, 214, and 216) are assigned to each task. As shown, content injector 40 uses all network layers 1-7. A client request entering the computer on which content injector 40 resides is diverted to content injector module 220. The request is received in a task 222. Task 224 checks to see if the content injector is enabled. If it is enabled, control passes to a task 226. If not enabled, the request is forwarded to its original destination via a task 228. In task 226, the request for information is verified against the content addition policy, and a determination is made whether to add external content. If the decision is to add external content, control is passed to task 230. If the decision is not to add external content, control passes to task 228 and the original request is forwarded to the destination. Task 230 adds external content to the original content request.

FIG. 4B depicts IP, TCP and UDP headers format. Using these known formats, the content injector is able to analyze a client request and to respond accordingly. This process will be illustrated using task 222 and task 226 of FIG. 4A. Task 222 receives IP packets and sorts them using the source IP address which is extracted from the IP header (layer 3 at Table 1). To identify the beginning of a new session, the content injector uses information from the flags field located in the TCP header (layers 4-5). Using OSI layers 3-5 information (Table 1), the content injector identifies a client's session initiative.

Task 226 decides if external content will be added or not using information from layer 3-7 and the pre-configured addition policy. A basic addition policy can be based on, for example:

a) Time interval (e.g. 60 seconds) implemented by using client IP address extracted from IP header (layer 3);
b) Remote host information (e.g. "port" no. 720, host name) extracted from TCP header (layers 4-5); or
c) Type of requested content by the HTTP protocol (e.g. html page, keywords, image, etc.) which is extracted from the data transported by the TCP (layers 6-7).

The above explanation also applies to FIG. 6 as described hereinafter. Additional information on Internet protocols can be found in the Stevens text referenced above.

FIGS. 5-7 depict a detailed flow diagram of the method performed by content injector module 220 of FIG. 4A. The detailed descriptions in FIGS. 5-7 further define content injector module 40.

FIG. 5 shows the process that handles a client request for content entering gateway 42 (FIG. 3). As mentioned above, a client request is assembled from IP packets, which contains upper protocols and request information. The request flows from the client to the ISP in IP packets and is received by gateway 42, which sorts and analyzes between various client requests.

'The process starts in task 43 where content injector 40 is connected and turned on. Task 41 (which generally corresponds to task 222 in FIG. 4A) receives all requests coming from clients and stores them in storage device 58 (FIG. 3). Task 164 reads the request from storage device 58 and checks to see if the content injector is enabled. If it is enabled, the request is forwarded to task 166; otherwise, the request is forwarded to its original destination at task 21, e.g. the remote server. Task 21 corresponds to task 228 of Fig. 4A. Task 166 checks to see if the request contains an "address lookup request", i.e., a DNS request. If it does, the request is forwarded to task 170 (see FIG. 7); otherwise it is forwarded, to task 168. Task 168 identifies the initial phase of the interactive session request. If content is requested, the request is forwarded to task 172 (see FIG. 6); otherwise, it is forward to its original destination 21. Task 21, after performing, returns control of the process to task 41.

FIG. 6 shows the process which handles the various client requests in which external content is added, or requests which are passed transparently. The system keeps a time-counter for each client, which is recognized by a unique IP address assigned to that client while connected to the Internet. The time-counter "decides" when to add external content to client's request. The addition is made when the client initiates a request.

Task 180 uses communication layers 2-3 to identify the beginning of the client request. The task checks the client time-counter by extracting the IP address from the client's IP packets (layer 3) by comparing them with the clients "time counter table". The "time counter table" saves updated time counter readings for each client. If the time counter indicates not to add external content, the request is directed to its original destination 21. If it indicates to add external content, the time-counter for this client is reset at task 181 and its request is directed to task 182.

Task 182 checks to see if the addition policy applies to protocols at ISO layers 4-6 for this request. Task 182 checks which application information this protocol transfers at the upper protocol layers 6-7, e.g. HTTP, FTP, and the like. The task is done by extracting information from header protocol of layers 4-5, e.g. header format (TCP,UDP), or port number (which usually associates to application protocol, e.g. HTTP, FTP, etc.). If the protocol information does not conform to the addition policy the request is directed to its original destination 21. If it does conform, the request is directed to task 188 and saved in the request table in storage 58 which contain requests to which external content might or might not be added.

Task 190 checks to see if the request application information at protocol layer 7 (which is transferred by protocols at layers 4-6) conforms to the addition policy, e.g. the adding is made at HTTP protocol request. If the application information conforms to the addition policy, external content is added at task 194. If not, the request is forwarded to task

192. Task 192 directs the client's request to retrieve its original requested content. The direction is done by forwarding the client's request to the remote server (which stored the original content) or to a location in the storage device 54 (FIG. 3) to where the original content has been transferred.

Task 194 adds external content to the client's request by a process which sends that content piggy-backed on the response for the request for the original content. The request for the original content can be done using two methods. The first method directs the original request to the remote server in which the original content is stored. The second method directs the request to a location in storage device 54, where the original content has been transferred while the external content is sent to the client. The external content is derived from content supplier 64 of Fig. 3 using client information request (at layers 1-3 plus application information) and information from content database storage 54.

FIG. 7 shows the process that handles client's address lookup request (DNS request). Task 301 receives the request after identifying it in FIG. 5, at task 166. Task 310 checks to see if it is time to add external content to client's request. The process is done in a similar way to the process that takes place in FIG 6, at task 180. If the time field in the "time counter table" indicates not to add external content, the request is directed to its original destination, namely, task 21. Otherwise, it is directed to task 302. Task 302 checks to see if the request already exists in the "lookup database table" (part of storage unit 58 in FIG. 3) by comparing the request information to the lookup database. If the request is found in the database, it is directed to its original destination, namely, task 21. Otherwise it is directed to task 304. Task 304 saves the request details in lookup database 58 while creating external content for the client's content request that is about to follow at task 305. As known in the art, a DNS request precedes a content request from a remote server. Meanwhile, the request is directed to DNS 20 at task 306.

Reference is now made to FIGS. 8A and 8B to describe a particular example using the present invention. A user of client 12 opens an Internet browser at step 350. Client 12 initiates an HTTP request by the user typing the URL of an Internet web server. e.g.: www.adwise.net, at a step 352. FIG. 9A depicts the entry of such a request in, for example, an Internet Explorer web browser from Microsoft. Alternatively, a hypertext link on the browser, or other shortcut, may be activated. Client browser 12 queries Domain Name Server (DNS) 20 to resolve the web server name to an IP address at step 354. The browser attempts to establish a session to the requested server over the Internet 32 at step 356. As is known, this attempt usually involves a certain delay.

Content injector 40 identifies the client attempt to establish a session to a remote server: www.adwise.net at step 358. Content injector 40 determines whether or not to add external content to the client session at step 374. If "no," the session is forwarded to its original destination www.adwise.net at step 376. If "yes," content injector 40 identifies itself as www.adwise.net and takes over the session, instead of forwarding the session to www.adwise.net at step 366. Content injector 40 establishes a separate session to www.adwise.net at step 362 and receives the content intended for the client at step 364, and saves the content at step 368 in storage medium 54 from Fig. 3.

In parallel to such processing, content injector 40 generates external content customized to the current session at step 374 and sends it to the client at step 372. The external content is typically a visual image or an HTML page, which is included in the HTML generated by the content injector. The client's browser receives and displays the external content at step 380. FIG. 9B depicts the client browser screen after local external content has been displayed. While displaying the external content, the browser reestablishes a session to www.adwise.net at step 382. Content injector 40 identifies this second request at step 384 and redirects the request to storage medium 54 at step 386 in which the requested content was previously received for the client. The client receives the original content at step 388. The process is repeated for each established session. The decision whether the add external content is made again as set forth above.

Referring now to FIGS. 9A, 9B, and 9C, FIG. 9A depicts a typical internet browser screen layout with the URL or domain name (host address) 400 (for example: www.adwise.net) shown entered in the address window of the browser.

FIG. 9B depicts the screen layout of FIG. 9A following the client's request for content. The external content 402 is shown, for example, as an overlay window including a clickable banner 406 containing a hyperlink. The original requested content 404 may appear (almost simultaneously) with the external content 406. In certain cases, the external content can be shown on the client browser as, for example, a clickable banner which is displayed until the original content arrives as shown in FIG. 9C. At will, the user clicks banner 406 to activate the hyperlink and receives associated content 408, shown in a new browser window.

As a further explanation to FIGS. 8A and 8B, FIGS. 10A, 10B and 10C show how content injector 40 may use network idle time for content injection. FIG. 10A shows traffic generated by the client. Time slot t0 represents client DNS request (task 354 in FIG. 8A). This request is answered by a DNS server at time slot t1 in FIG. 10B. Following the DNS request, the client initiates an HTTP request to a host (task 356). This request is represented by time slot t2 in FIG. 10A. Due to the fact that an HTTP request involves creation of a session between a client and a host, and requests processing by the host, there is a time delay until the client receives the requested content and the content is fully loaded on the client browser. This time delay is represented by time slot t8 in FIG. 10B.

FIG. 10C shows how content injector 40 utilizes the client line while waiting for the requested content. The external content is sent (task 372) between time slots t2 and t7 shown as t3 through t6 in Fig. 10C. As the content injector brings the content to the client in a separate session, the client is free to accept the external content. The external content is designed to fit the delay window between the client request and the original content arrival (task 388). It is noted that time slots t0, t1, etc. are usually unequal and depend on network performance.

A glossary of common communication and Internet expressions as used herein is set forth below:

BROWSER: A client program that allows users to read hypertext documents on the World Wide Web, and navigate between them. Examples are Netscape Navigator, Lynx, and Microsoft Internet Explorer. Browsers can be text-based or graphic.

DNS: Domain Name System. A database system that translates an IP address into a domain name. For example, a numeric IP address such as 232.452.120.54 can become a domain name such as xyz.com.

E-MAIL: Electronic mail. A service that sends messages on computers via local or global networks.

FIREWALL: An electronic boundary that prevents unauthorized users from accessing certain files on a network; or, a computer used to maintain such a boundary.

FTP: File Transfer Protocol. A client/server protocol for exchanging files with a host computer

HTTP: Hypertext Transfer Protocol. The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol

HUB: Like the hub of a wheel, a central device that connects several computers together or several networks together. A passive hub may simply forward messages; an active hub, or repeater, amplifies or refreshes the stream of data, which otherwise would deteriorate over a long distance.

IP: Internet Protocol. The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.

ISO: International Organization for Standardization. A voluntary organization founded in 1946, comprised of the national standards organizations of many countries, and responsible for creating international standards in many areas, including computers and communications. ANSI (American National Standards Institute) is the American member of ISO. ISO produced OSI (Open Systems Interconnection), a seven-layer model for network architecture.

ISP: Internet Service Provider. A company that provides Internet accounts.

LAN: Local Area Network. A network that connects computers that are close to each other, usually in the same building, linked by a cable.

NNTP: Network News Transfer Protocol. Internet protocol for connecting to Usenet newsgroups and post messages.

ROUTER: A device that finds the best path for a data packet to be sent from one network to another. A router stores and forwards electronic messages between networks, first determining all possible paths to the destination address and then picking the most expedient route, based on the traffic load and the number of hops. A router works at the network layer (layer 3 of the OSI model); a bridge works at the data link layer (layer 2). A router does more processing than a bridge does.

SMTP: Simple Mail Transfer Protocol. A server-to-server protocol for delivering electronic mail. The standard protocol used on the Internet; also used on other TCP/IP networks.

SNMP: Simple Network Management Protocol. The Internet standard protocol for network management software. Using SNMP, programs called agents monitor various devices on the network (hubs, routers, bridges, etc.).Another program collects the data from the agents. The database created by the monitoring operations is called a management information base (MIB).This data is used to check if all devices on the network are operating properly.

TCP: Transmission Control Protocol. The most common Internet transport layer protocol, defined in STD 7, RFC 793. This communications protocol is used in networks that follow U.S. Department of Defense standards. It is based on the Internet Protocol as its underlying protocol; TCP/IP means Transmission Control Protocol over Internet Protocol. TCP is connection-oriented and stream-oriented, and provides for reliable communication over packet-switched networks.

TELNET: (TN). A terminal emulation protocol that lets a user log in remotely to other computers on the Internet; it has a command line interface. Originally developed for ARPAnet, Telnet runs on top of the TCP/IP protocol.

UDP: User Datagram Protocol. A communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Like TCP (Transmission Control Protocol), UDP is used with IP (the Internet Protocol).Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.

Accordingly, the present invention provides a system and method of injecting external content into a client/server interactive session, such as a web browsing session, without interfering with regular communications. The content can be selectively customized and provide advertisements, information, news and the like, especially during the normal period of delay between a request for a particular web page and its actual delivery and loading.

It will thus be seen that the objects set forth above, among those made apparent from the preceding description, are efficiently attained and, since certain changes may be made in carrying out the above methods and in the systems set forth without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention which, as a matter of language, might be said to fall therebetween.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for injecting external content into a computer network interactive session comprising the steps of:

receiving an electronic request from a client for specified content from a specified address location;

determining based on predetermined criteria whether to deliver external content to said client;

upon determining to deliver external content, transmitting said external content to said client and transmitting said specified content request to its specified address location for response; and

upon determining not to deliver external content, transmitting said specified content request to its specified address location for response.

2. The method for injecting external content as claimed in claim 1, wherein said predetermined criteria includes an addition policy.

3. The method for injecting external content as claimed in claim 2, wherein said addition policy uses at least one of a time interval, remote host information and type of requested content to determine whether to deliver external content to said client.

4. The method for injecting external content as claimed in claim 1, further comprising the step of storing said received electronic request in a storage device.

5. The method for injecting external content as claimed in claim 4, wherein said predetermined criteria includes whether an electronic request is similar to a stored electronic request.

6. The method for injecting external content as claimed in claim 2, further comprising the steps of receiving said specified content from said specified address location and storing said specified content.

7. The method for injecting external content as claimed in claim 6, further comprising the step of modifying said stored specified content with said external content.

8. The method for injecting external content as claimed in claim 7, further comprising the step of transmitting said modified stored specified content to said client as a response to said electronic request for specified content.

9. The method for injecting external content as claimed in claim 6, further comprising the step of delivering said stored specified content to said client.

10. The method for injecting external content as claimed in claim 9, further comprising the step of displaying said external content at said client until said specified content is delivered to said client.

11. The method for injecting external content as claimed in claim 9, further comprising the step of displaying said external content at said client for a predetermined time.

12. The method for injecting external content as claimed in claim 9, further comprising the step of displaying said external content at said client along with said specified content.

13. The method for injecting external content as claimed in claim 10, wherein said client is a computer having a display device.

14. The method for injecting external content as claimed in claim 11, wherein said client is a computer having a display device.

15. The method for injecting external content as claimed in claim 1, wherein said electronic request received from said client is in the form of a packet.

16. The method for injecting external content as claimed in claim 15 wherein said packet includes at least one of a content type information and a specified address location information.

17. A method of browsing in a computer network having at least one client computer electronically connectable to the Internet, said client computer being adapted to transmit requests for selected content to a specified address location and to allow downloading of requested selected content from said location on the Internet, comprising the steps of:

receiving a request for selected content from a client computer, said selected content being located at a specified address location;

intercepting said request for selected content upon delivery to said location;

selectively delivering external content in addition to said selected content to said client computer for display; and

transmitting said request for said selected content to said location.

18. The method of browsing as claimed in claim 17, further comprising the step of receiving said selected content.

19. The method of browsing as claimed in claim 18, further comprising the step of delivering said selected content to said client computer.

20. The method of browsing as claimed in claim 18, further comprising the step of storing said selected content after receipt.

21. The method of browsing as claimed in claim 18, further comprising the step of piggy-backing said external content to said received selected content.

22. The method of browsing as claimed in claim 17, wherein a computer network delay occurs over the Internet, said external content being delivered to said client computer during said delay.

23. The method of browsing as claimed in claim 17, further comprising the step of delaying delivery of said selected content to said client computer until after said external content is delivered to said client computer.

24. The method of browsing as claimed in claim 17, wherein said external content is delivered to said client computer without changing said request for selected content.

25. The method of browsing as claimed in claim 24, wherein said external content is delivered to said client computer without changing said selected content.

26. An automated system which allows for the delivery of external content to a web browser of a client coupled to the Internet through an ISP, comprising an ISP junction which receives a request for a web page directed to a specified address from said client, said ISP junction including a content injector, said content injector including access to an addition determining system which selectively determines when to deliver external content to said client based on predetermined criteria, and a transmission system which transmits said request for a web page to the specified address.

27. The automated system as claimed in claim 26, wherein said content injector includes a system administrator.

28. The automated system as claimed in claim 26, wherein said content injector is a computer.

29. The automated system as claimed in claim 26, wherein said content injector is an embedded CPU.

30. The automated system as claimed in claim 26, wherein said content injector further includes external content for delivery to said client computer.

31. The automated system as claimed in claim 26, wherein said addition determining system uses an addition policy to determine whether to deliver external content to said client.

32. The automated system as claimed in claim 31, wherein said addition policy uses at least one of a time interval, remote host information and type of requested content to determine whether to deliver external content to said client.

33. The automated system as claimed in claim 26, wherein said addition determining system is remotely located from said ISP.

34. The automated system as claimed in claim 31, where said addition determining system uses a central policy controller to configure said addition policy.

35. The automated system as claimed in claim 26, wherein said content injector takes over control of a network session of said client over the Internet.

36. The automated system as claimed in claim 26, wherein said content injector further includes a transmission system for transmitting said external content to said client.

37. A system for injecting external content into a computer network interactive session, comprising:

a content injector including a processor, electronic storage and a gateway, said storage including external content information;

said gateway including means for reading information packets transmitted from a client during a network interactive session, said packets including request information;

said processor determining whether to deliver external content to said client by comparing said request information to predetermined criteria.

38. The system as claimed in claim 37, wherein said content injector further includes means for transmitting said external content to said client.

39. The system as claimed in claim 38, wherein said content injector further includes means for transmitting requested content to said client, said requested content associated with said request information.

40. The system as claimed in claim 39, wherein said content injector further includes means for adding a delay period of time before at least one of said transmitting said external content to said client and said transmitting requested content to said client.

41. The system as claimed in claim 37 further comprising a central policy controller which controls when to deliver external content to said client.

42. The system as claimed in claim 41, where said central policy controller is located remotely from said content injector.

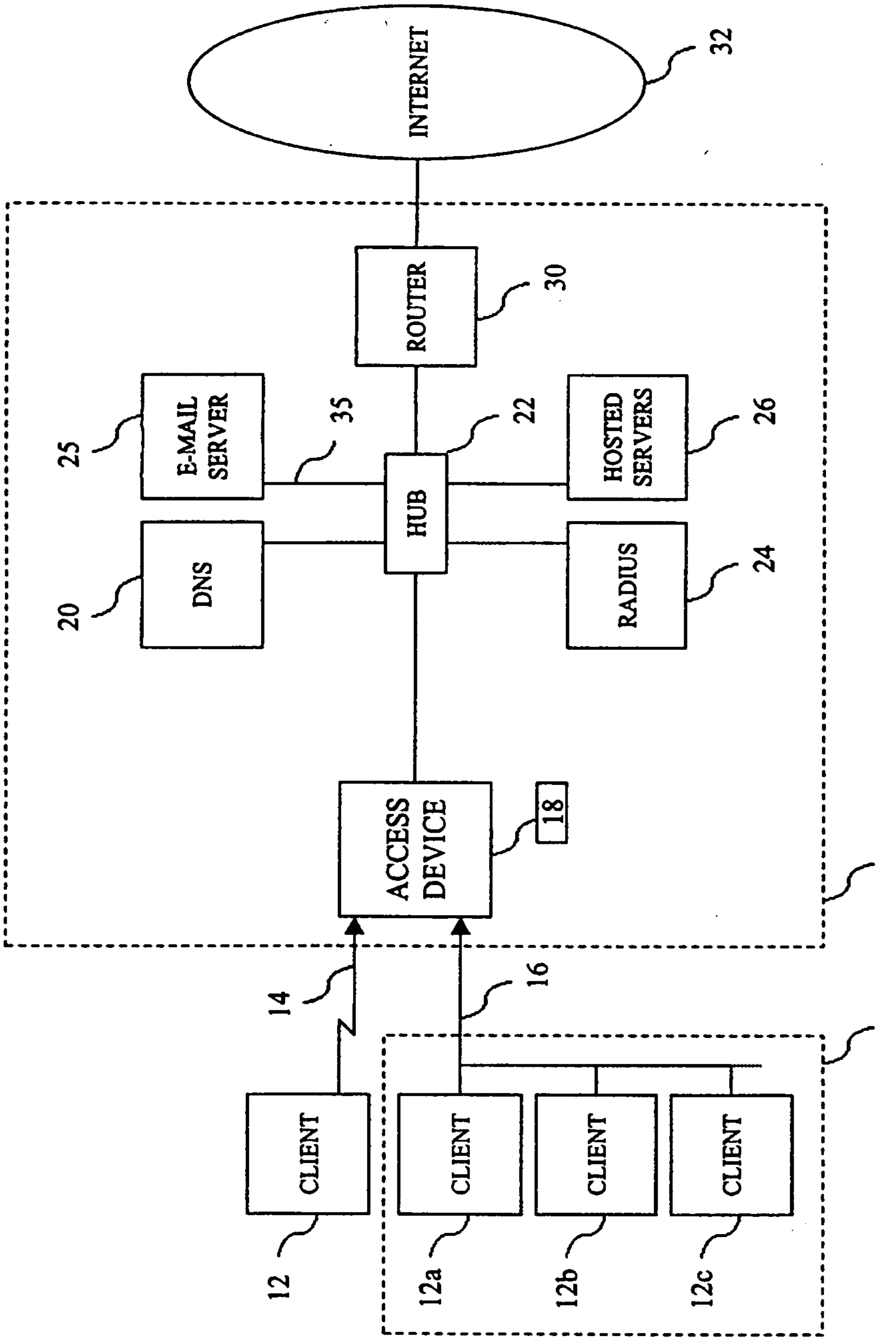


Fig. 1 (PRIOR-ART)

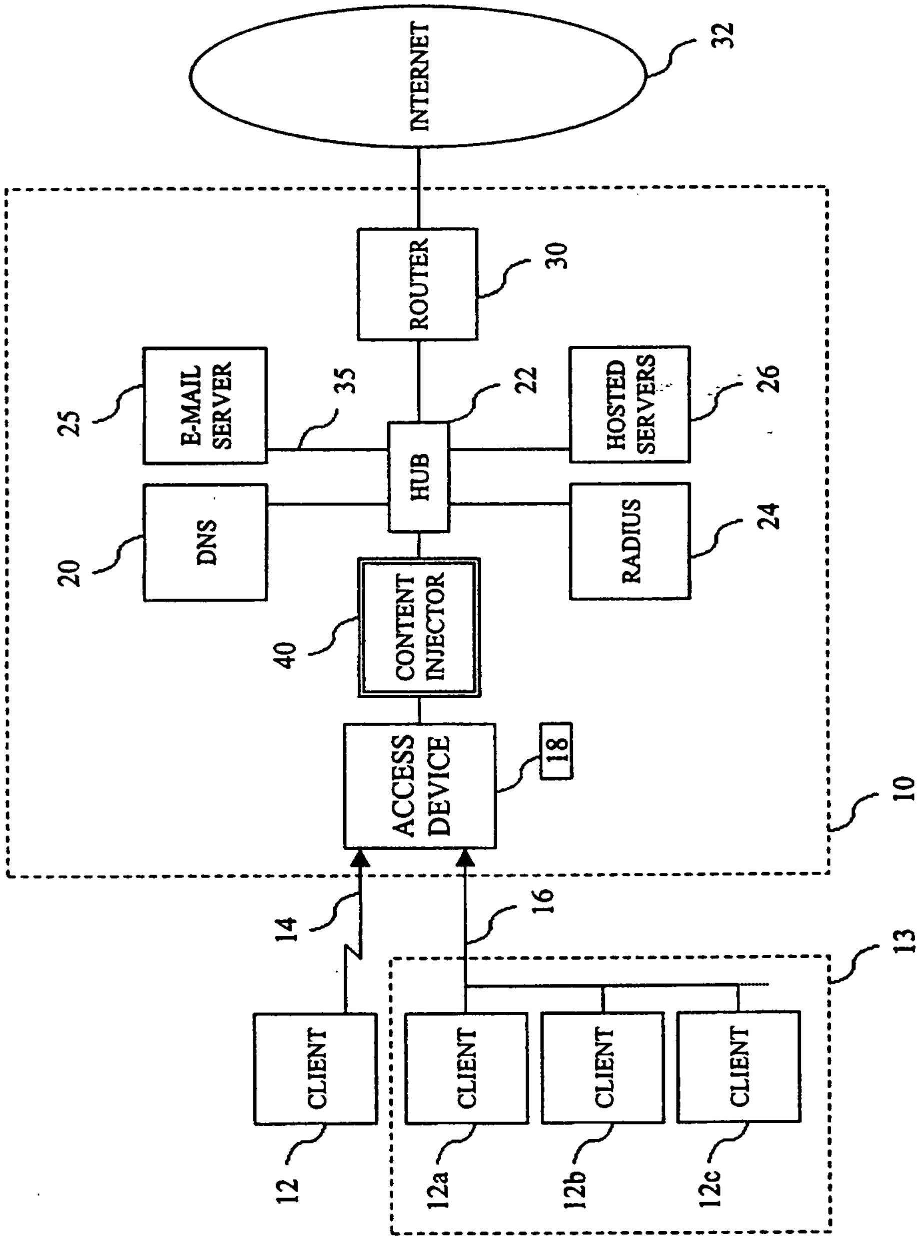

INTERNET
32
ROUTER
30
E-MAIL SERVER
25
35
HUB
22
HOSTED SERVERS
26
DNS
20
RADIUS
24
CONTENT INJECTOR
40
ACCESS DEVICE
18
10
14
16
13
CLIENT
12
CLIENT
12a
CLIENT
12b
CLIENT
12c

Fig. 2

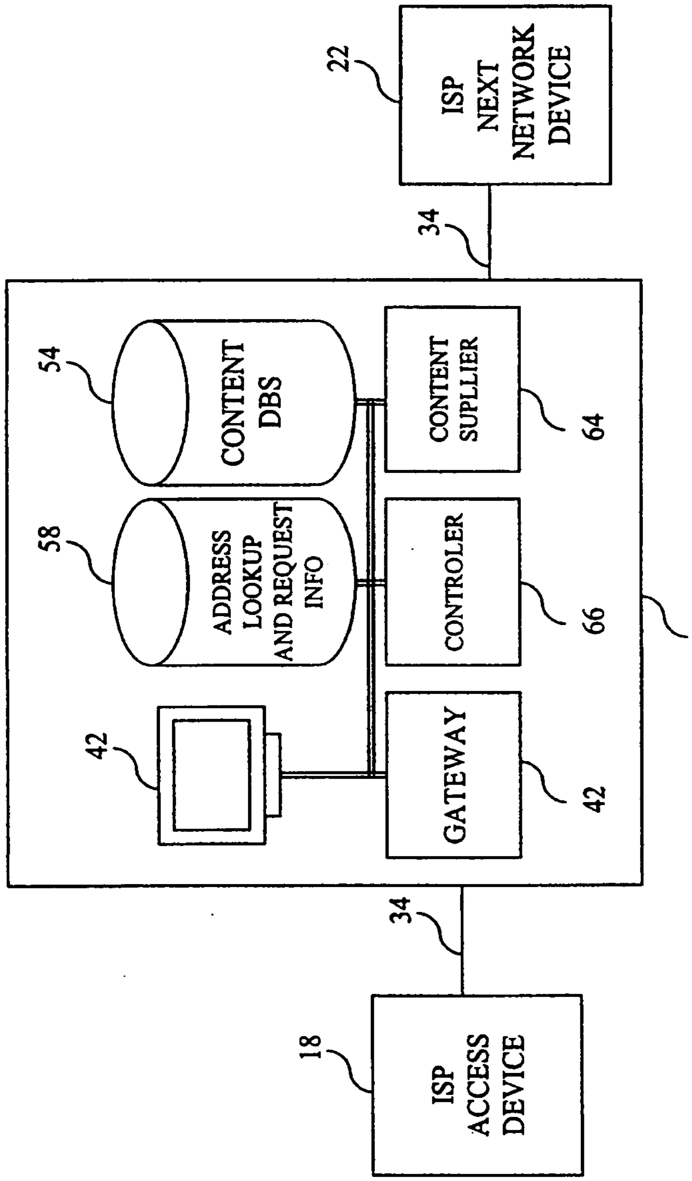

18
ISP ACCESS DEVICE
34
42
GATEWAY
42
58
ADDRESS LOOKUP AND REQUEST INFO
CONTROLER
66
40
54
CONTENT DBS
CONTENT SUPLLIER
64
34
22
ISP NEXT NETWORK DEVICE

Fig. 3

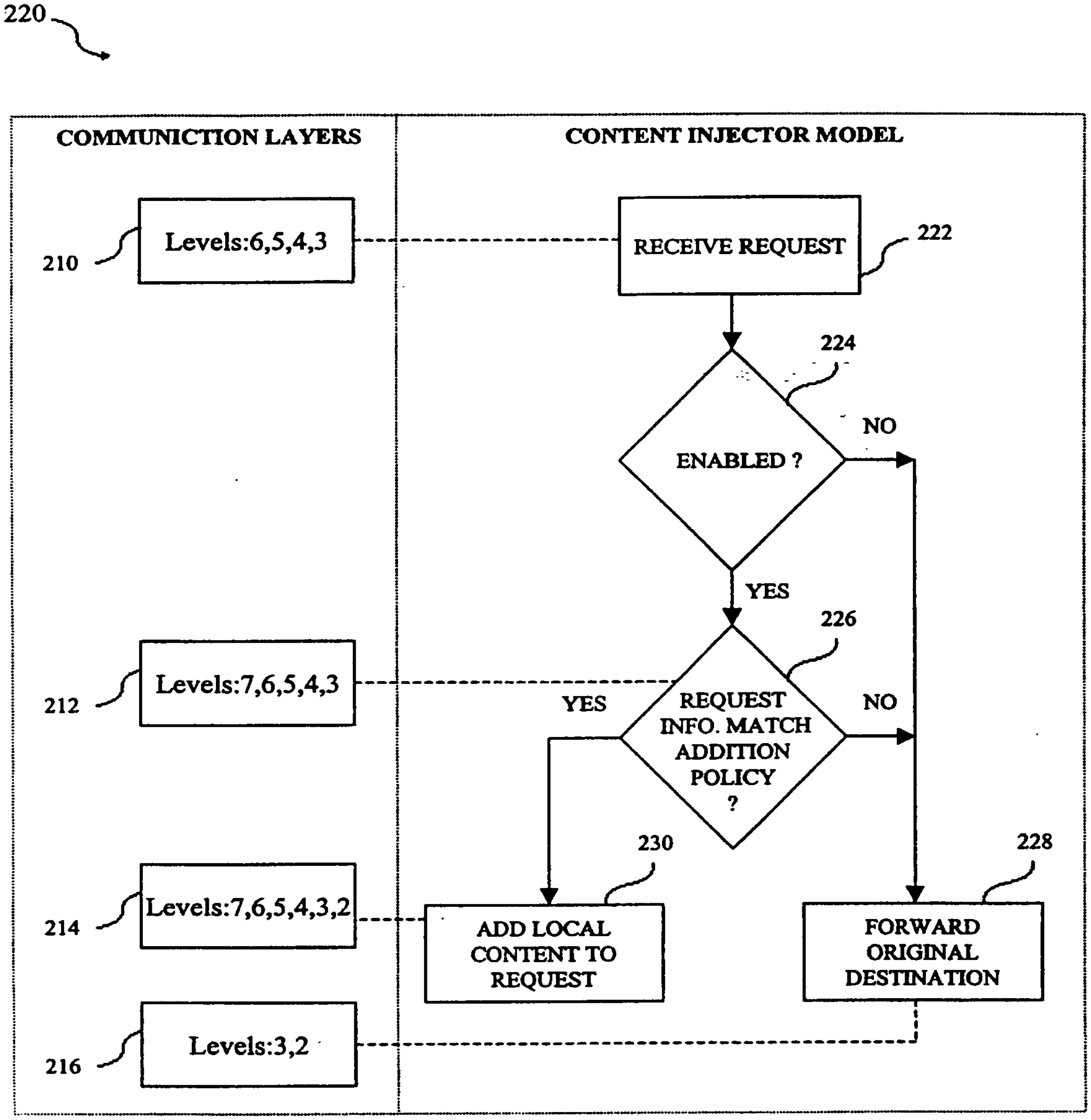

220
COMMUNICTION LAYERS
CONTENT INJECTOR MODEL
210
Levels:6,5,4,3
RECEIVE REQUEST
222
224
ENABLED ?
NO
YES
226
212
Levels:7,6,5,4,3
YES
REQUEST INFO. MATCH ADDITION POLICY ?
NO
230
228
214
Levels:7,6,5,4,3,2
ADD LOCAL CONTENT TO REQUEST
FORWARD ORIGINAL DESTINATION
216
Levels:3,2

Fig. 4A

IP Header

<table>
<tr><td>4 bit version</td><td>4 bit header length</td><td>8 bit type of service (TSO)</td><td colspan="2">16-bit total length (in bytes)</td></tr>
<tr><td colspan="3">16-bit identification</td><td>3- bit flags</td><td>13-bit fragment offset</td></tr>
<tr><td colspan="2">8-bit time to live (TTL)</td><td>8-bit protocol</td><td colspan="2">16-bit header checksum</td></tr>
<tr><td colspan="5">32-bit source IP address</td></tr>
<tr><td colspan="5">32-bit destination IP address</td></tr>
<tr><td colspan="5">Options (if any)</td></tr>
<tr><td colspan="5">data</td></tr>
</table>

UDP Header

<table>
<tr><td>16-bit source port number</td><td>16-bit destination port number</td></tr>
<tr><td>16-bit UDP length</td><td>16-bit UDP checksum</td></tr>
<tr><td colspan="2">Data (if any)</td></tr>
</table>

TCP Header

<table>
<tr><td colspan="3">16-bit source port number</td><td>16-bit destination port number</td></tr>
<tr><td colspan="4">32-bit sequence number</td></tr>
<tr><td colspan="4">32-bit acknowledgment</td></tr>
<tr><td>4 bit header length</td><td>reserved (6 bits)</td><td>flags</td><td>16-bit window size</td></tr>
<tr><td colspan="3">16-bit TCP checksum</td><td>16-bit urgent pointer</td></tr>
<tr><td colspan="4">Options (if any)</td></tr>
<tr><td colspan="4">Data (if any)</td></tr>
</table>

Fig. 4B

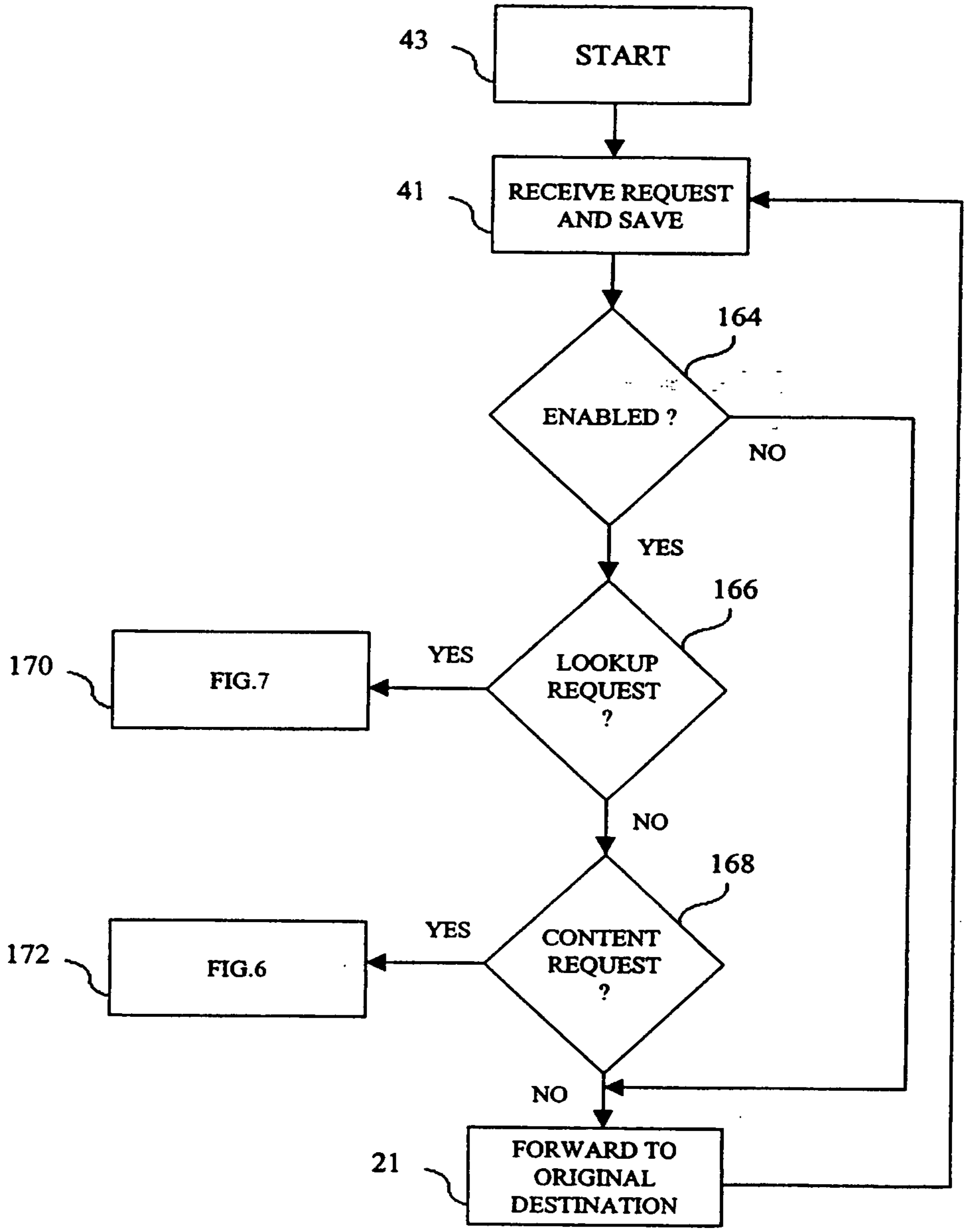

43
START
41
RECEIVE REQUEST AND SAVE
164
ENABLED ?
NO
YES
166
LOOKUP REQUEST ?
YES
170
FIG.7
NO
168
CONTENT REQUEST ?
YES
172
FIG.6
NO
21
FORWARD TO ORIGINAL DESTINATION

Fig. 5

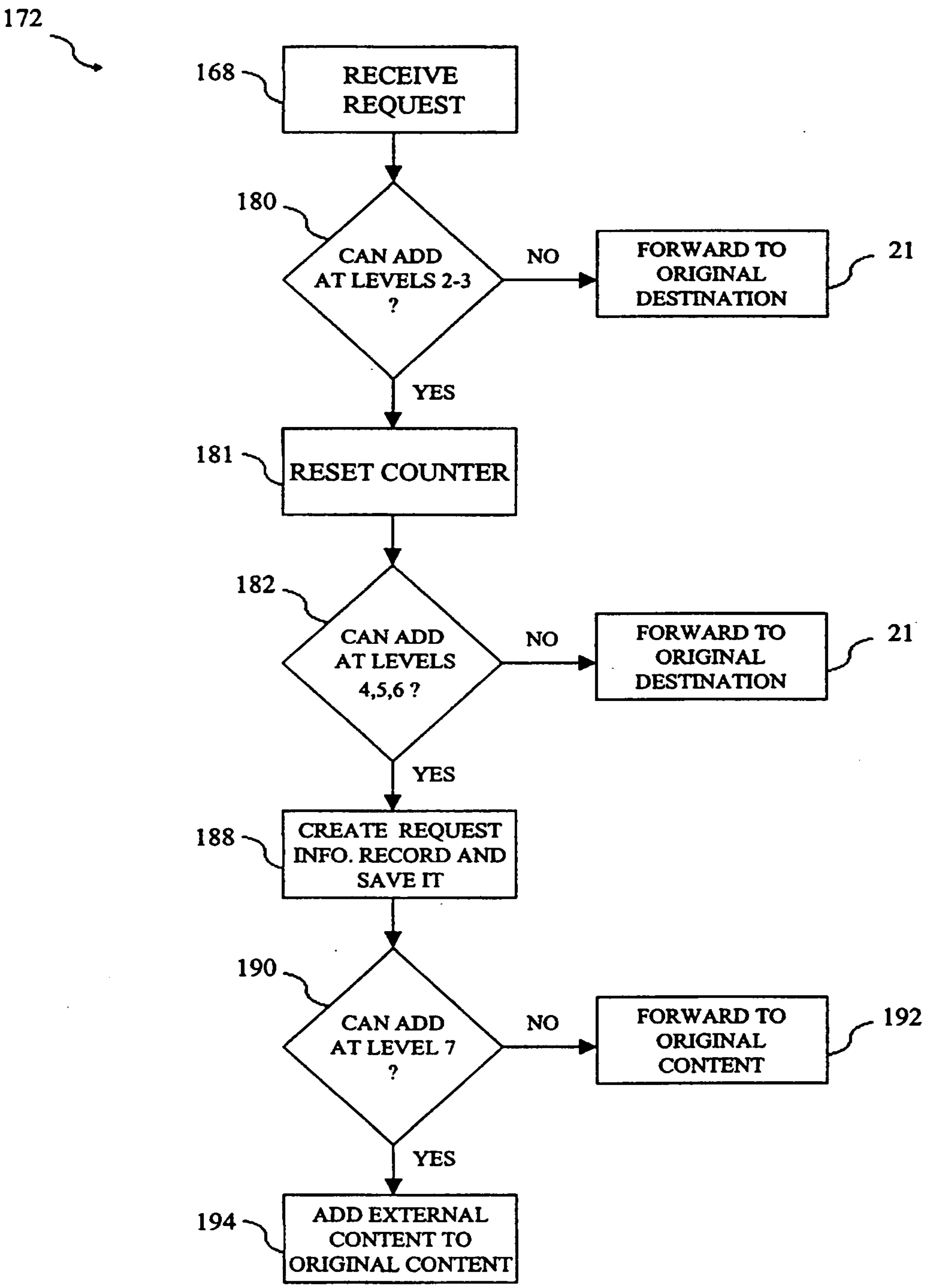

172
168
RECEIVE REQUEST
180
CAN ADD AT LEVELS 2-3 ?
NO
FORWARD TO ORIGINAL DESTINATION
21
YES
181
RESET COUNTER
182
CAN ADD AT LEVELS 4,5,6 ?
NO
FORWARD TO ORIGINAL DESTINATION
21
YES
188
CREATE REQUEST INFO. RECORD AND SAVE IT
190
CAN ADD AT LEVEL 7 ?
NO
FORWARD TO ORIGINAL CONTENT
192
YES
194
ADD EXTERNAL CONTENT TO ORIGINAL CONTENT

Fig. 6

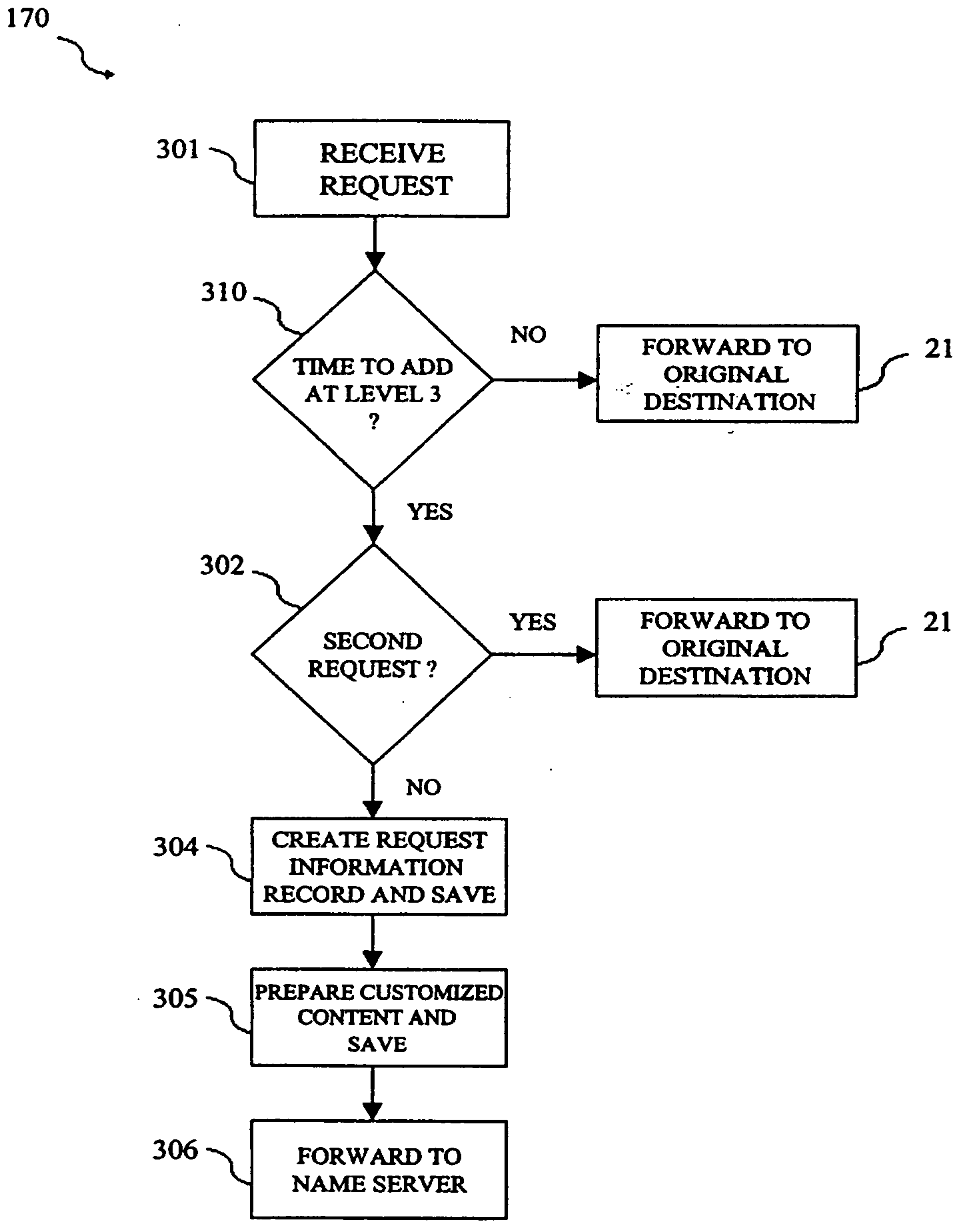

170
301
RECEIVE REQUEST
310
TIME TO ADD AT LEVEL 3 ?
NO
FORWARD TO ORIGINAL DESTINATION
21
YES
302
SECOND REQUEST ?
YES
FORWARD TO ORIGINAL DESTINATION
21
NO
304
CREATE REQUEST INFORMATION RECORD AND SAVE
305
PREPARE CUSTOMIZED CONTENT AND SAVE
306
FORWARD TO NAME SERVER

Fig. 7

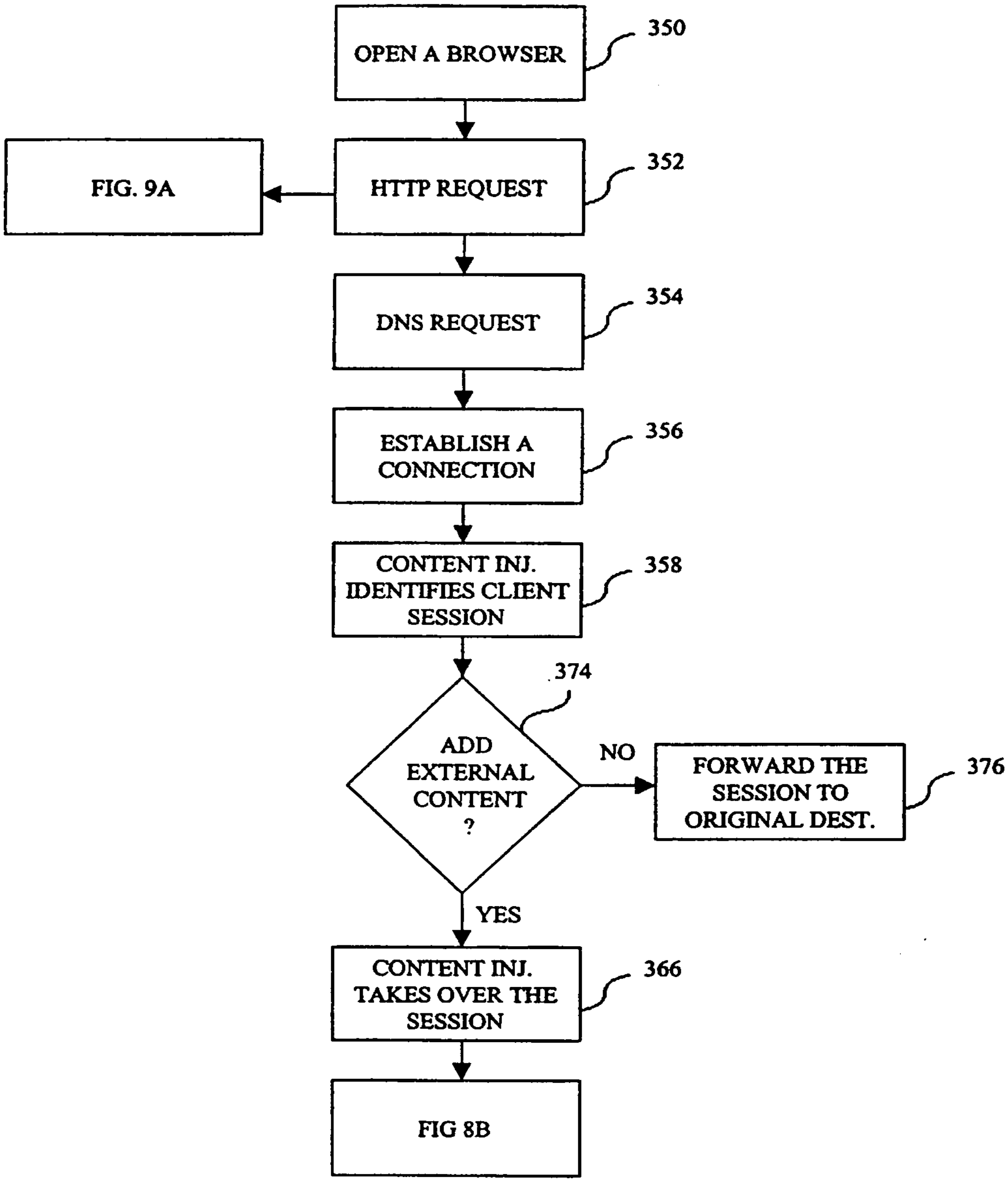

OPEN A BROWSER
350
FIG. 9A
HTTP REQUEST
352
DNS REQUEST
354
ESTABLISH A CONNECTION
356
CONTENT INJ. IDENTIFIES CLIENT SESSION
358
374
ADD EXTERNAL CONTENT ?
NO
FORWARD THE SESSION TO ORIGINAL DEST.
376
YES
CONTENT INJ. TAKES OVER THE SESSION
366
FIG 8B

Fig. 8A

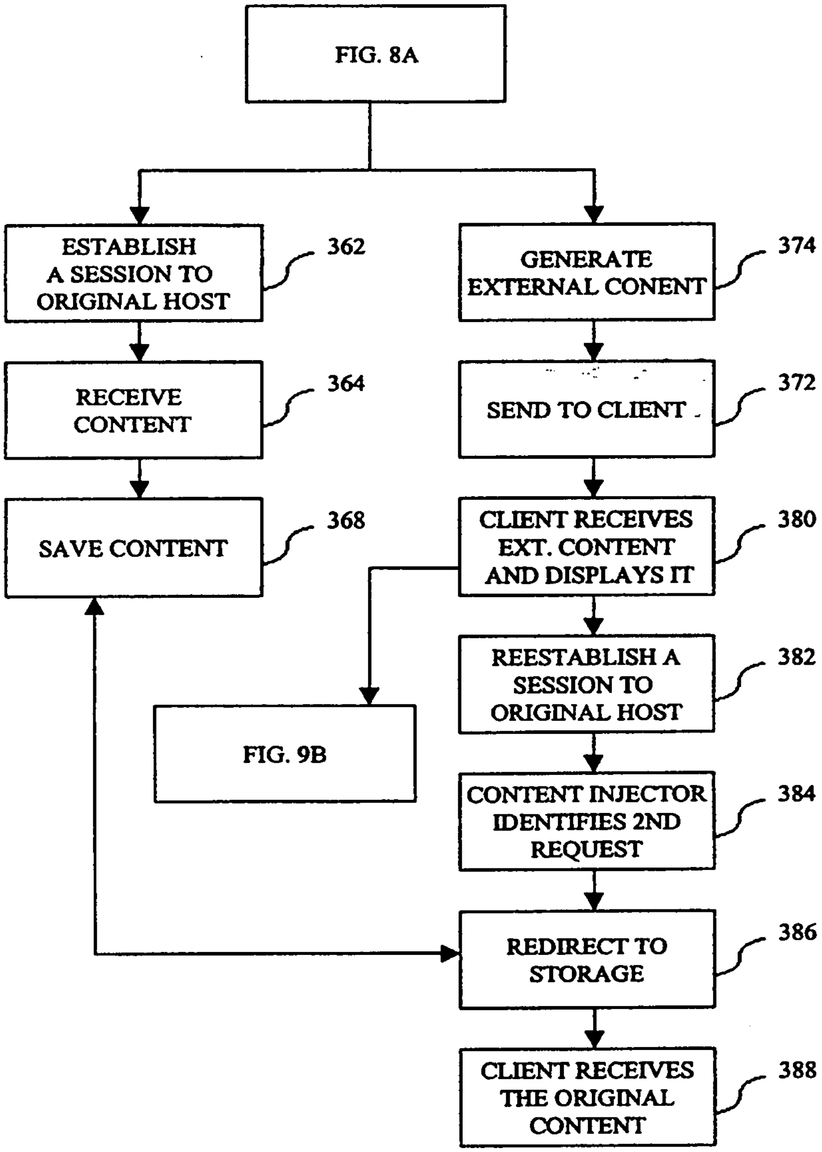


FIG. 8A
ESTABLISH A SESSION TO ORIGINAL HOST
362
RECEIVE CONTENT
364
SAVE CONTENT
368
GENERATE EXTERNAL CONENT
374
SEND TO CLIENT
372
CLIENT RECEIVES EXT. CONTENT AND DISPLAYS IT
380
FIG. 9B
REESTABLISH A SESSION TO ORIGINAL HOST
382
CONTENT INJECTOR IDENTIFIES 2ND REQUEST
384
REDIRECT TO STORAGE
386
CLIENT RECEIVES THE ORIGINAL CONTENT
388

Fig. 8B

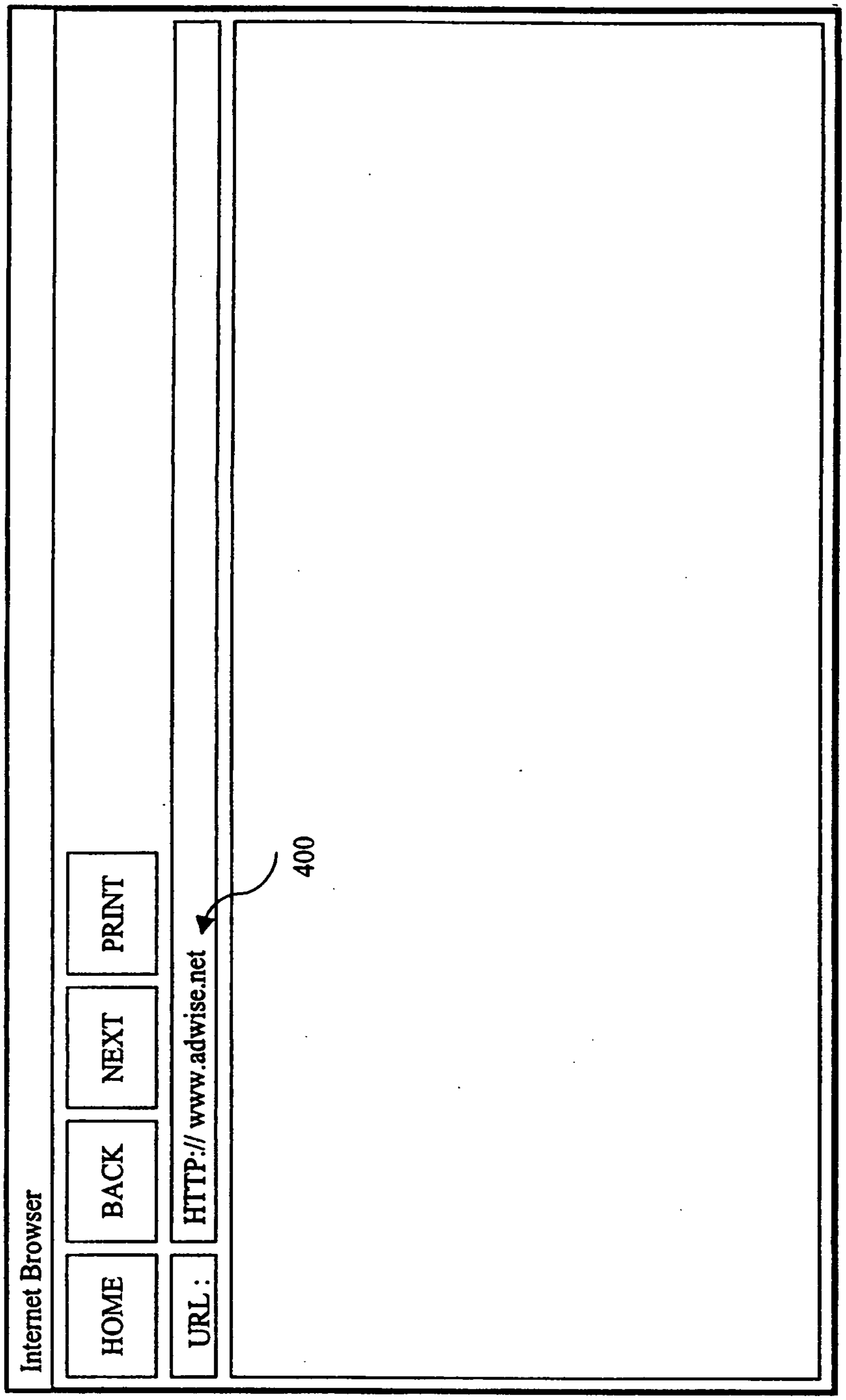

Internet Browser
HOME
BACK
NEXT
PRINT
URL :
HTTP:// www.adwise.net
400

Fig. 9A

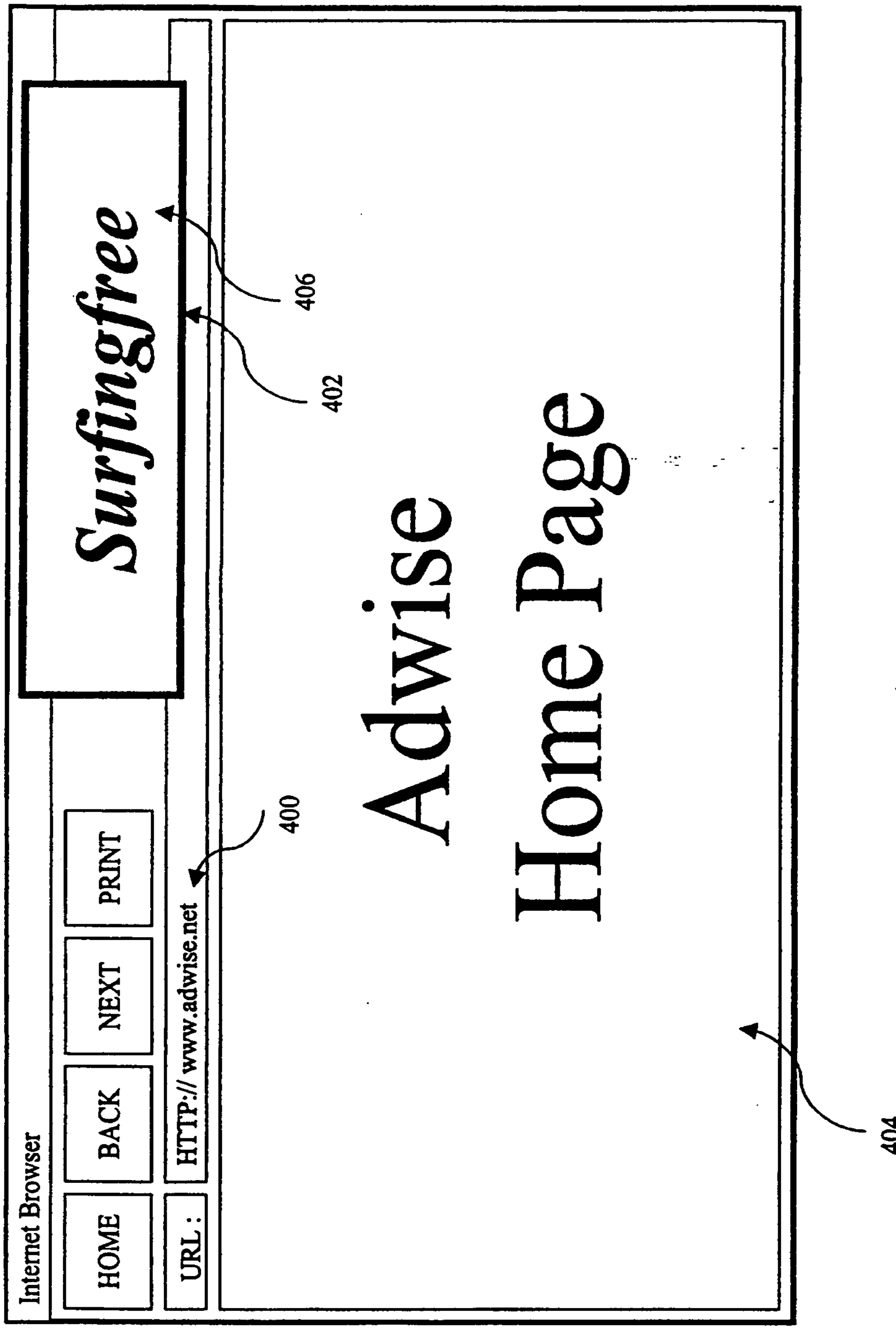

Internet Browser
HOME
BACK
NEXT
PRINT
URL :
HTTP:// www.adwise.net
Surfingfree
Adwise
Home Page
400
402
404
406

Fig. 9B

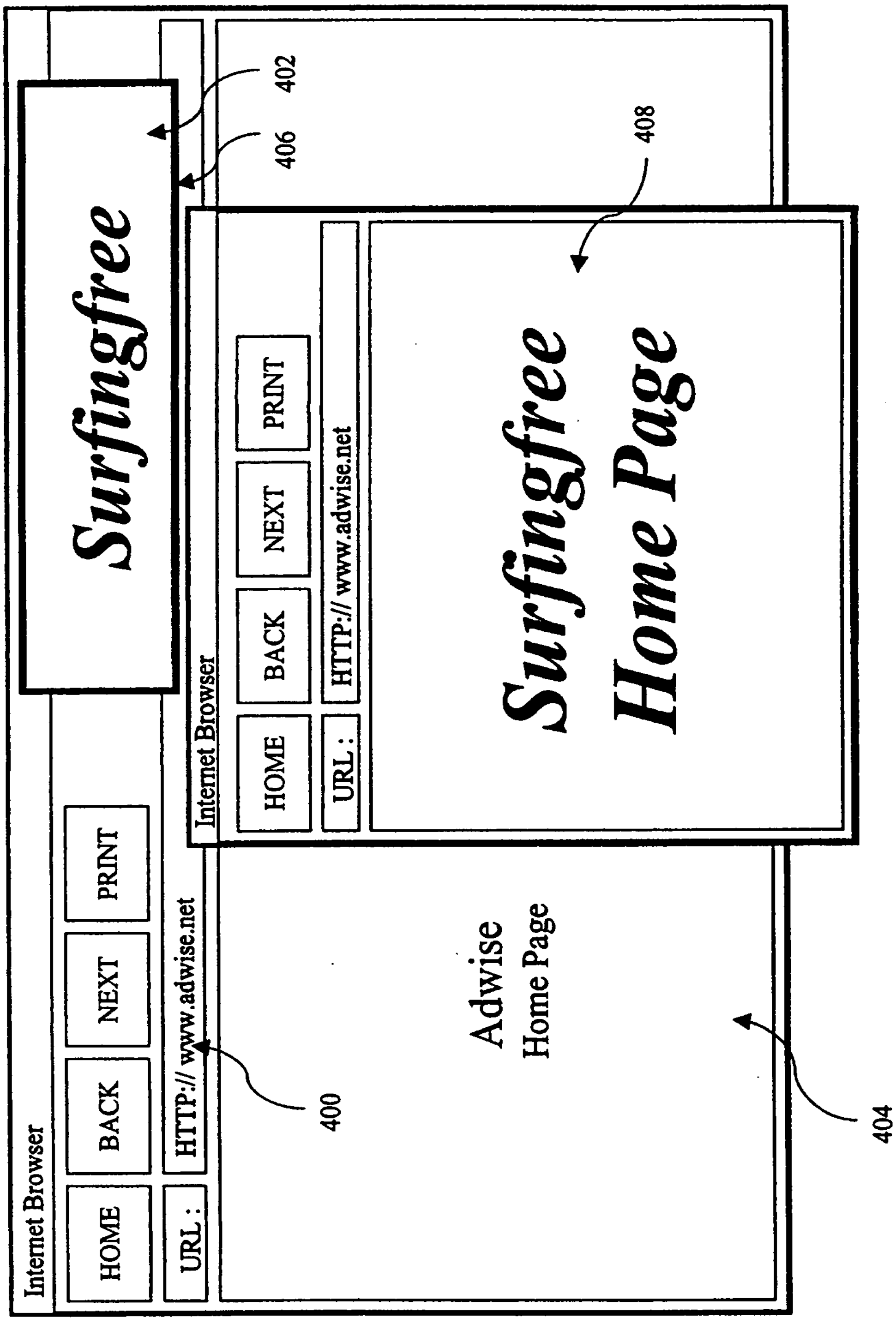

Internet Browser
HOME
BACK
NEXT
PRINT
URL :
HTTP:// www.adwise.net
Surfingfree
402
406
Adwise
Home Page
400
404
Internet Browser
HOME
BACK
NEXT
PRINT
URL :
HTTP:// www.adwise.net
Surfingfree
Home Page
408

Fig. 9C

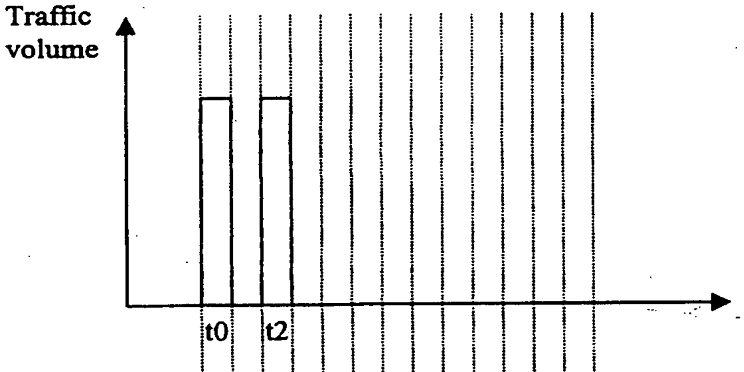


Fig. 10A

Upstream
Traffic generated
by the client

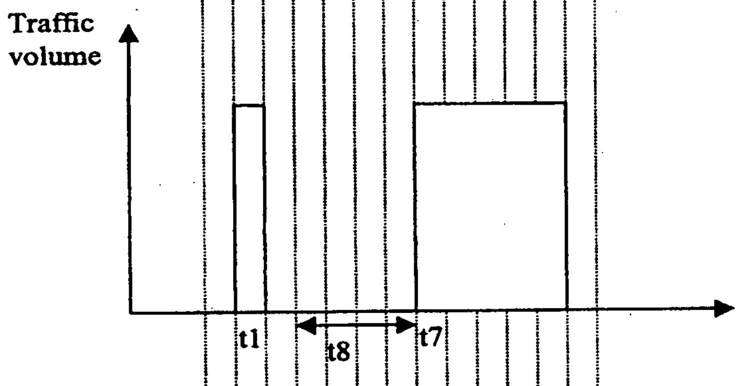


Fig. 10B

Downstream
Traffic response from
servers to a client

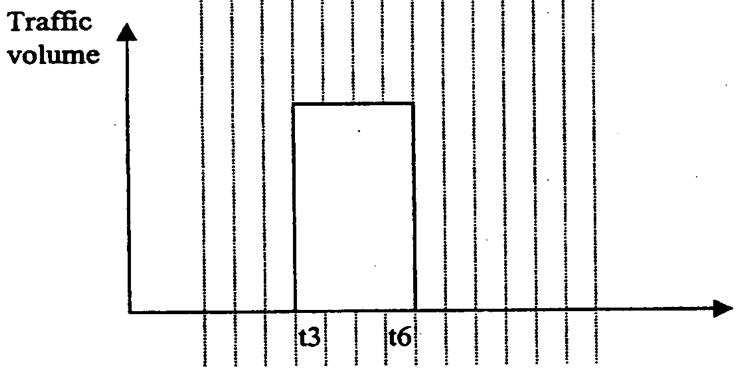


Fig. 10C

Traffic from the
content injector
to the client

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 99/01493

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F17/30

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 572 643 A (JUDSON DAVID H) 5 November 1996 (1996-11-05) abstract figure 1 column 1, line 6 - line 10 column 1, line 59 -column 2, line 11 column 2, line 29 - line 53 column 5, line 50 -column 6, line 12 column 6, line 45 - line 61 ---	1-42
P,X	WO 99 16003 A (BELARC INC) 1 April 1999 (1999-04-01) abstract page 1, line 1 - line 4 page 3, line 13 - line 27 page 5, line 17 -page 6, line 15 claim 1 --- -/--	1-42

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 17 January 2000	Date of mailing of the international search report 27/01/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Adkhis, F

2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 99/01493

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	KOHDA Y ET AL: "UBIQUITOUS ADVERTISING ON THE WWW: MERGING ADVERTISEMENT ON THE BROWSER" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 28, page 1493-1499 XP002037594 ISSN: 0169-7552 abstract page 1494, left-hand column, line 15 - line 28 page 1495, left-hand column, line 25 - line 41 page 1495, right-hand column, line 4 - line 7 page 1497, left-hand column, line 3 -right-hand column, line 19 ---	1,17,26, 37
X	COOPER L F: "More than just hits Web advertising" INFORMATIONWEEK,US,MANHASSET, NY, no. 608, page 63,68,72 XP002082816 ISSN: 8750-6874 page 72, left-hand column, line 18 - line 33 -----	1,17,26, 37

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 99/01493

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5572643 A	05-11-1996	AU 699439 B	03-12-1998
		AU 7458896 A	07-05-1997
		CA 2235014 A	24-04-1997
		EP 0856180 A	05-08-1998
		WO 9715020 A	24-04-1997
		US 5737619 A	07-04-1998
WO 9916003 A	01-04-1999	AU 9494198 A	12-04-1999

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
G06F 17/31

A1

(11) International Publication Number: WO 99/57660

(43) International Publication Date: 11 November 1999 (11.11.99)

(21) International Application Number: PCT/IL99/00237

(22) International Filing Date: 6 May 1999 (06.05.99)

(30) Priority Data:

60/084,397	6 May 1998 (06.05.98)	US
09/205,729	4 December 1998 (04.12.98)	US

(71) Applicant *(for all designated States except US)*: IWEB LTD. [IL/IL]; Ha'yetsira 5, 43663 Raanana (IL).

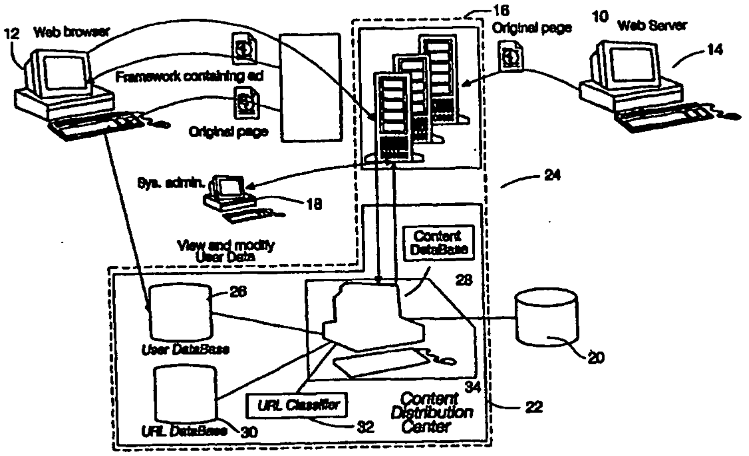
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SAMBOURSKY, Ja'acob [IL/IL]; Yigal Alon 30/B, 46324 Herzliya (IL). GIRMONSKY, Alon [IL/IL]; Hageula Street 19, 45272 Hod Hasharon (IL).

(74) Agent: FRIEDMAN, Mark, M.; Beit Samueloff, Haomanim Street 7, 67897 Tel Aviv (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CONTENT ENHANCEMENT SYSTEM



(57) Abstract

A system (10) and a method for delivering the content, including rich media content, to a particular audience of computer users, preferably according to characteristics of these users, such that the content is exposed in a controlled manner and such that the content is delivered by a third party into a "two–party" system such as the World Wide Web. For example, rather than delivering the content, such as an advertisement, as part of a Web page at a Web site which is remote (14) to the computer user, the present invention delivers the advertisement through the ISP (Internet Service Provider) of the user on the screen of the user's computer, for example. The advertisement or other content is therefore optionally displayed to the user regardless of the Web page being displayed on the screen of the computer of the user, in a manner which is substantially transparent to the user. Thus, the content is targeted specifically to the user rather than being generally displayed on the Web page or otherwise delivered through "two–party" channels such as Web servers (14).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

CONTENT ENHANCEMENT SYSTEM

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system for content enhancement and, in particular, to a system which enables various types of content, such as information, to be presented to a computer user according to specific criteria, preferably through a Web browser. The information is optionally in the form of advertisements or other messages, for example, and preferably includes rich media such as audio samples and video clips. The system of the present invention is able to inject such content as a third party, such that the content is preferably provided to the computer user directly at substantially any convenient time, such as during a waiting period, and in a manner which is preferably substantially transparent to the computer user.

Many consumers are connected to the World Wide Web (WWW) on the Internet through a computer connection at home. For the vast majority of consumers, such a connection to the Internet is obtained by purchasing services from an ISP (Internet Service Provider), which charges monthly fees for such access. These consumers can then view Web pages on the World Wide Web for news, entertainment or information. Viewing Web pages, or "surfing the Web", is a popular leisure activity for many consumers.

Since many Web pages can be viewed without a separate access charge from the provider of the Web page itself, other sources of revenue have been sought by providers of commercial Web pages. Advertisements incorporated into the Web page itself are frequently sold by these Web page providers as a source of revenue. One drawback of such advertisements is the difficulty of determining how many computer users actually view these advertisements, let alone the demographic characteristics of these users. Without such information, the value and efficacy of the advertisements is difficult to ascertain.

Other media, such as television and radio, have developed ratings systems for determining how many consumers typically watch or listen to a given program and/or a given time slot, as well as the demographic characteristics of such consumers. Such ratings information enables the value of the advertisements to be more easily determined.

Ratings information is more difficult to obtain from the World Wide Web because of its diffuse, non-localized and non-controlled nature. First, monitoring viewing of advertisements to determine the number of users who actually see a particular advertisement is very difficult, and must currently be performed only as a measure of past performance. Furthermore, Web pages can be viewed all over the world, without regard to the physical location of the computer user. However, many advertisers are only interested in reaching a particular segment of the population. For example, a restaurant owner in London does not necessarily want to advertise to consumers in Tokyo, and so forth. Therefore, determining the ratings information for a Web page, in order to determine the value of advertisements on this page, is not as simple as counting the number of computer users who view the Web page.

In addition, it is very difficult to gauge the number of computer users who not only view the Web page, but for whom the advertisement has any relevance. Such relevance may be geographical, as in the example of the restaurant, and/or demographic, as for advertisements aimed at parents of young children. Currently, proper targeting of the advertisement to the intended audience cannot be guaranteed.

Furthermore, the exposure of advertisements to computer users is part of a more general characteristic of the World Wide Web. The World Wide Web is structured as a "two-party" system, in which a first party, the computer user, receives content from a second party, the Web server. Client-server systems are also "two-party" systems. However, these systems do not enable a third party to inject content directly to the screen of the computer user, for example through a Web browser or other computer software on the computer of the user, in a manner which is substantially transparent to the user. Thus, current "two-party systems" have limitations for the transparent, controlled exposure of rich media content to the computer user.

Clearly, a system is required which would enable a third party to inject such content and to control exposure of the content to the computer user. For example, such a system would enable advertisers to target a particular audience of computer users, according to geographical and/or demographic information about the users, such that the advertisement would be displayed substantially only to members of that audience and such that the number of exposures of an advertisement could be sold in advance. Furthermore, such a system could advantageously load such content onto the computer of the user during waiting periods and other "down" times. Unfortunately, such a system does not currently exist.

Therefore, there is an unmet need for, and it would be highly useful to have, a system and a method for delivering content, including rich media content such as audio samples and video clips, to a targeted audience according to a controlled exposure in a manner which is preferably substantially transparent to the computer user, such that the content could be presented to each user in the audience optionally without being tied to the Web page or other "two-party system" content being examined by the user.

SUMMARY OF THE INVENTION

The present invention is of a system and a method for delivering content, including rich media content, to a particular audience of computer users, preferably according to characteristics of these users, such that the content is exposed in a controlled manner and such that the content is delivered by a third party into a "two-party" system such as the World Wide Web. For example, rather than delivering the content, such as an advertisement, as part of a Web page at a Web site which is remote to the computer user, the present invention delivers the advertisement through the ISP (Internet Service Provider) of the user on the screen of the user's computer, for example. The advertisement or other content is therefore optionally displayed to the user regardless of the Web page being displayed on the screen of the computer of the user, in a manner which is substantially transparent to the user. Thus, the content is targeted specifically to the user rather than being generally displayed on the Web page or otherwise delivered through generic "two-party" channels such as a generic Web server.

According to the present invention, there is provided a method for displaying an added content on a GUI (graphical user interface) of a first client of a first user being served by a general server, the general server serving a substantially similar general content to a plurality of clients of a plurality of users, the method comprising the steps of: (a) providing an added content server for serving an added content; (b) receiving a request for the general content from the first client by the general server; (c) selecting the added content according to a selection characteristic by the added content server; (d) sending the added content by the added content server to the first client for being displayed on the GUI of the first client; (e) sending the general content to the first client for being displayed on the GUI of the first client; and (f) displaying the added content and the general content on the GUI of the first client, such that a display of the added content is controlled according to the selection characteristic.

According to another embodiment of the present invention, there is provided a method for displaying an added content to a Web page on a Web browser of a user, the Web page being served by a remote Web server, the method comprising the steps of: (a) providing an added content server for serving the added content; (b) receiving a request for the Web page from the Web browser; (c) transmitting the request to the remote Web server; (d) receiving the Web page from the remote Web server; (e) selecting the added content according to at least one user characteristic by the added content server, such that the added content is targeted to the user; (f) adding the added content to the Web page to form a content-added Web page by the added content server; (g) sending the content-added Web page from the added content server to the Web browser; and (h) displaying the content-added Web page by the Web browser.

According to yet another embodiment of the present invention, there is provided a system for delivering a content to a Web browser of a computer user when the user requests a Web page, the system comprising: (a) a content distribution center for storing, distributing and managing the content; (b) an content enhancement module for receiving the content from the content distribution center and for delivering the content to the Web browser upon receiving the request for the Web page, such that the content is specifically targeted to the computer user; and (c) a service provider for providing a connection between the Web browser and the content enhancement module.

According to still another embodiment of the present invention, there is provided a system for delivering a content to a Web browser of a user computer when a user requests a Web page, the system comprising: (a) a content distribution center for storing, distributing and managing the content; (b) an content enhancement module for receiving the content from the content distribution center; (c) a client module for requesting the content from one of the content enhancement module or the content distribution center, and for providing the content to the Web browser, such that the content is specifically targeted to the computer user; and (d) a service provider for providing a connection between the client module and the content enhancement module.

According to still another embodiment of the present invention, there is provided a method for transparently installing a client module on a Web browser of a user computer, the Web browser being operated by a user computer, the method comprising the steps of: (a) starting to operate the Web browser by the user computer; (b) detecting the start of operation of the Web browser; and (c) installing the client module on the user computer when the user computer is connected to the Internet substantially without any intervention by the user, such that the client module operates in a manner which is substantially transparent to the user.

Hereinafter, the term "computing platform" refers to a particular computer hardware system or to a particular software operating system. Examples of such hardware systems include, but are not limited to, personal computers (PC), Macintosh ™computers, mainframes, minicomputers and workstations. Examples of such software operating systems include, but are not limited to, UNIX, VMS, Linux, MacOS™, DOS, one of the Windows™ operating systems by Microsoft Inc. (Seattle, Washington, USA), including Windows NT™, Windows 3.x™ (in which "x" is a version number, such as "Windows 3.1™"), Windows CE™, Windows95™ and Windows98™. For the present invention, a software application could be written in substantially suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computing platform according to which the software application is executed. Examples of suitable programming languages include, but are not limited to, C, C++ and Java.

Hereinafter, the term "Web browser" refers to any software program for displaying a GUI (graphical user interface), and in particular for any software program which can be used to view a document written at least partially with at least one instruction taken from HTML (HyperText Mark-up Language), DHTML (Dynamic HyperText Mark-up Language) or VRML (Virtual Reality Modeling Language), or any other equivalent computer document language, hereinafter collectively and generally referred to as "document mark-up language". Examples of Web browsers include, but are not limited to, Mosaic™, Netscape Navigator™ and Microsoft™ Internet Explorer™.

Hereinafter, the term "two-party system" refers to any system, such as a client-server system or a Web browser-Web server system, in which content is normally delivered from a first party (the server) to a second party (the client).

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

FIG. 1 is a flowchart of an exemplary method for adding content by a third party into a two-party system according to the present invention;

FIG. 2 is a schematic block diagram illustrating an exemplary system according to the present invention;

FIG. 3 is a schematic block diagram showing the system of Figure 2 in greater detail;

FIG. 4 is a schematic block diagram illustrating an exemplary display screen according to the present invention;

FIG. 5 is a flowchart of an exemplary method for the operation of Promo according to the present invention;

FIG. 6 is a schematic block diagram of an illustrative embodiment of a system for collecting a charge for added content according to the present invention;

FIG. 7 is a schematic block diagram of an illustrative but preferred embodiment of a portion of the system of Figure 2; and

FIG. 8 is a schematic block diagram of an illustrative but preferred embodiment of the system of Figure 7.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is of a system and a method for presenting various types of content, such as information, to a computer user according to specific criteria, preferably through a Web browser. The information is optionally in the form of advertisements or other messages, for example, and preferably includes rich media such as audio samples and video clips. The system of the present invention is able to inject such content as a third party, such that the content is provided to the computer user directly at substantially any convenient time, such as during a waiting period, and in a manner which is substantially transparent to the computer user.

For example, if the content is in the form of advertising, rather than delivering the advertisement as part of a Web page at a Web site which is remote to the computer user, the present invention delivers the advertisement through the ISP (Internet Service Provider) of the user on the screen of the user's computer. The advertisement is therefore optionally displayed to the user regardless of the Web page being displayed on the screen of the computer of the user. Thus, the advertisement is targeted specifically to the user rather than being generally displayed on the Web page, and is delivered to the user in a transparent, controlled manner.

The principles and operation of the system and method according to the present invention may be better understood with reference to the drawings and the accompanying description.

Referring now to the drawings, Figure 1 is a flowchart of an example of a method for operating a general system for injecting content as a third party into a two-party system. The method displays an added content on a GUI (graphical user interface) of a user. The GUI is connected to, and is served by, a general server. This general server serves a plurality of such users as part of a "two-party system". The method of the present invention, as shown in Figure 1, is capable of injecting specific, tailored content to the user through the GUI in a controlled manner, preferably according to at least one characteristic of the user. Preferably, this additional content is served by an added content server, which could be a separate server computer from the general server computer, or alternatively could be a separate function of the general server computer, for example as a separate software module. Thus, the method of the present invention generally controls the exposure of the added content to the user from a third party into the two-party system.

In step 1, the general server receives a request for the general content from the GUI. In step 2, preferably at least one user characteristic of the user is determined. In step 3, the added content is selected according to some criteria by the added content server, preferably according to the at least one user characteristic, such that the added content is preferably targeted to the at least one user. In step 4, the added content and the general content are sent to the client for being displayed on the GUI, such that the added content is injected into the client GUI-server relationship, either by the added content server or by the general content server. Preferably, the added content is sent to the client in a controlled manner, such that the added content is sent during a period when the client is idle or otherwise has capacity for receiving the content for example. More preferably, the added content is to the client in a substantially transparent manner to the user, such that the user does not need to interact with the GUI specifically in order to receive the content.

Preferably, the method also includes two more steps. In step 5, first the added content is displayed on the GUI. In step 6, more preferably the general content is displayed on the GUI, such that the added content is displayed substantially before the general content. This preferred embodiment might be suitable for Web advertising, for example if the added content is an advertisement, the GUI is a Web browser, the general content is a Web page and the general server is a Web server. Most preferably, the added content could be removed from the GUI substantially before the general content is displayed. Alternatively, the added content and the general content could be displayed substantially simultaneously. For example, if the added content was an advertisement and the general content was a Web page, the advertisement could be displayed as an overlay to the Web page, either static or moving.

Alternatively, the general server and the GUI of the client are optionally connected through an intranet of a corporation, and the user is an employee of the corporation, such that the added content is targeted to the employee.

In any case various types of added content are possible. For example, the added content could feature information of a type selected from the group consisting of customer support, news, entertainment and instruction.

Figure 2 is a schematic block diagram illustrating a specific example of a system according to the present invention for delivering targeted advertising and other messages. Although the following description centers upon targeted advertising, it is understood that this is for the purposes of discussion only and is not meant to be limiting in any way, since the present invention could be used for delivering substantially any type of targeted content to the user, including but not limited to, advertisements, messages, software objects, audio and video clips and other rich content.

As shown in Figure 2, in a general system **10**, a computer user interacts with a Web browser **12**. As used herein, the term "Web browser" can apply to substantially any type of GUI (graphical user interface) being displayed by the display device of the computer user, and not only to software which is capable of rendering mark-up documents for display. However, the following description is directed toward software programs which render mark-up documents for display only for the purposes of clarity and without intending to be limiting in any way.

Web browser **12** receives content from, and sends commands to, a remote Web server **14**, according to the HTTP (HyperText Transfer Protocol) protocol. Web browser **12** is not directly connected to remote Web server **14**, however. Rather, Web browser **12** is connected to an content enhancement module **16**. Content enhancement module **16** is also connected to remote Web server **14**. In this embodiment of the present invention, substantially all interactions between Web browser **12** and remote Web server **14** therefore pass through content enhancement module **16**, such that content enhancement module **16** is an intermediary layer between Web browser **12** and remote Web server **14**. Optionally, content enhancement module **16** may also connect to remote Web server **14** indirectly, through one or more additional proxy servers (not shown).

Content enhancement module **16** accesses the data streams transmitted according to the HTTP protocol between Web browser **12** and remote Web server **14**, and is able to inject additional data according to the HTTP protocol for display by Web browser **12**. For example, content enhancement module **16** can send data to Web browser **12** which causes Web browser **12** to display an advertisement, such that the Web page displayed by Web browser **12** is a "content-added Web page". The advertisement optionally features a static graphic, with or without text, preferably including sound data. More preferably, the advertisement features animation. The advertisement can be static, but alternatively and preferably moves within the display of Web browser 12 in order to more effectively catch the attention of the computer user. Most preferably, additional rich content, such as audio and/or video clips, or optionally streaming audio and/or video data, is included.

In order to more effectively use the period of time required for Web browser 12 to load a particular Web page requested from remote Web server 14, preferably content enhancement module 16 displays the content, such as the advertisement, within the display of Web browser 12 as the requested Web page loads into Web browser 12. More preferably, the content is displayed in the context of a display Web page, which is optionally a completely separate Web page with separate Web content from the requested Web page. Thus, the time which is required for the requested Web page to load can now be used for displaying an advertisement or other content. The advertisement or other content, such as the display Web page, then preferably disappears from the display of Web browser 12 after the requested Web page has been loaded.

Alternatively, the advertisement or other content could appear at substantially any time during the operation of Web browser 12, and not only when a requested Web page was being loaded, such that the display Web page could be built from a combination of the content and the requested Web page, for example. Other preferred features and embodiments of the content itself and of the display of the content are discussed in greater detail below with reference to Figures 5 and 6. According to one particularly preferred embodiment of the present invention, the content itself is quite rich, including for example video data in the form of video clips. This rich content is optionally and preferably supported by a pre-fetch method of the present invention, described in greater detail below.

In either case, the content is preferably displayed as an overlay to the Web page display, even if the Web page itself is in the process of being downloaded.

In order to provide external control over the advertisements, the type of display and the timing of the display, content enhancement module 16 is optionally connected to a system administrator Web browser interface 18. System administrator Web browser interface 18 provides a management interface which enables the administrator of the service provider to control the type of advertisement shown, the type and timing of the display, and the identity of the user or users to whom the advertisement is shown. System administrator Web browser interface 18 controls the management functions of content enhancement module **16**.

The exact identity of the administrator depends upon the type of connection provided between Web browser **12** and remote Web server **14**. For example, if this connection is provided by an ISP (Internet service provider), then the administrator could be an employee of the ISP. Alternatively, if the connection was an intranet connection provided by a company to employees of that company, then the administrator could be an employee of that company. Of course, the administrator could be substantially any individual charged with administering system **10**.

According to preferred embodiments of the present invention, general system **10** also features a content management system **20** for enabling the content provider to transmit content. Preferably, the content provider can also receive statistics concerning the number of users to whom the content was made available, as well as an analysis of the characteristics of these users. Such characteristics optionally and preferably include the types of Web pages visited by the users, as well as demographic and/or geographic characteristics. More preferably, the content provider is also able to request users with certain demographic and/or geographic characteristics through content management system **20**.

The identity of the content provider, as well as the type of information requested or required by that content provider in order to determine which content is to be served to each user or groups of users, can vary depending upon the implementation of general system **10**. Such variations could easily be determined according to one of ordinary skill in the art for the particular implementation of general system **10**. For example, if the content is advertisements, then the content provider could optionally be an advertisement agency or vendor of products and/or services to be advertised. On the other hand, if the content is corporate information being provided to employees of a corporation, then the content provider could optionally be the corporation itself.

Content management system **20** is connected to a content distribution center **22**. Content distribution center **22** is directly associated with, and interacts with, content enhancement module **16**, such that collectively content distribution center **22** and content enhancement module **16** form a content enhancement system **24** according to the present invention.

Content distribution center **22** preferably receives content from content management system **20**, in the form of graphics, sounds, video, text or other data to be displayed by Web browser **12**. Content distribution center **22** then relays the content to content enhancement module 16, which actually performs the necessary steps for preparing the content to be sent to Web browser 12 for display.

Preferably, content distribution center 22 features a plurality of databases for storing different types of information. These databases preferably include a user database 26, for storing demographic and/or geographic information about the computer users; and a content database 28 for storing the content such as advertisements. User database 26 preferably contains demographic information about the computer user, such as age, family size, profession, hobbies and interests, and other potentially useful information for the content provider such as an advertiser. Such information could be provided voluntarily by the computer user. Optionally, the information could be gathered by an analysis of the Web pages requested through Web browser 12. Also optionally, the information could be provided by the content provider, such as the ISP. Preferably, all of these sources of information are gathered for storage in user database 26.

Preferably, the demographic information includes such personal information as the name of the user, age, gender, marital status, occupation, hobbies or other interests. The geographic information preferably enables the user to be located within a fairly precise geographical area. For example, in the United States of America, such geographic information would optionally and preferably include the zip code, state and city of the user.

The information preferably also includes the language preference of the user, which is not necessarily determined according to the country in which the user physically resides. The language preference is particularly preferred for displaying advertisements which include text, and enables the advertisements to be adjusted according to the language of the user, rather than using only one language for all advertisements throughout the World Wide Web.

Also, user database 26 preferably stores user profile information, such as the history of Web page browsing, or "surfing" and the ratings of the user in various categories which might be of interest to advertisers. All of this information, including the classification of the requested Web page and the user information, is preferably accessible as a "request factor" to enable a particular type of content, such as a particular advertisement, to be selected.

In addition, user database 26 preferably also stores such information as the permissions which the user has given for access by content enhancement module 16. For example, the user is preferably able to determine whether advertisements from content enhancement module 16 can be blocked, or whether content enhancement module 16 is allowed to construct a dynamic history of the Web page browsing by a user.

Optionally and preferably, content distribution center **22** also includes an URL (universal resource locator) database **30** for storing the Web page addresses (URL's) for any Web pages associated with the advertisement content stored in content database **28**. More preferably, these URL's are classified by an URL classifier module **32**. Distribution module **28** preferably receives information concerning the type of Web page being requested from URL classifier module **32**. URL classifier module **32** could include information about different types of Web pages which is manually entered through system administrator Web browser interface **18**, for example. Alternatively and preferably, the Web pages could be classified automatically according to keywords.

Within content distribution center **22**, distribution module **34** determines which content is selected from content database **28** for being served by content enhancement module **16**. The selection of content is preferably performed according to the profile of the computer user, and more preferably is also performed according to the type of Web page being displayed. The selection according to the type of Web page being displayed is particularly important for computer users in the home environment, in which more than one user may share Web browser **12**. Under these circumstances, the content, such as an advertisement, is preferably tailored according to the type of Web page being displayed.

Figure 3 shows a more detailed view of an illustrative, preferred embodiment of general system **10**. In this preferred embodiment, again Web browser **12** requests Web pages from remote Web server **14** through content enhancement system **24**. Content enhancement system **24** includes content enhancement module **16**, which serves both the Web page and the added content to Web browser **12**. Content enhancement module **16** receives the added content from distribution module **34** of content distribution center **22**. The operation of these components of general system **10** is explained in greater detail below.

Content enhancement module **16** features a proxy server **36**, which is an HTTP server. Proxy server **36** receives a request for a particular Web page from Web browser **12**. If proxy server **36** already has the Web page stored, then proxy server **36** can serve the Web page directly, without transmitting the request to remote Web server **14**. Otherwise, proxy server **36** must transmit the request to remote Web server **14** and wait to receive the Web page from remote Web server **14**.

Proxy server **36** also serves the advertisement or other content to Web browser **12**, for example while the computer user waits for Web browser **12** to load the Web page. Proxy server 36 receives the content from a Core module 38.

Core module 38 preferably communicates with proxy server 36 according to the HTTP protocol, or alternatively through another type of software-based interface. Core module 38 receives HTTP events from proxy server 36, such as requests for a particular Web page. Preferably, Core module 38 filters the event according to a preconfigured event filter. Core module 38 then passes the event to a Brain module 40.

Brain module 40 then receives the event from Core module 38. Brain module 40 preferably controls the session with Web browser 12, including initiating communication with Web browser 12 and terminating such communication. Brain module 40 also preferably can alter the event filter in Core module 38. Brain module 40 preferably communicates with URL classifier 32 to classify the Web page being requested according to site-related information. The site-related information describes the Web site holding the requested Web page. The site-related information can be important for displaying the advertisement, as described in further detail below. URL classifier 32 communicates with distribution module 34 and URL database 30 to receive this information.

After receiving the site-related information from URL classifier 32, Brain module 40 then decides which plug-in module should handle the event and passes the event to that plug-in module. Brain module 40 preferably also passes the site-related information to that plug-in module. Preferably, there is a plurality of plug-in modules, although for the purposes of illustration, only one such module is shown in Figure 3, a Promo module 42.

Once Promo module 42 has received the event, Promo module 42 performs a number of functions. First, Promo module 42 decides whether to serve the content, such as the advertisement, to Web browser 12. Preferably, the decision is made by Promo module 42 at least partially according to information received from content management system 20. Such information could include criteria for deciding when the content should be displayed, for example.

Next, if Promo module 42 decides to serve the content, Promo module 42 retrieves the framework for the content. For example, if the content is an advertisement which is to be displayed on an HTML page, Promo module 42 first retrieves a framework for that page. Promo module 42 then requests at least one advertisement from content management system 20. Promo module 42 adds the at least one advertisement to the framework, as well as causing distribution module 34 to serve the advertisement to proxy server 36 for serving to Web browser 12. The framework is then given to Brain module 40.

Brain module **40** receives the framework from Promo module **42**. Brain module **40** then passes the framework to Core module **38**, which also receives the original requested Web page from proxy server **36**. Core module **38** first passes the framework to Web browser **12**, preferably either while the Web page is being received by proxy server **36** or while the Web page is being served to Web browser **12**.

Web browser **12** then displays the framework with the advertisement. For example, as noted previously, preferably an advertisement can be displayed on Web browser **12** in several ways. The advertisement could be seamlessly integrated onto the displayed Web page, such that the advertisement appeared to be another banner advertisement, for example. Banner advertisements are a common feature of advertising on the World Wide Web, and are displayed at the top or side of a Web page. Alternatively and preferably, the advertisement could be a "fly-by" advertisement, which moves across the Web page and then disappears. Also preferably, the user might specify "audio only" advertisements, in which only sounds would be produced for the advertisement. Brain module **40** is preferably able to receive a request for a particular type of advertising from Web browser **12** and to transmit the request to Promo module **42**, such that proxy server **36** then delivers the correct type of advertisement to Web browser **12**.

In addition, preferably Brain module **40** is able to support various criteria which determine the length of time for displaying the advertisement. For example, the advertisement could disappear after a fixed length of time has elapsed. Alternatively and preferably, the advertisement could disappear after some positive action by the user, for example clicking a button on the advertisement with the mouse or other pointing device. The advertisement could also disappear when the requested Web page has finished loading, assuming that the advertisement is displayed while the Web page is being loaded. Alternatively, the advertisement could disappear only after the content of the advertisement, such as video or animation, has finished being displayed. All of these different display modes, as well as the control over the display of the advertisement, is preferably handled by Brain module **40**.

An example of the displayed framework with the content is shown in Figure 4. A display **44** of Web browser **12** is shown, with content in the form of a banner **46**. Banner **46** could include text or graphic images, for example.

The implementation of the display of the advertisements on Web browser **12** is optionally performed in a number of ways. For example, a Web page produced by Brain module 40 could be substituted for the requested Web page, preferably adding a refresh tag to the original request for the Web page. Alternatively and preferably, the requested Web page could be changed into a Web page with at least two style sheets or layers. One layer would contain the original requested Web page, while the other layer would display the Web page with the additional advertising. The latter option is particularly preferred because the delay for loading the Web page is substantially reduced or eliminated. In addition, with the latter option the user is able to request that the advertisement disappear after a period of time has elapsed or some other criterion has been fulfilled, leaving only the originally requested Web page being displayed by Web browser 12.

Web browser 12 displays the framework with the advertisement until the Web page has been received from proxy server 36. Preferably, Web browser 12 then removes the advertisement from the display and displays the requested Web page.

Promo module 42 preferably also gathers data related to the content which is served. For example, Promo module 42 preferably records which content was displayed to the user through Web browser 12. In addition, Promo module 42 preferably gathers content-specific data. For example, if the content is an advertisement, Promo module 42 preferably determines the advertisement(s) which were "clicked through" by the user. More preferably, Promo module 42 determines which users purchased a product from a vendor after "clicking through" or otherwise interacting with an advertisement. All of this gathered data can be used to assess the efficacy of the content which is served. For example, in the case of advertisements, the gathered data could be used to determine the cost for serving the advertisement.

According to a preferred embodiment of the present invention, a slightly different protocol is optionally followed for initiating a session between Web browser 12 and content enhancement module 16. Web browser 12 initiates the session by requesting an initial Web page in order to start the session. Core module 38 receives the request for the Web page through proxy server 36. As for the previous embodiment, Core module 38 then passes the event to a Brain module 40, as well as requesting the original Web page from remote Web server 14.

Brain module 40 receives the event from Core module 38, and decides which plug-in module should handle the event and passes the event to that plug-in module, in this case Promo module 42.

Web browser 12 receives the requested Web page from remote Web server 14 through proxy server 36. Once Web browser 12 requests the next Web page, apart from the home page, Brain module 40 initializes Promo module 42. Such initialization preferably includes obtaining user data from user database 26, as well as "pre-fetching" content, as described with regard to Figure 5 below.

Figure 5 is a flowchart of an exemplary method for "pre-fetching" content such as advertisements, in order to more rapidly display such content to the user through Web browser 12. Web browser 12 and Promo module 42 each has a storage area for storing the pre-fetched content: Web browser 12 has a cache, and Promo module 42 has a prefetch FIFO (first in first out) storage. At the beginning of the process, both storage areas are empty.

In step 1, Web browser 12 connects to Promo module 42. In step 2, Promo module 42 requests at least one, and preferably two, prefetched content parcels such as advertisements from content management system 20. In step 3, content management system 20 sends the advertisement(s) to Promo module 42, which stores these advertisement(s) in the pre-fetch storage FIFO. In step 4, Web browser 12 requests a Web page. In step 5, Promo module 42 sends the framework with at least one advertisement to Web browser 12. In addition, in step 6, Promo module 42 also sends at least one, and preferably two, additional advertisements to Web browser 12. In step 7, Web browser 12 preferably stores the advertisement(s) in the cache. More preferably, if the file, such as the advertisement, is relatively large, such that the period of time required to load it into the cache of Web browser 12 is undesirably long, the file is broken into more than two portions, and each portion is loaded separately. The advertisement(s) are now optionally available for future display, such that the amount of time required for Web browser 12 to display the next advertisement is much shorter, since the advertisement is stored locally. Steps 2-7 could optionally be repeated during the session with Web browser 12.

Figure 6 shows yet another preferred embodiment of the present invention, featuring another plug-in module, the Meter module. In this embodiment, an content enhancement system 48 again features an content enhancement module 50 and a content delivery center 52. Now, however, content enhancement module 52 also includes a Meter module 54. In addition, content delivery center 52 also includes a billing module 56. Components which have the same numbering as for Figure 3 retain their previously described function, unless otherwise specified.

Meter module 54 enables the user to pay for content obtained from remote Web server 14 or from content database 28, or from a combination thereof. For example, if the user requests a Web page from a Web site for which payment is required, remote Web server 14 communicates with Meter module 54 to request payment. If such payment is authorized, manually for example by having the user click on a button displayed by Web browser 12, or automatically, Meter module 54 communicates with billing module 56. Billing module 56 then records the payment. The service provider is then able to request remuneration from the user. The service provider also sends payment to the holder of the Web site, possibly after subtracting a commission or other handling fee. Thus, Meter module 54 enables users to purchase content through regular billing, such as part of a monthly bill from an ISP, without entering a credit card number.

As noted previously, the system and method of the present invention are useful for many types of content, such as advertisements, messages, customer support, announcements and educational materials. Furthermore, control over the type of content and the display of the content would depend upon the service provider. For example, if the service provider was an ISP, then the ISP could optionally control the content in order to generate advertising revenue. Alternatively, if the service provider was a corporation, the corporation could optionally control the content in order to inform or instruct its employees, for example.

Figure 7 shows a preferred, illustrative embodiment of the system of Figure 2. In this embodiment, a system 58 again includes a Web browser 60 for interacting with a computer user, as described for Web browser 12 of Figure 2. However, in system 58, Web browser 60 is alternately connected to a content enhancement module 62 and to a remote Web server 64 for serving a Web page 66. Content enhancement module 62 is also connected to remote Web server 64. In addition, as for Figure 2, a content distribution center 22 is connected to content enhancement module 62. Thus, Web browser 60 is either connected directly to remote Web server 64 or alternately is connected indirectly, through content enhancement module 62.

When Web browser 60 is connected to content enhancement module 62, substantially all interactions between Web browser 60 and remote Web server 64 therefore pass through content enhancement module 62, such that content enhancement module 62 is an intermediary layer between Web browser 60 and remote Web server 64, as described for system 10 of Figure 2. However, such a connection can place a heavy load on content enhancement module 62, which effectively acts a proxy server. Therefore, as shown in Figure 7, preferably Web browser 60 can also connect directly to remote Web server 64, thereby by-passing content enhancement module 62 such that content enhancement module

62 is not able to send data to Web browser 60 in this mode.

More preferably, system 58 alternates between these two different modes, with Web browser 60 either connected directly to remote Web server 64, or alternately connected indirectly through content enhancement module 62, most preferably according to either a predetermined schedule or alternatively according to a dynamic schedule. For example, Web browser 60 could be connected to content enhancement module 62 only when the user first "logs on" and connects to the Internet. Alternatively, Web browser 60 could periodically connect to content enhancement module 62 in order for content enhancement module 62 to be able to more effectively track the activity of the user on the Internet. For example, Web browser 60 could periodically connect to content enhancement module 62 every *n* minutes for such tracking, in which *n* is an integer. In any case, such a periodic connection significantly reduces the burden on content enhancement module 62, such that the amount of traffic flowing through content enhancement module 62 is significantly reduced.

In the other, alternative and optional embodiment of system 58, Web browser 60 connects to content enhancement module 62 dynamically, preferably according to the traffic between Web browser 60 and remote Web server 64, such that as the amount of traffic is increased, Web browser 60 connects to content enhancement module 62 more frequently. Such detection of the amount of traffic could be performed by a client module 68 as shown, which could be an applet being operated by Web browser 60 for example.

In either embodiment, as for Figure 2, in order to more effectively use the period of time required for Web browser 60 to load a particular Web page 66 requested from remote Web server 64, preferably content enhancement module 62 causes the content, such as the advertisement, to be displayed within the display of Web browser 60 as the requested Web page 66 loads into Web browser 60. More preferably, the content is displayed in the context of an additional displayed Web page. Thus, the time which is required for Web page 66 to load can now be used for displaying an advertisement or other content. The advertisement or other content, such as the displayed Web page, then preferably disappears from the display of Web browser 60 after the Web page has been loaded.

Alternatively, the advertisement or other content could appear at substantially any time during the operation of Web browser 60, and not only when a Web page was being loaded, such that the display Web page could be built from a combination of the content and the requested Web page 66, for example. Other preferred features and embodiments of the content itself and of the display of the content were previously discussed. More preferably, the rich content is supported by a pre-fetch method of the present invention.

Figure 8 shows a preferred, illustrative embodiment of the system of Figure 7. In this embodiment, system **58** again features a Web browser **60** connected to a client module **68**. Both Web browser **60** and client module **68** are installed on, and are operated by, a user computer **70**. In addition, a service provider **72** for providing a connection to the Internet, which could be an ISP (Internet Service Provider) for example, is shown for clarity. User computer **70** could be connected to service provider **72** through substantially any type of suitable connection, such as a modem connection to the telephone network for example, which could easily be selected by one of ordinary skill in the art.

However, Web browser **60** now connects directly to Web server **64** in order to request and download Web page **66**. Client module **68** now connects directly to content enhancement module **62** and requests the additional content, such as the advertisement or other media content, directly from content enhancement module **62**. Thus, this embodiment of the present invention can be distinguished in that client module **68** now "pulls" content from content enhancement module **62**, rather than having content enhancement module **62** push this content. Alternatively, client module **68** could retrieve content from content distribution center **22**.

Preferably, client module **68** is automatically installed on user computer **70**, in a manner which is transparent to the user, such that client module **68** is able to cause the additional content to be displayed by Web browser **60** as previously discussed, without intervention by the user. Client module **68** would therefore be a "hidden" client software module. For example, client module **68** could be installed on user computer **70** by content enhancement module **62** only when the user first "logs on" and connects to the Internet, particularly for a non-permanent connection, such that user computer **70** is alternately connected to, and disconnected from, the Internet. Optionally, content enhancement module **62** could detect when client module **68** was no longer operating on user computer **70**, and could then install client module **68** on user computer **70** again.

More preferably, content enhancement module **62** is employed as a proxy server at certain times, and most preferably is employed as such a server when the user first "logs on", or first activates Web browser **60** and/or first connects to the Internet, for example through service provider **72**, thereby enabling client module **68** to be installed on user computer **70**. For example, either Web browser **60** or service provider **72** could be configured such that when Web browser **60** first connects to service provider **72**, Web browser **60** initially connects to content enhancement module **62** as a proxy server. Content enhancement module **62** would then install client module **68**.

Optionally and most preferably, client module **68** is implemented as an applet, which is installed on user computer **70** in a non-permanent, transient installation, such that client module **68** is not installed on the hard disk or other permanent storage medium of user computer **70**. Rather, client module **68** is preferably only stored in the RAM (random access memory) or other volatile memory of user computer **70**. Thus, client module **68** preferably does not consume any permanent resources of user computer **70**.

While the invention has been described with respect to a limited number of embodiments, it will be appreciated that many variations, modifications and other applications of the invention may be made.

WHAT IS CLAIMED IS:

1. A method for displaying an added content on a GUI (graphical user interface) of a first client of a first user being served by a general server, the general server serving a substantially similar general content to a plurality of clients of a plurality of users, the method comprising the steps of:

(a) providing an added content server for serving an added content;

(b) receiving a request for the general content from the first client by the general server;

(c) selecting said added content according to a selection characteristic by said added content server;

(d) sending said added content by said added content server to the first client for being displayed on the GUI of the first client;

(e) sending the general content by the general server to the first client for being displayed on the GUI of the first client; and

(f) displaying said added content and the general content on the GUI of the first client, such that a display of said added content is controlled according to said selection characteristic.

2. The method of claim 1, wherein said selection characteristic is a user characteristic and wherein step (c) further comprises the step of:

(i) determining at least one user characteristic of the user, such that the added content is targeted to said at least one user.

3. The method of claim 2, wherein the GUI is a Web browser, the general content is a Web page and the general server is a Web server.

4. The method of claim 3, wherein the added content is an advertisement.

5. The method of claim 4, wherein said advertisement includes at least one type of content selected from the group consisting of an image, a text, an animation, a video clip and a sound.

6. The method of claim 4, wherein step (f) further comprises the steps of:

(i) displaying the added content on the GUI; and

(ii) displaying the general content on the GUI, such that the added content is displayed substantially before the general content.

7. The method of claim 6, wherein the step of displaying the general content on the GUI further includes the step of removing the added content from being displayed on the GUI substantially before the general content is displayed.

8. The method of claim 7, wherein said at least one user characteristic is selected from the group consisting of demographic information and geographic information about the user.

9. The method of claim 8, wherein said at least one user characteristic is determined according to said Web page being requested.

10. The method of claim 2, wherein the general server and the GUI are connected through an intranet of a corporation, and the user is an employee of said corporation, such that the added content is targeted to said employee.

11. The method of claim 1, wherein the added content features information of a type selected from the group consisting of customer support, news, entertainment and instruction.

12. The method of claim 11, wherein the added content features a type of data selected from the group consisting of an audio sample, a graphic image, a text message, a software object and a video clip.

13. The method of claim 1, wherein step (d) further comprises the steps of:

(i) detecting a period of time when the client is receptive to receiving data; and

(ii) sending the added content substantially only during said period of time.

14. A method for displaying an added content to a Web page on a Web browser of a user, the Web page being served by a remote Web server, the method comprising the

steps of:

(a) providing an added content server for serving the added content;

(b) receiving a request for the Web page from the Web browser;

(c) transmitting said request to the remote Web server;

(d) receiving the Web page from the remote Web server;

(e) selecting the added content according to at least one user characteristic by said added content server, such that the added content is targeted to the user;

(f) adding the added content to the Web page to form a content-added Web page by said added content server;

(g) sending said content-added Web page from said added content server to the Web browser; and

(h) displaying said content-added Web page by the Web browser.

15. A system for delivering a content to a Web browser of a computer user when the user requests a Web page, the system comprising:

(a) a content distribution center for storing, distributing and managing the content;

(b) an content enhancement module for receiving the content from said content distribution center and for delivering the content to the Web browser upon receiving the request for the Web page, such that the content is specifically targeted to the computer user; and

(c) a service provider for providing a connection between the Web browser and said content enhancement module.

16. The system of claim 15, further comprising:

(d) a remote Web server for serving the Web page to said content enhancement module upon receiving a Web page request from said content enhancement module;

such that said content enhancement module delivers the content to the Web browser substantially before serving the Web page to the Web browser, the content being delivered in a form of a display Web page.

17. The system of claim 15, further comprising:

(d) a remote Web server for serving the Web page to said content enhancement module upon receiving a Web page request from said content enhancement module;

such that said content enhancement module delivers the content to the Web browser substantially simultaneously with the Web page, such that the Web page is a content-added Web page.

18. The system of claim 17, wherein said content enhancement module further comprises:

(i) a proxy server for serving the content to the Web browser, said proxy server receiving the content from said content distribution center.

19. The system of claim 18, further comprising:

(d) a content management system for managing the content and for determining the content for delivering to the Web browser from said content distribution center.

20. The system of claim 19, wherein said content enhancement module further comprises:

(ii) a Core module for receiving the request from the Web browser;

(iii) a Promo module for requesting the content from said content management system according to at least one request factor; and

(iv) a Brain module for receiving the request from said Core module and for passing the request to said Promo module, and for determining said at least one request factor.

21. The system of claim 20, wherein said at least one request factor is at least partially determined according to the Web page.

22. The system of claim 21, wherein said content distribution center further comprises:

(i) an URL database for storing at least one URL of at least one Web page; and

(ii) an URL classifier for classifying said at least one URL according to information presented in said at least one Web page.

23. The system of claim 22, wherein said Brain module requests a classification of the Web page from said URL classifier, such that said at least one request factor is at least partially determined according to said classification.

24. The system of claim 23, wherein said content distribution center further comprises:

(iii) a user database for storing user information, such that the content is selected by said Promo module according to said user information.

25. The system of claim 24, wherein the content is an advertisement.

26. The system of claim 25, wherein said user information is selected from the group consisting of demographic and geographic information.

27. The system of claim 26, wherein the Web browser, said remote Web server, said proxy server and said Promo module communicate according to the HTTP (HyperText Transfer Protocol) protocol, and wherein the content is delivered in a form of a display Web page, the system further comprising:

(e) a framework for the display Web page for holding said advertisement, said framework being retrieved by said Promo module, and said framework determining a display of the content.

28. The system of claim 27, wherein said display is determined according to a criterion selected from the group consisting of a length of time for said display and a location on the Web browser of said display.

29. The system of claim 28, wherein said length of time for said display is a fixed period of time.

30. The system of claim 28, wherein said length of time for said display is determined according to an action of the computer user.

31. The system of claim 28, wherein said advertisement is displayed substantially only until the requested Web page is loaded by the Web browser.

32. The system of claim 28, wherein said location of said display is fixed.

33. The system of claim 28, wherein said location of said display is substantially continuously altered, such that said advertisement appears to move across a display of the Web browser.

34. The system of claim 27, wherein said framework for the display Web page features two layers, a first layer including the requested Web page and a second layer including the requested Web page and said advertisement.

35. The system of claim 27, wherein the Web browser further comprises a cache for storing a stored advertisement, said Promo module sending said stored advertisement to said cache of the Web browser substantially before the Web browser requests the requested Web page, such that the Web browser rapidly displays said display Web page upon receipt of said framework.

36. The system of claim 35, wherein said Promo module sends said stored advertisement in a plurality of portions to said cache of the Web browser, such that each of said plurality of portions is sent substantially separately to said cache.

37. The system of claim 36, wherein a size of each of said plurality of portions is adjusted according to a period of time available for sending each of said plurality of portions to said cache, such that a performance of the Web browser is not altered by receiving each of said plurality of portions.

38. The system of claim 25, wherein said service provider is an ISP (Internet Service Provider).

39. The system of claim 25, wherein said service provider is a corporation and the

computer user is an employee of said corporation.

40. The system of claim 19, wherein said content enhancement module further comprises:

(ii) a Core module for receiving the request from the Web browser; and

(iii) a Meter module for requesting the Web page from said remote Web page server, and for determining a cost of receiving the Web page from said remote Web page server.

41. The system of claim 40, wherein said service provider is an ISP (Internet Service Provider) and said ISP provider charges the computer user for said cost.

42. The system of claim 15, further comprising:

(d) a client for being operated by the Web browser;

(e) a remote Web server for serving the Web page to said content enhancement module upon receiving a Web page request from said content enhancement module or alternatively directly to the Web browser upon receiving a Web page request from the Web browser, said client determining whether said content enhancement module or alternatively the Web browser receives the content and the Web page.

43. The system of claim 42, wherein said client contacts said content enhancement module for said content enhancement module to receive the Web page.

44. The system of claim 43, wherein said client contacts said content enhancement module at predetermined intervals.

45. The system of claim 43, wherein said client contacts said content enhancement module at dynamically determined intervals, said intervals being determined according to a level of traffic to the Web browser.

46. The system of claim 15, further comprising:

(d) a remote Web server for serving the Web page to said content enhancement module upon receiving a Web page request from said content enhancement module or alternatively directly to the Web browser upon receiving a Web page request from the Web browser, said content enhancement module determining whether said content enhancement module or alternatively the Web browser receives the content and the Web page.

47. The system of claim 46, wherein said content enhancement module receives the Web page at predetermined intervals.

48. The system of claim 46, wherein said content enhancement module receives the Web page at dynamically determined intervals, said intervals being determined according to a level of traffic to the Web browser.

49. A system for delivering a content to a Web browser of a user computer when a user requests a Web page, the system comprising:

(a) a content distribution center for storing, distributing and managing the content;

(b) an content enhancement module for receiving the content from said content distribution center;

(c) a client module for requesting the content from one of said content enhancement module or said content distribution center, and for providing the content to the Web browser, such that the content is specifically targeted to the computer user; and

(d) a service provider for providing a connection between said client module and said content enhancement module.

50. The system of claim 49, wherein said client module requests the content from said content enhancement module.

51. The system of claim 50, wherein said client module is installed by said content enhancement module without any intervention by the user.

52. The system of claim 51, wherein said client module operates in a manner

which is substantially transparent to the user.

53. The system of claim 52, wherein said client module is installed temporarily by said content enhancement module, thereby obviating the need for storing said client module on said user computer.

54. The system of claim 53, further comprising:

(e) a Web server for serving the Web page, said Web server communicating with the Web browser through said service provider.

55. A method for transparently installing a client module on a Web browser of a user computer, the Web browser being operated by a user computer, the method comprising the steps of:

(a) starting to operate the Web browser by the user computer;

(b) detecting the start of operation of the Web browser; and

(c) installing the client module on the user computer when the user computer is connected to the Internet substantially without any intervention by the user, such that said client module operates in a manner which is substantially transparent to the user.

56. The method of claim 55, wherein step (a) further comprises the step of connecting the user computer to the Internet by a non-permanent connection before the start of operation of the Web browser, such that the user computer is alternately connected to, and disconnected from, the Internet.

57. The method of claim 55, further comprising the step of providing a content enhancement module for installing the client module on the user computer, said content enhancement module detecting when the user computer is connected to the Internet.

58. The method of claim 57, wherein step (b) further comprises the step of detecting if the client module is already installed on the user computer, such that step (c) is only performed if the client module is already installed on the user computer.

59. The method of claim 58, wherein step (c) is performed by installing the client module on a non-permanent memory storage media of the user computer.

60. The method of claim 59, wherein step (c) is performed by installing the client module on a RAM (random access memory) of the user computer.

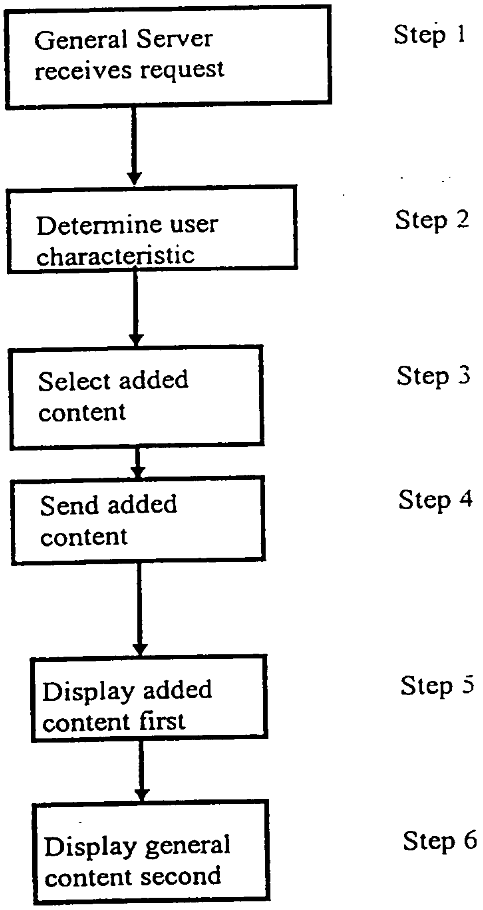
61. The method of claim 60, further comprising the steps of:

(c) requesting a Web page by the Web browser;

(d) requesting an additional content by the client module from said content enhancement module; and

(e) delivering the content to the Web browser by the client module.

Figure 1


General Server receives request
Step 1
Determine user characteristic
Step 2
Select added content
Step 3
Send added content
Step 4
Display added content first
Step 5
Display general content second
Step 6

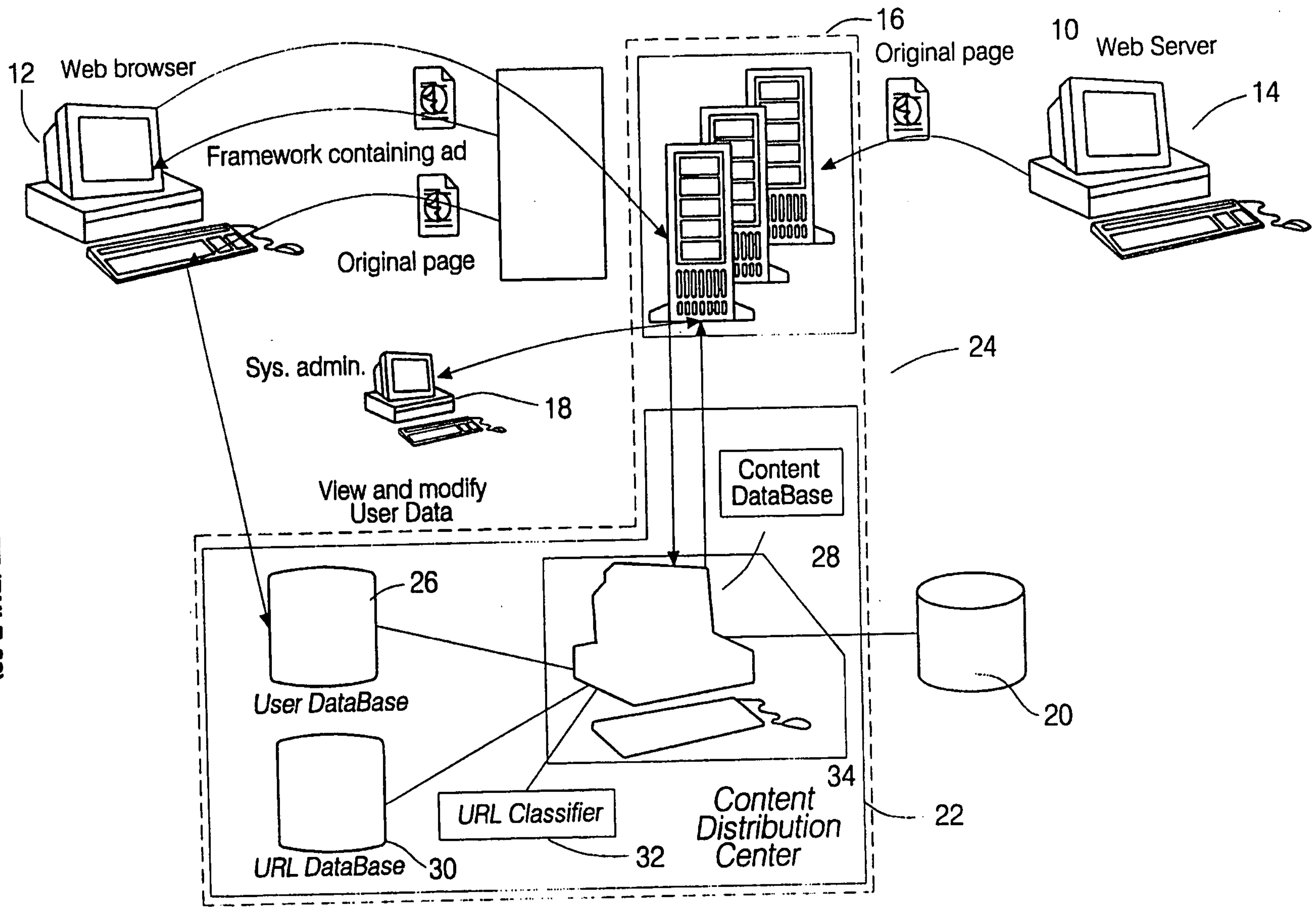


FIG. 2

SUBSTITUTE SHEET (RULE 26)

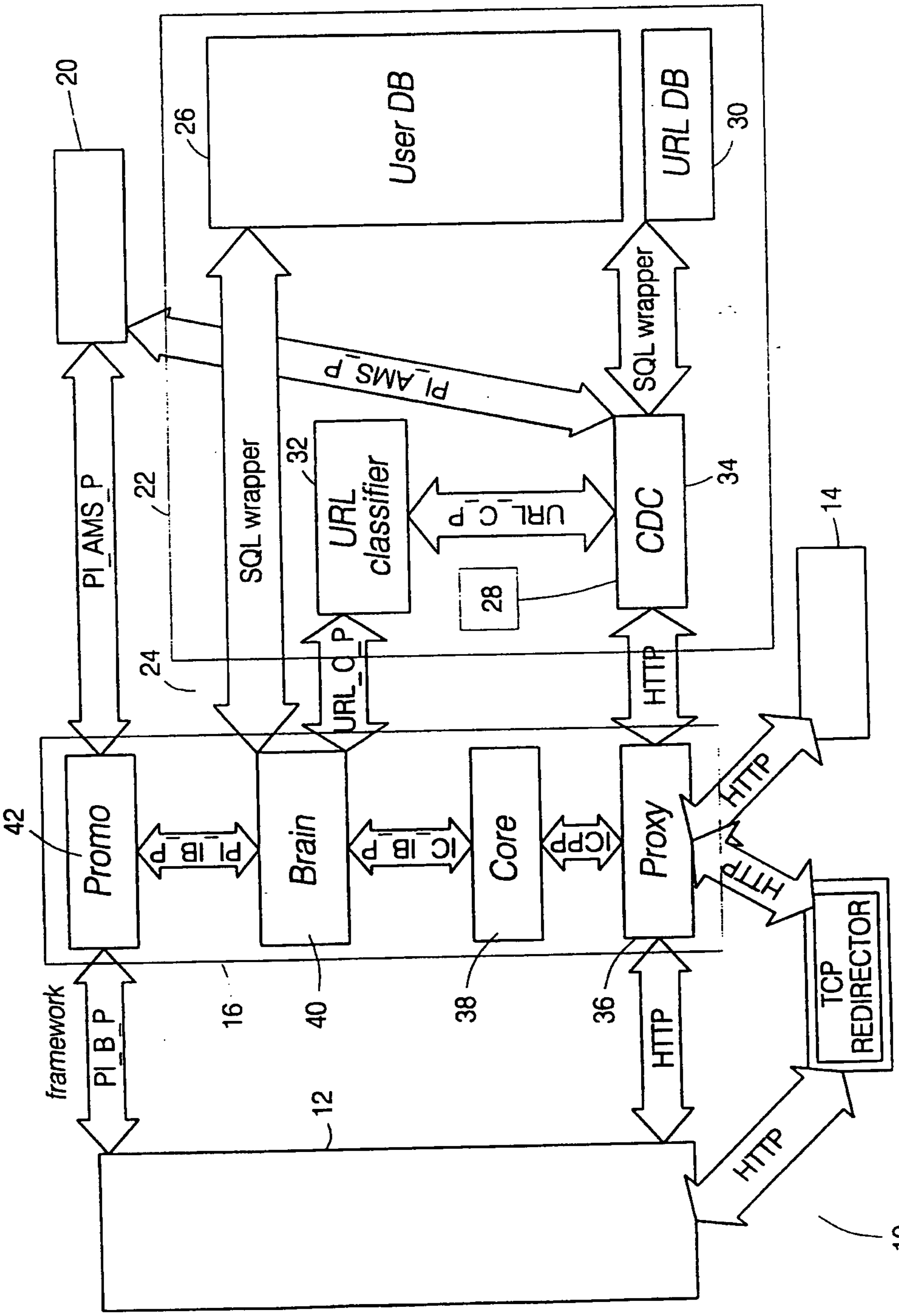
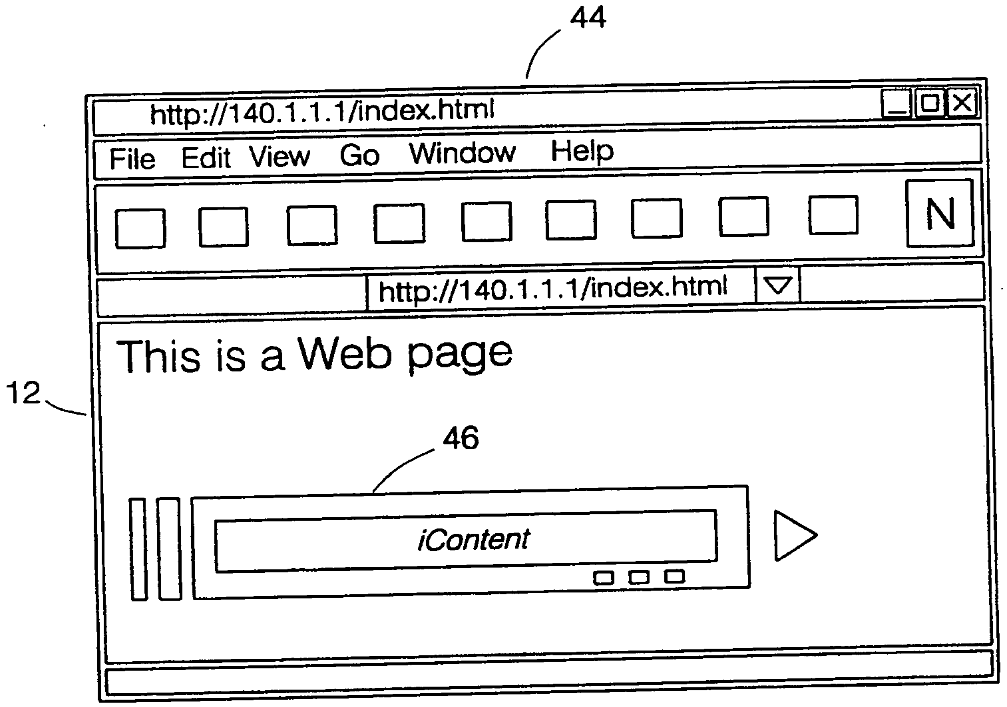


FIG. 3

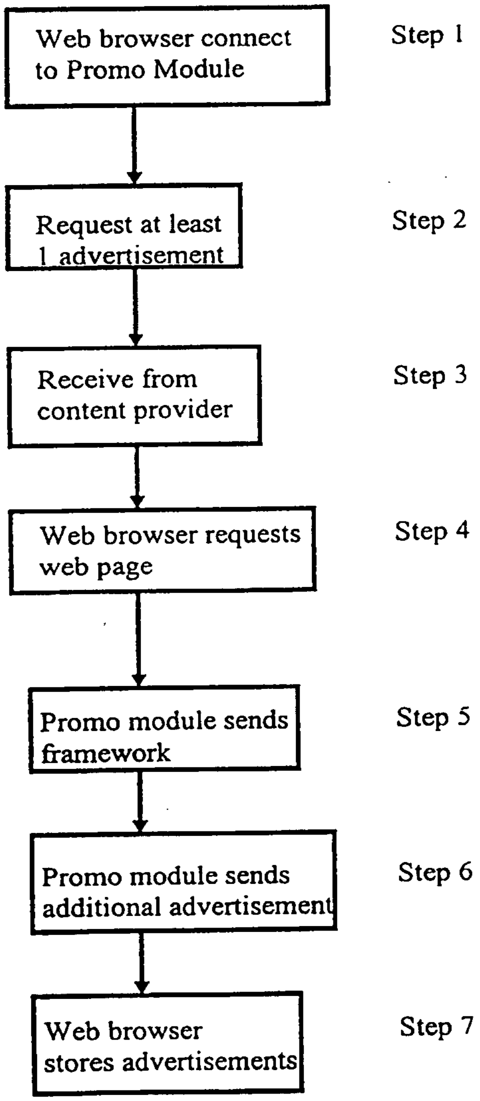
SUBSTITUTE SHEET (RULE 26)


44
http://140.1.1.1/index.html
File Edit View Go Window Help
N
http://140.1.1.1/index.html
12
46
iContent

This is a Web page

FIG. 4

Figure 5


Web browser connect to Promo Module
Step 1
Request at least 1 advertisement
Step 2
Receive from content provider
Step 3
Web browser requests web page
Step 4
Promo module sends framework
Step 5
Promo module sends additional advertisement
Step 6
Web browser stores advertisements
Step 7

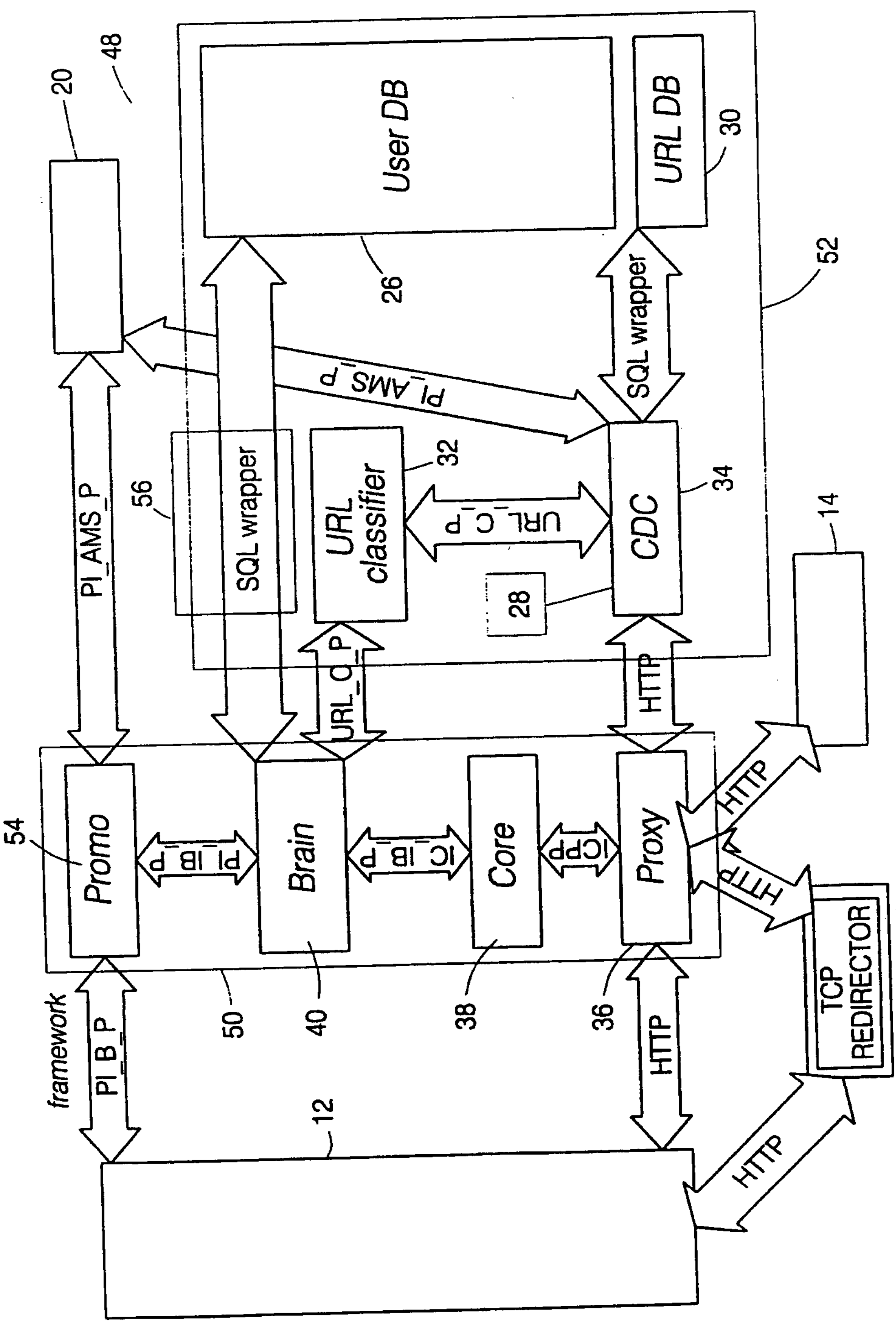

20
48
User DB
URL DB
30
26
52
SQL wrapper
PI_AMS_P
PI_AMS_P
56
SQL wrapper
URL classifier
32
URL_C_P
CDC
34
28
URL_C_P
HTTP
14
54
Promo
PI_IB_P
Brain
IC_IB_P
Core
ICPP
Proxy
HTTP
HTTP
TCP REDIRECTOR
framework
PI_B_P
50
40
38
36
HTTP
12
HTTP

FIG. 6

Figure 7

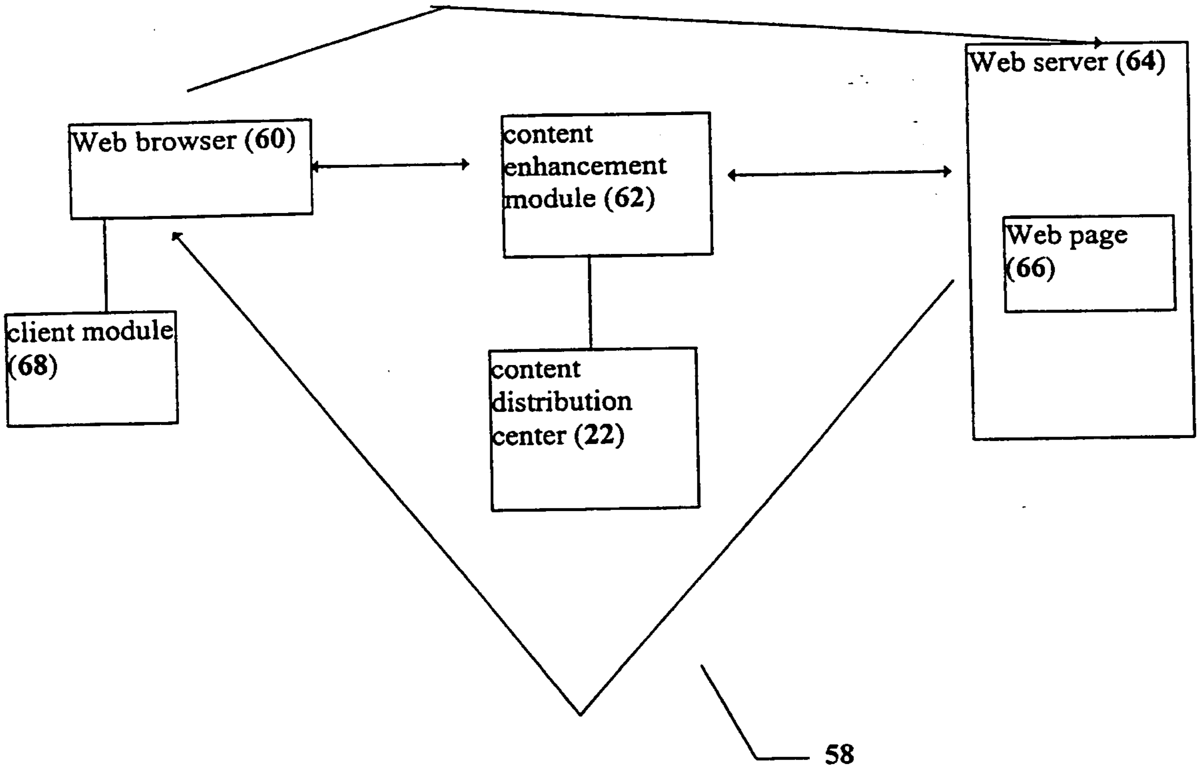
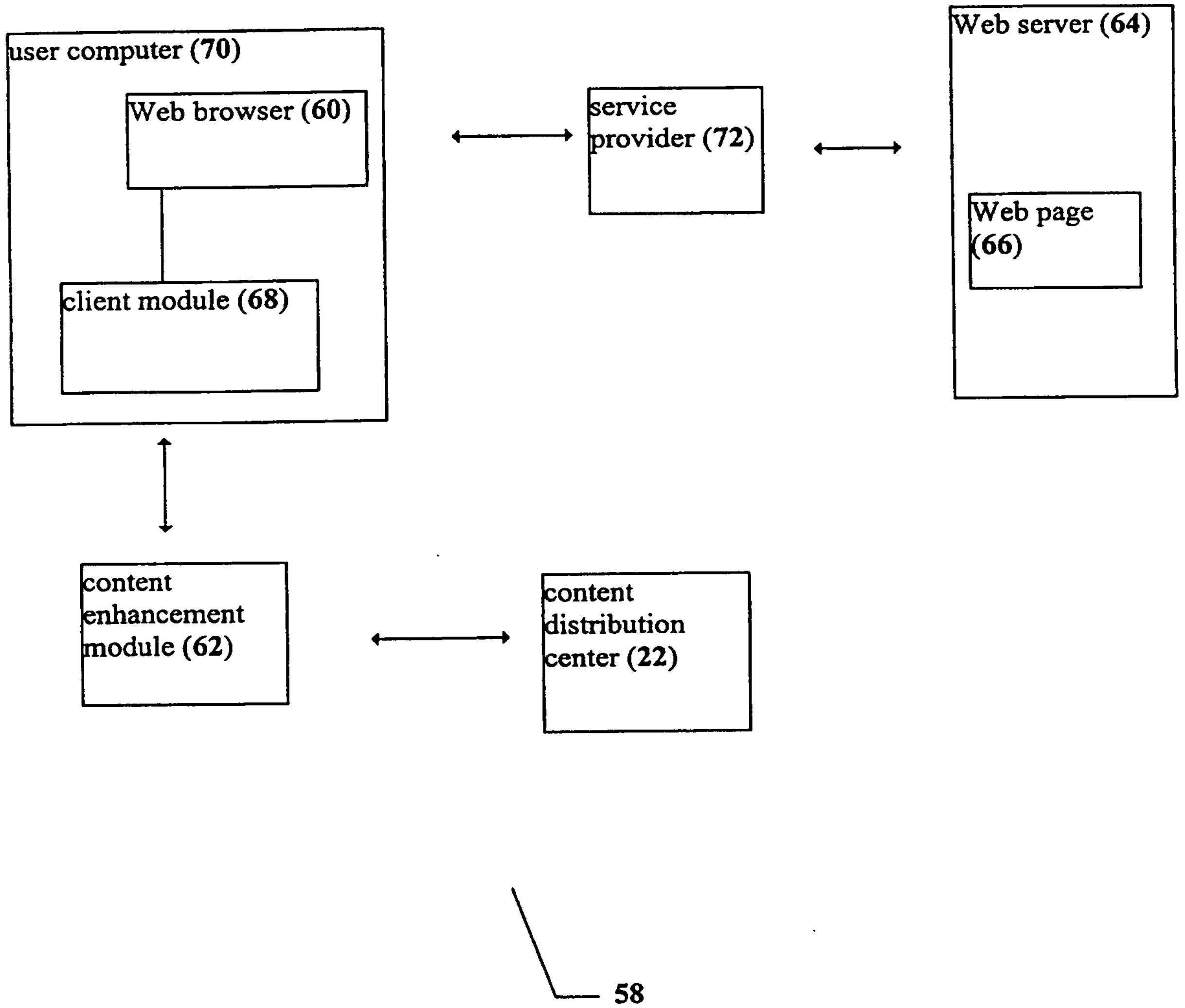

Web browser (60)
content enhancement module (62)
Web server (64)
Web page (66)
client module (68)
content distribution center (22)
58

Figure 8


user computer (70)
Web browser (60)
client module (68)
service provider (72)
Web server (64)
Web page (66)
content enhancement module (62)
content distribution center (22)
58

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL99/00237

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/31
US CL :707/ 1, 6, 10, 102, 104
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 707/ 1, 6, 10, 102, 104

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

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

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P ----- Y,P	US 5,778,367 A (WESINGER, JR. ET AL.) 07 JULY 1998 (07/06/98), See whole document	1, 14, 15, 49 ------- 2-13, 16-48, 50-60
Y, P	US 5,809,242 A (SHAW ET AL.) 15 SEPTEMBER 1998 (15/09/98), See whole document	1-60
A,P	US 5,799,151 A (HOFFER) 25 AUGUST 1998 (25/08/98), See whole document.	1-60

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

* Special categories of cited documents:

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

"E" earlier document published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 01 SEPTEMBER 1999	Date of mailing of the international search report 30 September 1999 (30.09.99)
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SANJIV S James R. Matthews Telephone No. (703) 305-8355

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

U.S. PTO APS

Search terms: ISP or (Internet Service Provider), advertisement, WWW or (World wide Web)

TENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 34503P/A522	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 99/09362	International filing date *(day/month/year)* 29/04/1999	(Earliest) Priority Date *(day/month/year)* 04/05/1998
Applicant AURIC WEB SYSTEMS		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   □ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   □ contained in the international application in written form.

   □ filed together with the international application in computer readable form.

   □ furnished subsequently to this Authority in written form.

   □ furnished subsequently to this Authority in computer readble form.

   □ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   □ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. □ **Certain claims were found unsearchable** (See Box I).

3. □ **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   ☒ the text is approved as submitted by the applicant.

   □ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   ☒ the text is approved as submitted by the applicant.

   □ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

   ☒ as suggested by the applicant.

   □ because the applicant failed to suggest a figure.

   □ because this figure better characterizes the invention.

   □ None of the figures.

In tional Application No
PCT/US 99/09362

A. CLASSIFICATION OF SUBJECT MA

IPC 6 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L G06F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 0 854 621 A (AT & T CORP) 22 July 1998 (1998-07-22) abstract page 2, line 10-51 page 3, line 33-56 page 4, line 28-47 page 5, line 34-43 ---	1-15
P,X	WO 98 26548 A (WHISTLE COMMUNICATIONS CORP ;COBBS ARCHIE L (US); LI JIM Y (US); O) 18 June 1998 (1998-06-18) abstract page 7, line 8-16 page 11, line 32 - page 15, line 17 page 15, line 31 - page 17, line 31 page 18, line 21 - page 20, line 22 figures 8,10 --- -/--	1-14

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 1 September 1999	Date of mailing of the international search report 10/09/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Lázaro Lõpez, M.L.

International Application No
PCT/US 99/09362

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 05549 A (SHIVA CORP) 22 February 1996 (1996-02-22) page 3, line 1-28 page 7, line 21 - page 11, line 2 page 14, line 15 - page 15, line 21 figure 1 ---	1-29
A	US 5 696 898 A (BAKER BRENDA SUE ET AL) 9 December 1997 (1997-12-09) cited in the application abstract column 3, line 29 - column 5, line 5 claims 1-7 -----	1-29

3

Info .ion on patent family members

In tional Application No

PCT/US 99/09362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854621 A	22-07-1998	CA 2226814 A	17-07-1998
		JP 10229418 A	25-08-1998
WO 9826548 A	18-06-1998	AU 3572697 A	03-07-1998
WO 9605549 A	22-02-1996	AU 3099295 A	07-03-1996
		CA 2197219 A	22-02-1996
		DE 69510551 D	05-08-1999
		EP 0775341 A	28-05-1997
US 5696898 A	09-12-1997	CA 2196867 A	07-12-1996
		CN 1159234 A	10-09-1997
		EP 0793826 A	10-09-1997
		WO 9715008 A	24-04-1997

07-20-00

GAU 2766 $

CONTINUED PROSECUTION APPLICATION (CPA) REQUEST TRANSMITTAL

Submit an original, and a duplicate for fee processing

(Only for Continuation or Divisional applications under 37 CFR 1.53(d))

Docket No. : 34503/WWM/A522
Inventor(s) : Koichiro Ikudome and Moon Tai Yeung
Title : USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Express Mail Label No. : EL366428305US Check if applicable: ___ **DUPLICATE**

ADDRESS TO: Assistant Commissioner for Patents
Box CPA
Washington, D.C. 20231

Date: July 19, 2000

This is a request for a continuation application under 37 CFR 1.53(d), (continued prosecution application (CPA) of prior application number 09/295.966, filed on April 21, 1999, entitled USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM.

1. _____ Enter the unentered amendment previously filed on , under 37 CFR 1.116 in the prior nonprovisional application.

2. _____ A preliminary amendment is enclosed.

3. This application is filed by fewer than all the inventors named in the prior application, 37 CFR 1.53(d)(4).

   a. _____ DELETE the following inventor(s) named in the prior nonprovisional application:

   b. _____ The inventor(s) to be deleted are set forth on a separate sheet attached hereto.

4. Information Disclosure Statement (IDS) is enclosed:
   a. __X__ PTO-1449
   b. __X__ Copies of IDS Citations

5. Small entity status:
   a. _____ A small entity statement is enclosed.
   b. __X__ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.
   c. _____ Is no longer claimed.

6. _____ Other

```
07/21/2000 HMICHAEL 00000013 09295966

01 FC:231                345.00 OP
02 FC:202                 39.00 OP
03 FC:203                 81.00 OP
```

CONTINUED PROSECUTION APPLICATION (CPA) REQUEST TRANSMITTAL

Submit an original, and a duplicate for fee processing

(Only for Continuation or Divisional applications under 37 CFR 1.53(d))

Docket No.: 34503/WWM/A522

FEE CALCULATIONS

	CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	CALCULATIONS
A	TOTAL CLAIMS	29 - 20 =	9	9 x $9.00	$81.00
B	INDEPENDENT CLAIMS	4 - 3 =	1	1 x $39.00	$39.00
C	SUBTOTAL			SMALL ENTITY FEE = A + B LARGE ENTITY FEE = 2 X (A + B)	$120
D	BASIC FEE			SMALL ENTITY FEE = $345.00 LARGE ENTITY FEE = $690.00	$345
E	MULTIPLE-DEPENDENT CLAIMS FEE			SMALL ENTITY FEE = $130.00 LARGE ENTITY FEE = $260.00	
F	TOTAL FILING FEE (ADD LINES C, D, AND E)				$465

List Independent Claims: 1, 8, 15 and 26

7. ____ A Petition for Extension of Time for the parent application and the required fee are enclosed as separate papers.

8. X Payment Enclosed: Check for $465

9. X The Commissioner is hereby authorized to charge any fees under 37 CFR 1.16 and 1.17 which may be required during the **entire pendency** of the application to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A duplicate copy of this sheet is enclosed.**

NOTE: The prior application's **correspondence address** will carry over to this CPA **UNLESS** a new correspondence address is provided.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ________________
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/sl

GP 2761

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Donald V. Burt)
) Art Unit: 2761
Serial No.: 09/295,866)
) Examiner: Not Yet Assigned
Filing Date: April 21, 1999)
)
Title: METHOD AND APPARATUS FOR MANAGING AND DELIVERING ACCESS OR ENTITLEMENT CODES FOR CONTENT PROVIDED TO SUBSCRIBERS)
)
Our File No.: 18484-005)

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8

To: Assistant Commissioner for Patents
Washington, DC 20231

The undersigned hereby certifies that the following documents:

1. Certificate Under 37 C.F.R. 3.73(b); and

2. Return Post Card

are being deposited with the United States Postal Service as first-class mail, postage prepaid, in an envelope addressed to: Assistant Commissioner of Patents, Washington, DC 20231, on this 7th day of June, 2000.

CERTIFICATE UNDER 37 CFR 3.73(b)

Applicant(s): Donald V. Burt

Application No.: 09/295,866 Filed: April 21, 1999

Entitled: METHOD AND APPARATUS FOR MANAGING AND DELIVERING ACCESS OR ENTITLEMENT CODES FOR CONTENT PROVIDED TO SUBSCRIBERS

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

certifies that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of either:

A. [X] An assignment from the inventor(s) of the patent application identified above. The assignment was recorded in the Patent and Trademark Office at Reel ______, Frame ________, or for which a copy is attached.

OR

B. [ ] A chain of title from the inventor(s) of the patent application identified above, to the current assignee as shown below:

1. From:________________ To:______________________________
The document was recorded in the Patent and Trademark Office at
Reel ______, Frame _____, or for which a copy thereof is attached.

2. From:____________________ To:____________________________
The document was recorded in the Patent and Trademark Office at
Reel _____, Frame , or for which a copy thereof is attached.

3. From:____________________ To:____________________________
The document was recorded in the Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy there is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet.

[X] Copies of assignment or other documents in the chain of title are attached.

The undersigned has reviewed all the documents in the chain of title of the patent application identified above and, to the best of undersigned's knowledge and belief, title is in the assignee identified above.

The undersigned (whose title is supplied below) is empowered to sign this certificate on behalf of the assignee.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Aug 11, 1999
Date

Donald V Burt
Signature

Donald V. Burt
Typed or printed name

President
Title

GAU ~~2766~~ 2764
3/15/00

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on October 22, 1999.

Signature

Applicant	:	Koichiro Ikudome, et al.
Application No.	:	09/295,966
Filed	:	April 21, 1999
Title	:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
Grp./Div.	:	2766
Examiner	:	Not Assigned
Docket No.	:	34503/WWM/A522

INFORMATION DISCLOSURE STATEMENT AND CERTIFICATION UNDER § 1.97(e)(1)

Post Office Box 7068
Pasadena, CA 91109-7068
October 22, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

Commissioner:

In compliance with the duty of disclosure under 37 CFR §§ 1.56, 1.97 and 1.98, and in accordance with the provisions in the Manual of Patent Examining Procedure §§ 609 and 707.05(b), enclosed is FORM PTO-1449 with a listing of references that are known to applicant. Copies of each of the listed references are enclosed.

It is respectfully requested that these references be considered in the examination of this application and identified on the list of references cited on the patent issuing on this application. Applicant also requests that an initialed copy of said FORM PTO-1449 be entered in the application file and returned to applicant with the next communication from the Office in accordance with MPEP § 609.

Applicant's undersigned attorney hereby certifies, in accordance with 37 CFR § 1.97(e)(1), that the above information was cited in a communication from a foreign Patent Office in a counterpart foreign application not more than three months prior to the filing of this statement.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By

Wesley W. Monroe
Reg. No. 39,778
626/795-9900

WWM/amb
Enclosures: PTO 1449, w/references

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06, G06F 9/445	A1	(11) International Publication Number: WO 98/26548 (43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/10600

(22) International Filing Date: 18 June 1997 (18.06.97)

(30) Priority Data:
08/762,737 10 December 1996 (10.12.96) US

(71) Applicant *(for all designated States except US)*: WHISTLE COMMUNICATIONS CORPORATION [US/US]; Suite 100, 110 Marsh Drive, Foster City, CA 94404 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LI, Jim, Y. [US/US]; 2946 Polk Street, San Francisco, CA 94117 (US). COBBS, Archie, L. [US/US]; 114 Frederick Street, #17, San Francisco, CA 94117 (US). OZZELLO, Paul, D. [US/US]; 990 Fulton, #506, San Francisco, CA 94117 (US).

(74) Agent: HICKMAN, Paul, L.; Hickman Beyer & Weaver, P.O. Box 61059, Palo Alto, CA 94306 (US).

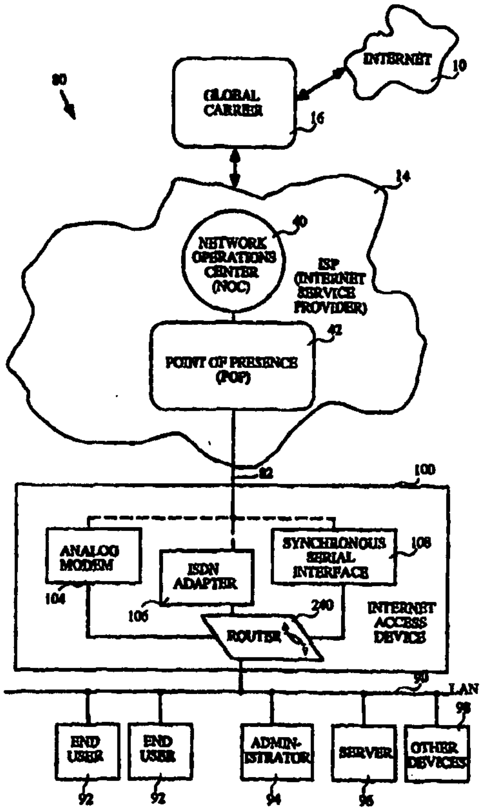
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AUTOMATIC CONFIGURATION FOR INTERNET ACCESS DEVICE

(57) Abstract

An Internet access device (100) uses an automatic configuration process (600) to handle the task of configuring the Internet access device at a customer site for communication with the Internet (10). Once configured, the customer has electronic mail and other access to the Internet from his local area network. A not yet configured Internet access device is shipped directly to a customer without having to be manually configured first. The customer enters a registration identification number (326) and a telephone number onto the Internet access device. The Internet access device then automatically connects to the Internet, downloads configuration data from a configuration server (410) containing customer site specific configuration data, and then automatically configures itself for communication with the Internet. The Internet access device is simple to install for a customer and provides valuable features such as a router (240), firewall, e-mail gateway (212), web server (220), and other servers (222). The Internet access device initially connects to the Internet through an Internet service provider (14) over a standard analog telephone line using a standard modem (52) and using a dynamic IP address. Once automatically configured, the Internet access device may then communicate with the Internet using any suitable connection including an analog telephone line, or a higher-speed line such as an ISDN line or a frame relay circuit and is assigned a static IP address and a range of IP addresses for other devices on its local area network.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

AUTOMATIC CONFIGURATION FOR INTERNET ACCESS DEVICE

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to PCT International Application No. _______________ (Attorney Docket No. WSTLP002.P), entitled "Automatic Setup Of Services For Computer System Users", filed on the same date herewith, which claims priority of U.S. Patent Application Serial No. 08/762,736 filed on December 10, 1996, both of which are incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computing systems and communications networks. More specifically, the present invention relates to automatically configuring a computing system for communication with a communications network.

BACKGROUND OF THE INVENTION

In recent years, the popularity of the Internet has been increasing dramatically. Every day, more and more home users, small business users and large corporations are connecting to the Internet to improve communication. The term "Internet" (upper-case "I") refers to that particular global communications network that is in use around the world and that grew out of a U.S. Department of Defense funded research project named the ARPANet. Currently, most of the Internet is commercially owned and is an extremely complex, highly redundant network of telecommunications circuits that are connected together with routers. The "Internet" refers to a particular network of communications networks, while, in general, any interconnection of networks may be termed an "internet" (lower-case "i"). The "Internet" is one example of an "internet". Currently, the Internet is used for a variety of services including communication, education, news, advertising, reference materials, broadcast like media, financial services, and other.

The Internet may be described in a very simplistic sense as follows. There are six major global telecommunications carriers each of which maintains a global telecommunications network. Examples of these global carriers are companies such as SPRINT or MCI. These global carriers have links between each of their networks to allow communication between the networks. Companies termed Internet service providers (ISPs) lease access to these global networks from one of the global carriers and provide this access to their customers such as businesses, universities and individuals. These ISPs maintain their own IP (Internet protocol) networks that are connected to the Internet. An IP network of an ISP allows an ISP to establish a presence in many different locations around the country, so that customers will have local dial-in access or a short leased-line access to the IP network. Once a customer gains access to the IP network, he or she has access to the Internet. In reality, a hierarchy of local access providers, network service providers, and network access providers provide a link from a customer to the Internet.

In general, it can be said that connecting a computer or computer network to the Internet is not a simple task. Many configuration variables must be taken into account including whether the computer is a single host at a home, or is part of a local area network (LAN) in a corporation, whether a customer desires a dynamic or static IP address, and what type of line connection the customer desires. In general, a customer connects to the Internet using either a dial-up telephone line, or a more permanent leased line connection. Most home or casual use customers connect to the Internet through a dial-up line using a modem, while corporate or heavy use customers often connect with a permanent leased line connection.

Another distinction between customers relates to the type of address on the Internet used by the customer. An IP (Internet protocol) address represents a communications end point. This may or may not correlate to a user. For example, time-sharing or multi-user systems have many users per address. Typically though, each end point will have a unique IP address (or IP number or "dotted quad"). Each IP address has four parts separated by dots, e.g., "101.100.2.2", and is a 32-bit number. A router that directs information to various end hosts has an IP address such as "101.100.2.1", where the last part will be a unique number identifying the end hosts that are attached to the router. For example, for three hosts connected to such a router, these hosts may have IP addresses of 101.100.2.2, 101.100.2.3, and 101.100.2.4.

A home or casual use customer who only dials up to connect to the Internet occasionally, may only need a dynamic or temporary address for that session only. This dynamic IP address is unique for that user for only a particular transaction. Once the user has disconnected from the Internet, the dynamic IP address may be reassigned to another user. However, providers of services or information on the Internet require a permanent or static IP address so that other users may access this information at any time using a known address. Corporate customers having a web site and a domain name may also require one or more static IP addresses. Another configuration variable is that customers may choose between a variety of types of connections to the Internet that are offered by an ISP. For example, a casual use customer may choose to use a modem on a dial-up line to access the Internet, or may choose to use an ISDN (integrated services digital network) adapter in order to access the Internet over a dial-up ISDN line. A corporate or heavy use customer may wish to utilize a permanent leased line connection to the Internet that uses frame relay technology for high-speed access.

Thus, there are complexities and difficulties involved with connecting a computer or LAN to the Internet and configuring the computer or LAN for communication with the Internet. One such difficulty is that routers both at the ISP and in the customer's computer must be configured correctly. At the ISP, a trained network operator is available for entering configuration information into the router such as the IP address of a customer, an account number, etc. Other configuration information that must be entered includes telephone numbers to dial, passwords, packet filter rules, LAN network information, domain name information, e-mail configuration, compression parameters, etc. Once this is done, however, the customer must be told of this information and then must manually enter this same information into his own networking hardware in order to configure a router, for example. This duplicity of entering information is tedious for the customer, and is prone to errors. Also, a configuration will be different depending upon whether a customer wishes to access the Internet using a modem, an ISDN line, a frame relay circuit, or other high-speed line.

Furthermore, connecting a LAN is considerably more difficult than connecting a single host as it requires the correct installation and configuration of a wide variety of interrelated systems. By way of example, routers, firewalls, DNS servers and DHCP servers, etc. must all be configured correctly before the LAN can successfully communicate with the Internet. Connecting a LAN is an all-or-nothing proposition. The minimum equipment necessary includes a firewall, router, and DNS server. Configuring this equipment correctly typically requires an IP networking engineer. This fact represents a significant obstacle to the wide adoption of Internet technologies, particularly amongst the majority of small business organizations. Internet service providers relying on the current state-of-the-art in networking equipment are unable to engage any customers but the technical elite.

Therefore, the automation of the setup of a full-service IP LAN network for communication with the Internet is desirable. It would further be desirable to have an Internet access device and configuration process for configuring a computer system to communicate with the Internet that is not prone to error and that is secure. It would be further desirable for this configuration process to be automatic, and for the configuration process to be able to use the existing infrastructure of the Internet in order to retrieve configuration data from any location. It would further be desirable if a customer need only perform a minimum of tasks and need only enter a minimum of information into such an

Internet access device in order for that device to be automatically configured for communication with the Internet.

SUMMARY OF THE INVENTION

To achieve the foregoing and other objects and in accordance with the purpose of the present invention, an Internet access device is disclosed that uses an automatic configuration process to handle the task of configuring the Internet access device at a customer site. This process allows a not yet configured Internet access device to be shipped directly to a customer without having to be manually configured first. In some embodiments, the customer simply enters a registration identification number and a telephone number onto the front panel of the Internet access device. The Internet access device then automatically connects to the Internet, downloads configuration data from a configuration server containing customer site specific configuration data, and then automatically configures itself for communication with the Internet.

In one embodiment, an Internet access device is a communications apparatus with at least two physical interfaces for connecting a LAN to the Internet over a wide area communications link. In addition to routing network data, an Internet access device may provide one or more related services to the LAN such as a domain name service, a DHCP service, security, electronic mail, etc.

In one embodiment, the Internet access device initially connects to the Internet through an Internet service provider over a standard analog telephone line using a modem that requires no configuration on the part of the customer. Once automatically configured, the Internet access device may then communicate with the Internet using either the analog line or a higher-speed line such as an ISDN line or a frame relay circuit.

In another embodiment, the Internet access device initially connects to the Internet acting as a single host computer, using a dynamic IP address as its address, requiring no configuration on the part of the user. Once automatically configured, the Internet access device may then act as a router, communicating with the Internet using a static IP address and a range of IP addresses for other devices on a local area network.

An Internet access device is as painless and simple to install for a customer as possible, while at the same time providing valuable features such as a router, firewall, e-mail gateway, web server, and other servers. The Internet access device is able to connect to a configuration server using the standard infrastructure of the Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 illustrates an embodiment of a global communications network including an Internet service provider.

FIG. 2 illustrates an embodiment of an IP network of an Internet service provider.

FIG. 3 illustrates an embodiment of a point of presence (POP) for an Internet service provider that has connections for various communications devices used by customers.

FIG. 4 illustrates an embodiment of an Internet access device that allows communication between the Internet and a local area network of a customer site.

FIG. 5 illustrates an embodiment of the hardware architecture of an Internet access device suitable for use in accordance with the present invention.

FIG. 6 illustrates an embodiment of the software architecture of the Internet access device illustrated in FIG. 5.

FIG. 7 illustrates an embodiment of a process by which a registration identification number is formed and then encrypted into decimal digits.

FIG. 8 illustrates how an Internet access device may connect to a configuration server on the Internet using a dynamic IP address.

FIG. 9 illustrates how an Internet access device may be permanently connected to the Internet using a static IP address.

FIG. 10 is a flowchart illustrating a method for automatically configuring an Internet access device for communication with the Internet in accordance with one embodiment of the present invention.

FIGS. 11A and 11B are flowcharts illustrating one method of accomplishing the automatic configuration process step of Figure 10.

FIG. 12 is a flowchart illustrating one method of accomplishing the Internet access device configuration step of Figure 11B.

DETAILED DESCRIPTION OF THE INVENTION

In general, there are at least four components to any internet and to the Internet in particular. These four components include server computers, client computers, networks and routers. These components communicate with each other mainly over leased lines provided by the global carriers. A server is any computer on which information is stored and from which other computers, called clients, can retrieve that information. A client computer is a computer used for accessing the Internet, retrieving information from server computers, entering data, and performing other data processing work. A client computer may be used for word processing, sending e-mail, retrieving information from the Internet, transferring files, and many other tasks. A network is any interconnection of computers using wires, switches, network adapters, etc., that allow these computers to communicate. A network may be a local area network (LAN), for example, or may be a wide area network (WAN). Networks are classified as LANs or as WANs depending upon their geographic reach. Networks are connected to each other via routers or gateways, forming internets.

Figure 1 shows a global communications internet 10 that in one embodiment is the Internet. The Internet has any number of Internet service providers (ISPs) 12 and 14 that connect a communication line 18 to a global carrier 16. Global carriers 16 and 22 may be one of the commercial Internet backbone providers such as SPRINT or MCI. Each global carrier has its own separate communications network 20. Communication lines 18 are typically T-1, T-3 or other high-speed lines. An ISP 14 may connect to a global carrier 16 through a hierarchy of providers. For example, ISP 14 may connect through a network service provider such as Netcom Online, UUNET or ANS, which in turn communicate via a network access provider such as the California Network Access Provider in order to communicate with the global carrier. Each of the global carriers may communicate with each other and with a vBNS 28 (very high speed Backbone Service) through a number of Network Access Points (NAP) 26 and communication lines 24. An ISP 14 includes IP networks 30 and 32 each having their own network of communication lines 34. The global carriers 16 and 22 control the physical portions of the Internet including the wires, fiber-optics and the switching equipment. The global carriers lease access to parts of their network to the ISPs, which in turn sell access to the Internet to their customers.

Figure 2 illustrates in greater detail an IP network 30 as shown in Figure 1. Typically, an Internet service provider offers local access to the Internet to its customers through such an extended IP network 30 that consists of perhaps hundreds of points of presence that are connected by high-speed dedicated lines that are leased from a telecommunications provider. The IP network 30 may be one of many IP networks that are managed by an Internet service provider. IP network 30 contains any number of points of presence (POPs) 42 that are interconnected with each other and to a network operation center (NOC) 40. The network operations center 40 contains hardware, software and systems for managing and monitoring the IP network 30.

IP network 30 connects over one or more high-speed lines 46 to a global carrier 16. Typically, each POP 42 is connected to another POP and eventually to the NOC via a high-speed leased line 44 using a T-1 or T-3 circuit. Each point of presence 42 has any number of feeder lines 48 that connect the POP to a customer 50. The Internet customer 50 may be one of a wide variety of Internet customers. By way of example, customer 50 may be a casual user dialing in from their home with a single computer, a corporate user, a single computer in a corporation, a router which is used to connect any number of other computers in a local area network to the Internet, a computer used for connecting a corporate intranet to the Internet, or other similar connection. Feeder lines 48 may be dial-up or leased lines, or other type. In general, the communication lines shown take a wide variety of forms. By way of example, lines may be traditional telephone copper wire pairs, a permanently installed wire, a cable system coaxial cable, fiber optic cable, a microwave or other electromagnetic transmission device, or other communication line.

Figure 3 illustrates an embodiment of a POP 42 as shown in Figure 2. POP 42 has a connection 44 to either another POP, a NOC of an IP network, or even directly to a global carrier. POP 42 also has feeder lines 48 for connecting to various Internet customers. The type of feeder line 48 may vary depending upon the service desired by the Internet customer. By way of example, a customer may connect to the POP using an analog modem 52 over a switched dial-up telephone line. This line may be a plain old telephone service (POTS) line at up to speeds of 56 Kbps. A customer may also connect to a POP using an ISDN adapter 54 that connects over a switched digital telephone line. A customer may also connect to a POP using a synchronous serial interface 56 utilizing a frame relay standard over a high-speed leased digital line such as a T-1 or T-3 line. Such a customer may be part of a large corporate site that uses a wide area router to communicate information to any number of users at the corporate site. Communication may also take place between a customer and the POP using existing cable television network lines. In this case, a customer may have a cable modem 58 for connecting to the POP. Other types of lines and hardware interfaces for connecting with a POP are possible.

A typical POP contains a distribution router 62 connected to a local area network 64 that distributes information among various servers and various hardware interfaces for outside communication to Internet customers. A wide variety of servers may be present within the POP. By way of example, the POP includes an e-mail server 66, a world wide web server 68 and other servers 70 such as a DNS server, news server, etc. By way of example, the distribution router 62 may take the form of a Cisco 7000 router available from