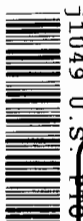


03/31/03



11049 U.S. PTO

Please type a plus sign (+) inside this box → ☐

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.

Approved for use through 10/31/2002. OMB 0651-0032

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

**UTILITY
PATENT APPLICATION
TRANSMITTAL**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	TTCC-01021US0
First Inventor	Hasan S. Alkhatib
Title	SECURE VIRTUAL COMMUNITY NETWORK SYSTEM
Express Mail Label No.	EV 251 363 937 US

JC398 U.S. PTO
10/403818
03/31/03**APPLICATION ELEMENTS**

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☐ Applicant claims small entity status.
See 37 CFR 1.27.
3. ☒ Specification [Total Pages **83**]
(preferred arrangement set forth below)
 - Descriptive title of the invention
 - Cross Reference to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to sequence listing, a table, or a computer program listing appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
4. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets **21**]
5. Oath or Declaration [Total Pages **1**]
 - a. ☐ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 CFR 1.63 (d))
(for continuation/divisional with Box 18 completed)
 - i. ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s)
named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - a. ☐ Computer Readable Form (CRF)
 - b. Specification Sequence Listing on:
 - i. ☐ CD-ROM or CD-R (2 copies); or
 - ii. ☐ paper
 - c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Request and Certification under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☐ Other:

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP)

of prior application No.: _____ / _____

Prior application information:

Examiner: _____

Group Art Unit: _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS☒ Customer Number or Bar Code Label**28554**

(Insert Customer No. or Attach bar code label here)

or ☐ Correspondence address below

Name	Burt Magen, Esq.				
Address	Vierra Magen Marcus Harmon & DeNiro, LLP 685 Market Street, Suite 540				
City	San Francisco	State	California	Zip Code	94105-4206
Country	U.S.A.	Telephone	(415) 369-9660	Fax	(415) 369-9665

Name (Print/Type)	Burt Magen	Registration No. (Attorney/Agent)	37,175
Signature		Date	March 31, 2003

Burden Hour Statement: This form is estimated to take 62 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

10403318-00000000

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Inventors

Hasan S. Alkhatib
Fouad A. Tobagi
Farid F. Elwailly

Express Mail No: EV 251 363 937 US

PREPARED BY
VIERRA MAGEN MACUS HARMON & DENIRO LLP
CUSTOMER ID: 000028554

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is related to the following Applications: U.S. Patent
5 Application No. 10/233,289, "Accessing An Entity Inside a Private Network," filed
on August 30, 2002; U.S. Patent Application No. 10/161,573, "Creating A Public
Identity For An Entity On A Network," filed on June 3, 2002; U.S. Patent
Application No. 10/233,288, "Communicating With An Entity Inside A Private
Network Using An Existing Connection To Initiate Communication," filed on
10 August 30, 2002; U.S. Patent Application "Secure Virtual Address Realm," filed
on March 31, 2003, Atty. Docket TTCC-01020US0; and U.S. Patent Application
"Group Agent," filed on March 31, 2003, Atty. Docket TTCC-01022US0. All
these related applications are incorporated herein be reference in their entirety.

15

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention is directed to a network services system.

20

DESCRIPTION OF THE RELATED ART

Networked data devices provide users with efficient means for
communication and collaboration. In recent years, the Internet has played a
central role in allowing different types of networked devices to connect and
25 share information across a myriad of networks. As technology advances and
more organizations and people rely on the Internet, new challenges are

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.app

Express Mail No: EV 251 363 937 US

presented for enhancing the ability to communicate. One such challenge is to enable the rapid creation of a secure means that allows local and remote specified entities to communicate and collaborate from any location via a standard Internet connection. For any solution to be widely accepted, it must
5 take into account the realities and limitations currently existing.

For communication on the Internet, the Internet Protocol (IP) has become the default protocol used by most hosts and to which communication applications are now written. To transmit data from a source to a destination, the Internet Protocol uses an IP address. An IP address is four bytes long and
10 consists of a network number and a host number. When written out, IP version 4 addresses are specified as four numbers separated by dots (e.g. 198.68.70.1). Users and software applications do not always refer to hosts or other resources by their numerical IP address. Instead of using numbers, they use ASCII strings called domain names. The Internet uses a Domain Name System (DNS) to
15 convert a domain name to an IP address.

The Internet Protocol has been in use for over two decades. It has worked extremely well, as demonstrated by the exponential growth of the Internet. Unfortunately, the Internet is rapidly becoming a victim of its own popularity, it is running out of addresses.

20 One popular solution to the depleting address problem is Network Address Translation (NAT). This concept includes predefining a number of network addresses to be private addresses and public addresses. Public addresses are unique addresses that should only be used by one entity having access to the Internet. That is, no two entities on the Internet should have the
25 same public address. Private addresses are not unique and are typically used for entities not having direct access to the Internet. Private addresses are used in private networks. Private addresses can be used by more than one

organization or network. NAT assumes that all of the machines on a network will not need to access the Internet at all times. Therefore, there is no need for each machine to have a public address. A local network can function with a small number of one or more public addresses assigned to a NAT device. The remainder of the machines on the network will be assigned private addresses. Since entities on the network have private addresses, the network is considered to be a private network.

When a particular machine having a private address on the private network attempts to initiate a communication to a machine outside of the private network (e.g. via the Internet), the NAT device will intercept the communication, change the source machine's private address to a public address and set up a table for translation between public addresses and private addresses. The table can contain the destination address, port numbers, sequencing information, byte counts and internal flags for each connection associated with a host address. Inbound packets are compared against entries in the table and permitted through the NAT device only if an appropriate connection exists to validate their passage. One problem with a many NAT implementations is that it only works for communication initiated by a host within the private network to a host on the Internet that has a public IP address. Many NAT implementations will not work if the communication is initiated by a host outside of the private network and is directed to a host with a private address in the private network.

For most organizations, the security of devices coupled to the Internet is a concern. As a result, not all devices are directly connected to or accessible via the Internet. Rather, many devices are placed in private networks for security concerns (in addition to the address usage issue describe above). Many private networks are secured by placing a firewall device between the private network and the Internet.

Another problem with many current communication schemes is that mobile computing devices can be moved to new and different networks, including private networks. These mobile computing devices may need to be reachable so that a host outside of the private network can initiate
5 communication with the mobile computing device. However, in this case the problem is two-fold. First, there is no means for allowing the host outside of the private network to initiate communication with the mobile computing device. Second, the host outside the private network does not know the address for the mobile computing device or the network that the mobile computing device is
10 currently connected to.

Thus, there is a need for a system that provides for local and remote entities to communicate and collaborate using the Internet, can work with existing NAT devices and firewalls, and allows for devices to move to different physical networks. To increase the ability of such a system to be accepted by
15 the Internet community, it is desirable for such a system to not require changes to existing applications, allow peer-to-peer applications to communicate directly across the Internet and to not require changes to existing protocols. Each of these issues will be discussed below.

Large amounts of resources have been used to purchase and deploy
20 existing applications currently running on the millions of computing devices. Organizations and individuals are not likely to want to adopt new communications solutions that require them to absorb the additional cost of replacing all of their applications.

To provide efficient and secure communication, it is desirable for devices
25 to have the ability to allow their IP based applications to communicate directly with each other. By allowing peer-to-peer applications to communicate directly across the Internet, security is enhanced since the recipient is specifically

identified and communication is passed directly between the applications on two or more respective machines.

Most machines on the Internet use the TCP/IP (Transmission Control Protocol/Internet Protocol) reference model to send data to other machines on the Internet. The TCP/IP reference model includes four layers: the physical and data link layer, the network layer, the transport layer, and the application layer. The physical layer portion of the physical and data link layer is concerned with transmitting raw bits over a communication channel. The data link portion of the Physical and Data Link layer takes the raw transmission facility and transforms it into a line that appears to be relatively free of transmission errors. It accomplishes this task by having the sender break the input data up into frames, transmit the frames and process the acknowledgment frames sent back by the receiver.

The network layer permits a host to inject packets into a network and have them travel independently to the destination. On the Internet, the protocol used for the network layer is the Internet Protocol (IP).

The transport layer is designed to allow peer entities on the source and destination to carry on a "conversation." On the Internet, two protocols are used. The first one, the Transmission Control Protocol (TCP), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error to another machine on the Internet. It fragments the incoming byte stream into discrete segments and passes each one to the network layer. At the destination, the receiving TCP process reassembles the received segments into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more segments than it can handle. The second protocol used in the transport layer on the Internet is the User Datagram Protocol (UDP), which does not provide the

TCP sequencing or flow control. UDP is typically used for one-shot, client server type requests-reply queries for applications in which prompt delivery is more important than accurate delivery.

The transport layer is typically thought of as being above the network
5 layer to indicate that the network layer provides a service to the transport layer. Similarly, the transport layer is typically thought of as being below the application layer to indicate that the transport layer provides a service to the application layer.

The application layer contains the high level protocols, for example,
10 Telnet, File Transfer Protocol (FTP), Electronic Mail - Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP).

Fig. 1 depicts the basic structure of an IP version 4 packet 10 used at the
Network Layer. IP packet 10 consists of header 12 and payload 14. Payload 14 stores the data received from the Transport Layer in the TCP/IP model. Fig. 2
15 depicts the format of a header of an IP packet. The header is depicted to include six rows. The first five rows are 32 bits wide. The first five rows of the header comprise a 20 byte fixed portion of the header. The last row of the header provides a variable sized options field 22. Version field 24 keeps track of which version of the protocol the packet belongs to. The current version used
20 on the Internet is version 4. IHL field 26 describes the length of the header in 32 bit words. Type field 28 indicates the type of service requested. Various combinations of reliability and speed are possible. Length field 30 contains the size of the packet, including both the header and the data. Identification field 32 is needed to allow the destination host to determine which packet the received
25 fragment belongs to. All fragments of a packet contain the same identification value. Next comes three flags, which include an unused bit 33 and then two 1 bit fields 34 and 36. DF field 34 stands for don't fragment. It is an order to the

-7-

5 routers not to fragment the packet because the destination is incapable of putting the pieces back together again. MF field 36 stands for more fragments. All fragments except for the last one have this bit set. Fragment offset field 38 indicates where in the current segment this fragment belongs. Time to Live field 40 is used to limit packet lifetime. It is supposed to count time in seconds, allowing a maximum life time of 255 seconds. In practice, it may count hops (or hops and seconds). The time is decremented on each hop by a router. When the time to live hits 0, the packet is discarded and a warning is sent back to the source using an Internet Control Messaging Protocol (ICMP) packet. This feature prevents packets from wandering around forever. Protocol Field 42 indicates which transport layer type is to receive the segment. TCP is one possibility, UDP is another. Checksum field 44 verifies the header. One method for implementing a checksum is to add up all 16 bit half words constituting the header and take the ones compliment of the result. Note that the checksum must be recomputed at each hop because the Time to Live field 40 changes or the content of the options field changes. Source field 46 indicates the IP address for the source of the packet and destination field 48 indicates the IP address for the destination of the packet. Options field 22 is a variable length field designed to hold other information. Currently, options used on the Internet indicate security, suggested routing path, previous routing path and time

25 UDP is an alternative to TCP. Fig. 2B depicts the structure of a packet that uses UDP. Like the TCP, UDP uses the Internet Protocol to actually send a data unit from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP does not provide sequencing of the packets that the data arrives in. Hence, application programs using UDP must ensure that the entire message has arrived and is in the right order. As

shown in Fig. 2B, the packet includes and IP header 12a and IP payload 14a. The payload 14a comprises the UDP header 50 and UDP data 60. UDP header 50 consists of a 16 bit source port identifier, a 16 bit destination port identifier, a length field and checksum field. In Fig. 2B, the Destination Port has a meaning
5 within the context of a particular Internet destination address, and the Length field is the length in octets of this user datagram including its header and the data. The checksum is the 16-bit one's complement of the sum of consecutive two octaves of a pseudo header of information from the IP header, the UDP header, and the data (padded with zero octets at the end, if necessary, to make
10 a multiple of two octets).

In addition to using the existing Internet infrastructure, another issue in allowing public-to-private, or private-to-private, communications lies in the addressing of the devices. Where a system is coupled to the public Internet with an IP address, communication packets can be routed directly to the machine.
15 However, many devices couple to the Internet via service providers which provide them with a dynamic IP address. Thus, those wishing to communicate with this type of user must know the constantly changing address of the user in order to communicate with them. Still other hosts may be coupled to networks that use technologies other than IP.

20 One solution currently in use that provides for local and remote specified entities to communicate and collaborate using the Internet is the Virtual Private Network ("VPN"). The VPN uses additional network software layers to increase security between users in the public realm and those in private realms. For example, some VPNs encrypt packets using IPsec (or other protocols). The
25 encrypted packets are then encapsulated within a standard packet and transmitted across the Internet to the destination. At the destination, the encrypted packet is decrypted. While the exiting VPN provides remote users

with secure access to a network, via the Internet, many existing VPNs have various shortcomings that prevent them from satisfying the needs of many users. For example, many VPNs do not provide for peer-to-peer communication with IPsec (or other security measures), do not work though NAT devices in all
5 cases, are difficult to set up and maintain, do not provide for full mobility of entities communicating on the VPN, and do not always provide for communication with entities in the various private network configurations discussed herein.

One method of overcoming the mobility problem includes the use of
10 Dynamic DNS. More information about Dynamic DNS can be found in RFC 2136 incorporated herein by reference.

Dynamic DNS is illustrated in Fig. 3. Figure 3 shows a first computer or device B having a host name of B.CO.b.com having a dynamic or static private IP address IPb and a second computer or device A having a host name of
15 A.CO.a.com and having a dynamic or static private IP address IPa. Devices B and A are coupled to the Internet 506 via firewall devices 302, 304 incorporating NAT. The addresses of B and A, as seen by devices on the Internet, are public IP addresses GIPb and GIPa, respectively. Also shown is device D, having a publicly address IPd and a host name of d.CO.d.com.

20 Also shown is a Dynamic DNS server, DDNS, residing on the Internet. In essence, the DDNS server is a DNS server supporting the dynamic DNS protocol of RFC 2136, and in this example is an authoritative name server containing records for B, A and D. The DDNS server will update it's records of B, A and D in real time, so that if or when D's address IPd changes, any query
25 by other devices (B, A, for example) based on D's host name, will result in the response being the correct IP – IPd. Any DNS records for devices B and A will

always reflect the public IP addresses (GIPa and GIPb) of the firewall/NAT devices.

Unfortunately, DDNS technology is complex and difficult to implement securely--two factors that have dramatically slowed the rate of deployment of
5 Dynamic DNS. As a result, VPNs have not been able to adopt DDNS to solve all of the problems discussed herein.

Hence, a system is desired that allows local and remote entities to communicate and collaborate from any location via a standard Internet connection and which solves the problems discussed above.

10

SUMMARY OF THE INVENTION

A system is disclosed that desired that allows local and remote entities to communicate and collaborate from various locations. In one embodiment, the
15 system makes use of a virtual subnet with a virtual address realm. The virtual address realm allows two or more users to communicate securely via at least one public network, whether the users are both coupled directly to the public network, both coupled directly to separate private networks or whether one is in a public network and one is in a private network. The virtual address realm uses
20 virtual addresses to identify the devices on the virtual subnet. Although the devices are in different physical subnets, from the point of view of the applications the devices of the virtual subnet appear to be in one local subnet.

In one embodiment, the virtual address realm comprises a virtual address realm definition including at least a set of users. Each user accessing the virtual
25 address realm may have at least one virtual address in the virtual address realm and at least one physical address.

Another embodiment of the present invention comprises a virtual community network for transmitting communications via at least one physical

network. The virtual community network comprises a virtual address realm including a logical name assignment, a set of users capable of communicating in the virtual address realm, and a secure communication channel. In a further aspect, the virtual community network logical name is a domain name, and the domain name may be a fully qualified domain name or a virtual domain name. In another aspect, the set of users includes at least a first user coupled to a first private physical network and a second user coupled to a second private physical network, and the first private physical network and the second private physical network may have at least one common private physical subnet address. The physical addresses may be dynamic or static.

Yet another embodiment of the invention is a method comprising the steps of: defining a virtual address realm overlying a public address realm, the virtual address realm including at least a user set and a logical name for said user set; and routing communications between users in the user set by means of virtual address realm addresses. In a further aspect, this method includes the step of registering users in the user set as members of the virtual address realm. Further, the method may include the step assigning each registered user a unique virtual address in the virtual address realm. The method may further include the steps of encrypting communications between devices in the realm, and/or applying at least one address realm group policy.

A further embodiment of the invention is a method for providing secure communications between two devices. The method comprises the steps of: providing a virtual realm identifier; defining a set of users for the virtual realm; registering users in the realm; assigning virtual addresses; and routing information between users in said virtual address realm.

A still further embodiment of the invention comprises one or more processor readable storage devices having processor readable code embodied

on said processor readable storage devices. In this embodiment, said processor readable code is for programming one or more processors to perform a method comprising the steps of: providing a virtual address realm configuration including a user set and a domain name for said user set; and
5 routing communications between users in said virtual address realm.

Another embodiment of the invention comprises a method for providing a secure virtual network. The method may include the steps of: providing a virtual network manager coupled to a public network; defining a member set of users entitled to communicated in the virtual network; registering members with the
10 manager; assigning members a virtual address; and routing network traffic between the members in the virtual community.

An additional further embodiment of the invention may comprise one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices. The processor readable
15 code may be for programming one or more processors to perform a method comprising the steps of: managing a virtual community network realm; defining a member set of users entitled to communicated in the virtual community; registering users with the virtual community; assigning each user a virtual address; and routing network traffic between the users in the virtual community.

20 Another embodiment of the invention is a virtual community network system. The system includes a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set; and at least one route director capable of communicating with users in the user set.

25 In a further aspect, the virtual community network includes a communication agent installed on a device. The agent may comprise a virtual

network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address.

For some devices, additional software or hardware cannot be installed on a member device or it is not desirable to install such additional software or hardware on the device. For such devices, a Group Agent can be used. The
5 Group Agent acts as a proxy for one or more members of a virtual community without requiring installation of member agent software on the client devices.

One embodiment of a system that uses a Group Agent includes communicating with a first client and acting as an intermediary between the first
10 client and members in a first virtual address realm so that the first client can communicate in the first virtual address realm. Note that in this embodiment the first client is not configured to communicate in the first virtual address realm. For example, no software is installed on the client to add drivers, layers or interfaces specific to the first virtual address realm.

15 Another embodiment of a system using a Group Agent includes communicating messages with a first client and communicating the messages with members in a virtual address realm on behalf of the first client. While communicating with the first client, the messages do not use virtual addresses. During the communication process, the messages are transformed so that the
20 messages include virtual addresses when communicating with members in the virtual address realm and the messages do not include virtual addresses when communicating with the first client.

In one implementation, the first entity resides in a first physical address realm and the second entity resides in a second physical address realm, where
25 the first physical address realm overlaps with the second physical address realm. For example, consider the situation where the first physical address realm is a first private network using a first set of private addresses and the

second physical address realm is a second private network using a second set of private addresses, where there are private addresses that exist in both the first set of private addresses and the second set of private addresses.

5 The present invention can be accomplished using hardware, software, or a combination of both hardware and software. The software used for the present invention is stored on one or more processor readable storage media including hard disk drives, CD-ROMs, DVDs, optical disks, floppy disks, tape drives, RAM, ROM or other suitable storage devices. In alternative
10 hardware including custom integrated circuits, gate arrays, FPGAs, PLDs, and special purpose computers. In one embodiment, software implementing the present invention is used to program one or more processors. The processors can be in communication with one or more storage devices, peripherals and/or one or more communication interfaces.

15 These and other objects and advantages of the present invention will appear more clearly from the following description in which the preferred embodiment of the invention has been set forth in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

20 The invention will be described with respect to the particular embodiments thereof. Other objects, features, and advantages of the invention will become apparent with reference to the specification and drawings in which:

Fig. 1 depicts an IP packet.

Fig. 2A depicts the format of a header of an IP packet.

25 Fig. 2B depicts the format of a UDP packet.

Fig. 3 depicts a print-out implementation of a dynamic routing system.

Fig. 4 depicts a block diagram of an implementation of the system of the present invention.

Fig. 5A is a structural network block diagram illustrating elements used in the system of the present invention.

5 Fig. 5B is a logical block diagram depicting communication types in an implementation of the system of the present invention

Fig. 6A depicts a packet structure for a communication packet in accordance with the present invention.

Fig. 6B is a table depicting the shim configuration of the packet in Fig. 6.

10 Fig. 7 is a flow chart describing the overall process for communicating.

Fig. 8 is a block diagram illustrating the structure of the Member Agent application in the system of the present invention.

Fig. 9 is a flowchart illustrating the steps which occur in the creation of a virtual community.

15 Fig. 10 is a flowchart illustrating the process of configuring a virtual community.

Fig. 11 depicts an HTTP wrapper structure.

Fig. 12A is a flow diagram depicting a user registration process of the present invention.

20 Fig. 12B is a table illustrating the structure of the registration file information structure.

Fig. 13 is a flowchart depicting a member join process in accordance with the present invention.

25 Fig. 14 is a flowchart depicting a member leave request in accordance with the present invention.

Fig. 15 is a flow diagram depicting DNS request for a member in the virtual community in accordance with the present invention.

-16-

Fig. 16A depicts the commonly used IKE phase one aggressive mode exchange.

Fig. 16B depicts the IKE phase one aggressive mode exchange used in accordance with the present invention.

5 Fig. 17 depicts a packet structure of the virtual IKE phase 1 packet.

Fig. 18 depicts the IKE ticket payload data structure.

Fig. 19 is a representation of a system ping sequence in accordance with the present invention.

10 Fig. 20 is a flow diagram depicting a query request in the system of the present invention.

Fig. 21 depicts a flow structure for addressing and routing conducted by a Route director.

Fig. 22 is a block diagram depicting one embodiment of various components of the present invention utilizing a Group Agent.

15 Fig. 23 is a flow chart describing one embodiment of the process for Group Agent initialization.

Fig. 24 is a flow chart describing one embodiment of a process for initiating communication with a member that is using a Group Agent.

20 Fig. 25 is a flow chart describing one embodiment of a process for communicating using a Group Agent.

Fig. 26 is a flow chart describing one embodiment of a process for initiating communication by a member that is using a Group Agent.

DETAILED DESCRIPTION

25 One embodiment of the present invention provides for a secure Virtual Community Network or "VCN." In essence, a VCN is a private dynamic network which acts as a private LAN for computing devices coupled to public networks or

-17-

private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. Thus, the invention provides a separate private virtual address realm, seen to each user as a private network while seamlessly crossing public and private network
5 boundaries.

A basic overview of the system is shown in Fig. 4. Fig. 4 shows a computer or device B (host name - b.CO_b.com) in a first private domain and computer or device A (host name - a.CO_a.com) in a second private domain, both of which are coupled to the Internet by firewall devices 402, 404. The
10 firewall devices are configured to implement Network Address Translation (NAT). A and B have dynamic or static private IP addresses. Computer or device X is coupled directly to the public Internet and has a public IP address.

In the present invention, a virtual community network (VCN) X.VCN is formed. Machines A, B and X can join the VCN, leave the VCN, or allow other
15 machines in the VCN to communicate with them. More than simply a virtual private network (VPN), all members of the VCN are accessible as if they were part of a physical local network. The application running on the members of the VCN can accomplish what they would be able to accomplish if they were on the same physical routed network (e.g. all in the same private network).
20 Membership in the VCN is controlled by an administrator via an administrative interface. In general, the administrator defines certain aspects of the VCN and then invites members into the VCN by specifying the domain name for each member. Members then register themselves with a VCN Manager, and notify the Manager via join and leave requests when they are available to participate in
25 the community. Once registered and joined, members can communicate with other members as though connected via a local LAN.

As shown in Fig.4, A, B and X may all make direct connections to each other through communications within the virtual domain. In Fig. 4, dashed lines represent direct communication paths seen to applications running on A, B and X, all "seeing" the virtual addresses of each other and communicating with each other using the application's IP interface.

A hardware architecture for the machines, server or other devices used to implement the present invention should be well understood to one of average skill in the art. Suitable hardware includes one or more processors, a memory, a mass storage device, a portable storage device, a first network interface, a second network interface and I/O devices, in communication with each other. The choice of processor is not critical as long as a suitable processor with sufficient speed is chosen. The memory can be any conventional computer memory. The mass storage device can include a hard drive, CD-ROM or any other mass storage device. The portable storage can include a floppy disk drive or other portable storage device. If the computer is acting as a router, it includes two or more network interfaces. In other embodiments, the computer may include only one network interface. The network interface can include a network card for connecting to an Ethernet or other type of LAN. In addition, one or more of the network interfaces can include or be connected to a firewall. For a gateway, one of the network interfaces will typically be connected to the Internet and the other network interface will typically be connected to a LAN. However, a gateway can exist physically inside a network. I/O devices can include one or more of the following: keyboard, mouse, monitor, display, printer etc. Software used to perform the methods of the present invention are likely to be stored in mass storage (or any form of non-volatile memory), a portable storage media (e.g. floppy disk or tape) and/or, at some point, in memory. The above described hardware architecture is just one suitable example depicted in a

generalized and simplified form. The present invention could include dedicated hardware, a dedicated router with software to implement the invention or other software and/or hardware architectures that are suitable.

A more detailed overview of one embodiment of the present invention is depicted in Figs. 5A and 5B. Fig. 5A illustrates various embodiments of devices coupled to public and private networks in a manner which allows use of the present invention, and is a representation of a physical connection of such devices. Fig. 5B illustrates a logical representation of elements used to create a VCN and of the various formats of communication traffic between those elements shown in Fig. 5A.

Specifically, Figs. 5A and 5B illustrate various user machines M_n coupled to the Internet 506, as well as other devices, described below, which implement a virtual community in accordance with the present invention. Devices M_n can be personal computers, servers or other computing devices (mobile or non-mobile). Each machine may have different communication connectivity with the Internet.

In general, an exemplary system for implementing a VCN in accordance with the invention comprises a VCN Manager 510, a Network Route Director 520 and/or Private Route Director 530, and a number of Member Agents 565. Communication between systems in various protocols is illustrated by dashed lines (UDP) and solid lines (TCP). The VCN manager and Network Route Director are shown in Fig. 5A as being coupled directly to Internet 506.

User devices M_A and M_E are connected to the Internet and have public IP addresses. These addresses may be dynamic or static. If static, M_A and M_E can easily communicate with each other in a manner well known in the art by simply addressing IP packets directly to each other. If the addresses are dynamic, then M_A and M_E require some means of knowing when the IP address

of the other changes in order to communicate. As described below, the VCN system provides such a means.

Device M_B is in a private domain (e.g. private network)) 540 and connected to a NAT Device 530 to access the Internet 506 by a private network path 540a. Device M_B may use have a dynamic or static IP address specific to the private domain 540. Generally, such addresses are part of the private received IP classes which are not routable via the Internet. For example, 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255 are network addresses classified for private networks. Firewall/NAT device 515 translates Machine M_B 's private IP address to a routable public IP address. NAT device 515 may include other security functions as well. M_B communicates with other non-VCN devices on the Internet via the NAT device 515, and with other members of the VCN via Private Route Director (PRD) 530, which is coupled to the private network path 540a and is a member of the private network 540. Device M_X is also shown as connected to and a member of the private domain 540 but has a static, routable public IP addresses. As such it may communicate with devices coupled to Internet 506 in a different manner, as illustrated in Fig. 5B.

Devices M_C and M_D are part of a second private domain (e.g. private network) 550 coupled to a second private network path 550a. Again, these machines have static or dynamic private IP addresses and are coupled to the Internet via a firewall/NAT device 517, which is itself coupled to network path 550a.

The VCN Manager 510 is a central server or server cluster providing management services, connection services and security services for the VCN. Each Member Agent 565 includes client agent software (or, in some embodiments, hardware) that runs on end machines and provides virtual

network services. It enables the machine to be reached from public and private networks, and implements the security aspects of the system. In Fig. 5B, machines M_A , M_B , M_C , M_D , M_E and M_X all include Member Agents and, therefore, can be members of a particular VCN.

5 The Network Route Director (NRD) 520 is a stand-alone unit that runs on the public side of the Internet enabling Member Agents and Group Agents (discussed below) to be reached inside one or more private networks from the public network. Private Route Director ("PRD") 530 is an element that runs inside a private network enabling access to machines inside the private network
10 from machines outside the private network. It can run as a service on a platform offering other services such as a Windows Server.

Generally, VCNs are defined and managed by the VCN Manager 510. Clients utilize Member Agents or Group Agents to access other client machines (M_n), in private or public realms. The NRD or PRD routes communications to
15 Member Agents.

As described herein, three forms of communication are used in creating and implementing the VCN. TCP is used in the registration and joining processes; encapsulated UCP packets are used between elements in establishing communication between joined devices and for management traffic,
20 and Encrypted UCP packets are used for agent-to-agent communications.

Fig. 5B shows exemplary traffic between elements of the VCN. A first type of traffic is TCP traffic. TCP traffic is used between member agents to establish membership in the VCN (the registration process), and make the VCN manager aware they are available to communicate with other members of the
25 VCN (the join process). In Fig. 5B, this is represented by solid lines 513b, 511b, 523b and 543b. TCP is also used: by the PRD 530 to establish communications with the VCN (lines 527b, 527d); and by the member agent of device M_B to

communicate with the PRD 530 (line 533b). TCP may also be used by devices M_C and M_D on private network 550 to communicate with each other.

Encapsulated UDP traffic is used by elements of the VCN once membership has been established and the elements are joined in the VCN for management and administrative communications. This is represented in Figure 5B by lines 511a, 513a, 523a, 527a, 527c, 523c, 527e, 521, 543a, 541, and 519. Encrypted UDP communications are used between devices, shown in Fig. 5B between device M_X and M_A at 525 and device M_B and M_C at 537.

In one embodiment, secure connections are built dynamically using IPsec tunnels based on a virtual IP space that can traverse from private networks, across the Internet and into other private networks. Strong authentication and the establishment of IPsec policies at the time members join the community offers privacy and security to the members of the virtual community. This facilitates the introduction of a variety of policy-based network services with centralized management such as Virtual Private Networks for intranets and extranets, IP-telephony domains, and IP-based PDA communities.

COMMUNICATION PROTOCOL

In the present invention, an encapsulation routing protocol allows packets to traverse addressing boundaries and identifies routing endpoints by unique DNS domain names. It employs an address virtualization scheme that accomplishes backwards compatibility with IPv4 applications. With certain optional exceptions, UDP encapsulation is used between elements of the Virtual Community.

One example of an encapsulated packet 600 is depicted in Fig. 6A. It includes a 20 octet IP header 602, an 8 octet UDP header 604, a 20 octet

system shim 606, and a variable size virtual IP packet 608. A virtual IP packet has the same format as a standard IP packet.

Members of a VCN communicate to other members of that VCN by means of virtual IP Packets 608. Virtual IP addressing is used to establish
5 unique connection identities for community connected devices. IPsec can (optionally) be applied to the Virtual IP Packet for end-to-end security. Virtual IP addresses are used to identify members in the community in the virtual packet and are not directly routable. Rather, they are unique identifiers of a given connection to the upper layer application. In one embodiment, virtual IP
10 addresses are in IPV4 format.

In general, the UDP header is set for a default port. System shim 606 carries enough addressing information to allow the Route Directors to forward the tunneled packet through the various address realms on its way to the destination. Such a routing methodology is often referred to as source routing.

15 In order to route packets to a peer in a different addressing realm, the protocol stack knows the address of the appropriate Route Director that serves the peer's realm, the private address of the peer or a NAT address. The Member Agent obtains the information by using the VCN Manager as a DNS authority for DNS lookup operations as described below (Figs. 13 and 21). The
20 DNS response from the VCN Manager will include the above-identified information in an optional text field of the response to the Member Agent.

TCP/IP connections require IP addresses to be used as connection identifiers at the user level. If an application wishes to make a connection to "m3.abcdef.com" and another to "m4.abcdef.com", it resolves both DNS
25 identifiers into IPv4 addresses. The system cannot assign the private IP addresses of the members to be unique connection identifiers, because two

members might have the same private address in different private address realms.

Assigning a virtual address to each peer designated by a DNS string solves the problem of ambiguous endpoints. These virtual addresses may be any legal IPv4 addresses, but conflicts will occur if the same addresses are used to directly designate a peer in an IPv4 network application. For instance, if 10.0.0.10 is used as a virtual address, and is also used on a member's network as the mail server, packets that are ordinarily destined to the mail server may be redirected to a random peer. In general, when choosing virtual addresses it is best to choose addresses that will not be routable to the member. Hence, each member is assigned a virtual IP address unique in the context of the virtual community and that will not conflict with any local addresses on its LAN or any public IP addresses on the Internet.

By having each member of a VCN use a virtual address, a virtual address realm is created. The virtual address realm is the set of addresses that can be used to identify and send communications to other members of the VCN. The virtual address realm is different from a physical address realm because the physical address realm is actually used to route on a physical network. The members of a VCN will all be in the virtual address realm of that VCN, but may be in different physical address realms. For example, looking at Figs. 5A and 5B, M_B and M_C are in different physical address realms (e.g. 540 and 550); however, they are both in the virtual address realm of the VCN. Another example can be seen with Fig. 4, where A and B are in different physical address realms (Cob.com and Coa.com); however, they are both in the same virtual address realm. Applications on members of a VCN will see the VCN as the local subnet; therefore, the VCN can be thought of as a virtual subnet. Each

-25-

member of the VCN will appear to the application as an entity connected to the local subnet.

Route Directors 530 and 520 facilitate routing UDP encapsulated traffic to private address domains 540, 550. In general, Route Directors either have public IP addresses or addresses that are statically remapped to a public IP address. The static translation of a Route Director's IP must leave the port in the UDP header unchanged to allow the UDP encapsulated destination port number to be directly used by public members, by other Route Directors, and by private members. Route Directors 520, 530 and VCN Manager 510 may be configured to use a non-default UDP encapsulation port. In one embodiment, all outgoing messages are sent to this port on the next destination node and all incoming messages are read from this port. As discussed below, information in a "join" packet tells Member Agents the UDP encapsulation port to use in communications to Route Directors, network managers, and other members of the community.

System Shim 606 (see Fig. 6A) has a format given by way of example in Fig. 6B. Protocol Version information, data type, header option flags, and Router Information are potentially stored in the Shim. (The abbreviation "gIP" stands for "global" or public IP address, indicating an Internet routable IP address). The Data Type field indicates the meaning of the optional data that may follow the Shim. This may include a Virtual IP Packet 608, a ping to a Route Director, a request for a Network Route Director virtual address, a Route Director response with a virtual address, a member leaving and releasing a virtual address, and a member-to-Route Director packet. The shim also includes the public IP address for the source machine's Route Director, the public IP address for the destination machine's Route Director, the private IP address for the source machine and the private IP address for the destination

machine. In the case where the source or destination use a public IP address, then the shim will not need to include the private addresses of the source/destination or a route director.

5 The system can optionally use TCP encapsulation between a member and a Route Director. If the VCN Manager determines that a Member Agent (e.g., Agent software on a member machine) and a Route Director are both able to support a TCP connection, then it may instruct the member to initiate a TCP connection with the Route Director. TCP port 80 may be used as the destination port for all TCP encapsulated messages to the Route Director, and TCP port
10 20202 may be used as the source port for all TCP encapsulated messages from a private member to the Route Director.

As noted above, Network Route Directors (NRDs) 520 facilitate routing traffic into and out of private address domains without requiring reconfiguration of a firewall 517 protecting the domain 550. As in UDP encapsulation, a special
15 field in the system join packet (explained below) tells the Member Agent which TCP encapsulation port to use as the source port. The NRD will then re-encapsulate virtual-traffic in UDP-encapsulation before passing it on to other elements of the virtual network.

Note that more than one user can use the same device, with each such
20 user having different virtual addresses in the same or different address realms.. Additionally, regardless of the number of users, one device can be in multiple virtual address realms. In some embodiments, a user can have multiple identities, each in a different address realm.

Fig. 7 is a flow chart describing the overall process for communicating
25 between members of a VCN. Any member of a VCN can communicate with any other member of a VCN regardless of whether either of the members are behind a firewall, behind a NAT device, directly accessible via the public Internet, in a

-27-

private network, etc. From the point of view of an application on a member device, all the other members appear to be on the same LAN. Thus all applications running on a member's device will think that all other members of the VCN are on the same LAN and in the same address realm (e.g. the virtual
5 address realm of the VCN).

In step 650 of Fig. 7, the Agent for the potential member joins the VCN and receives a virtual IP address. In order to establish or participate in communication within the VCN, a device must register with and join the VCN, thereby becoming a member of the VCN. The Agent will send a message to
10 VCN Manager 510 and receive a virtual IP address back. The virtual IP address received is used to identify the member in the VCN. More details of step 650 as well as other portions of Fig. 7 will be discussed below. Note that there is a dotted line between step 650 and step 652. This dotted line signifies that a lot of time can pass between step 650 and step 652. Additionally, after step 650 is
15 performed, it does not need to be repeated.

In step 652 of Fig. 7, an application on the source machine (the member initiating communication) intends to send a message to an application on the destination machine (another member of the VCN). Examples of applications that can communicate on the VCN include instant messaging, email, FTP,
20 browsers, data transfer programs, and other applications that can communicate. Consider an example when application on device M_A intends to initiate communication with an application on device M_B . Thus, M_A is the source device and M_B is the destination device. In step 654, the application on M_A will initiate a DNS request using the domain name for M_B . This DNS request is sent to VCN
25 Manager 510. In step 656, VCN Manager 510 returns the public address of the Route Director for the destination, the private address for the destination device and a virtual IP address for the destination device. In the example described

-28-

above, step 656 includes returning the public IP address for private Route Director 530, the private address for M_B and a virtual IP address for M_B . If the destination machine has a public IP address (and, thus, does not use a routing director) then step 656 will only include returning the public IP address for the destination. If the destination machine is in a private network that uses a Network Route Director (e.g., NRD 520), then step 656 will return the public IP address for the Network Route Director.

In step 658, the Agent for the source device, which received the information in step 656, will store that received information. This information can be stored in a table, or any other data structure. In step 660, the Agent for the source device will return the virtual IP address of the destination device to the application on the source device. In step 662, the application on the source device will initiate the sending of a message/data using the virtual IP address for the destination device. In step 664, a virtual IP packet will be created. The source IP address for the virtual IP packet will be the virtual IP address for the source device. The destination IP address for the virtual packet will be the virtual IP address for the destination device. The virtual IP packet will be in the same format as a standard IP packet. In step 664, the newly created virtual IP packet will be subjected to IPsec (or another security means). In some embodiments, IPsec is not used. In step 670, the virtual IP packet is encapsulated. For example, in one embodiment, the virtual IP packet is encapsulated as described above with respect to Figs. 6A and 6B. This encapsulation will include shim 630. As described above, shim 630 will include the public IP addresses for the Route Directors for the source and destination, and the private IP addresses for the source and destination devices. If either the source or destination do not have a Route Director, the shim will not need to include that information. For example, when the source machine is M_A , there is

no Route Director for the source. If the source machine was M_C , then the shim would include the public IP address for Network Route Director 520. If the source is M_B , the shim would include the public IP address for Private Route Director 530.

5 At this point, the path of the packet will depend on whether the destination is using a Private Route Director 530, Network Route Director 520 or has a public IP address. If the destination has a public IP address, the process moves to step 678 where the encapsulated packet is forwarded to the destination agent.

10 If the destination is in a private network that has a PRD, then in step 672 the encapsulated packet is sent to the NAT device for the destination. For example, the encapsulated packet is sent from M_A to NAT 515. In step 674, the encapsulated packet is sent from the NAT device for the LAN that includes the destination to the Route Director for the destination. For example, the
15 encapsulated packet is sent from NAT 515 to private Route Director 530. In step 676, the Route Director which received the encapsulated packet will remove the virtual IP packet and the shim from the encapsulation. The Route Director will read the shim to learn the local IP address to send the packet to. The shim and virtual IP address will then be re-encapsulated into a new packet
20 with the original virtual packet. The new outer packet includes a destination IP address equal to the private IP address of the destination device. The encapsulated packet received in step 674 will include a source IP address equal to the public IP address for M_A (or the source's Route Director) and a destination IP address equal to the public IP address for the Route Director of the
25 destination (e.g., PRD 530). In step 678, the new encapsulated packet will be sent from the Route Director to the Agent for the destination device.

-30-

If the destination agent is in a private network and is using a Network Route Director, then following encapsulation the encapsulated packet is sent to the Network Route Director for the destination agent in step 673. At step 675, the NRD will remove the virtual IP Packet and shim and re-encapsulate them in a UDP packet for transmission through a NAT device to the destination via a persistent UDP connection between the NRD and the destination. At step 677, the encapsulated packet is forwarded to the NAT device (via the persistent UDP connection) behind which the destination Agent resides, which will perform its own routing of the encapsulated packet to the destination Agent in step 678.

10 In step 680, the Agent will remove the shim and the virtual IP packet from the encapsulation. The virtual IP packet will be removed from IPsec (e.g. decrypted). In step 682, the information from the shim will be stored by the Agent. In step 684, the contents of the virtual packet will be presented to the application on the destination device. That is, the application on the destination
15 device will receive the contents of the data payload, or at least a portion of the data payload

When the destination wishes to respond to the source or the source wishes to send additional information, the process of Fig. 7 can be repeated. However, when repeating the process of Fig. 7 between two machines where
20 communication is already established, the steps of performing the DNS request do not need to be performed again. That is, when the destination wishes to respond, the destination will perform the steps in Fig. 7 starting at step 662. The Agent for the destination device will already know all the information to put in the shim. Additionally, when the source device wishes to send additional
25 information to the destination device, the source device can start Fig. 7 at step 662. In some embodiments, however, the steps of performing the DNS request will be performed again.

MEMBER AGENT

As noted above, devices in the VCN utilize a member agent installed on the device to communicate. One unique aspect of the system of the present invention is the integration of the agent software in a typical device.

5 Fig. 8 illustrates the functional flow diagram of an installed agent on a device such as a computer, server or other device. Region 810 illustrates the "user space," and region 820 represents the kernel area of the components interacting with the host device.

 Applications 830 interact directly with an IP stack 835 which is built on a
10 deterministic network extender or DNE 850. The deterministic network extender is provided by Deterministic Networks, Inc. The network extender allows one to implement any driver level functions such as IPsec, browsers, traffic redirectors, and the like, through a series of plug-ins. As shown in Fig. 8, a number of plug-ins, including a DNS plug-in 852, an IPsec plug-in 854, a virtual adapter
15 manager 856 and a domain name router 858 (see U.S. Patent 6,119,171, incorporated herein by reference) interact with the deterministic network extender 850. The DNS plug-in processes DNS queries by applications via the stack. The virtual adapter manager allows for additional adapters to co-exist in the same device.

20 The DNE is an NDIS compliant module (in Windows environments) which appears as a network device spire to the protocol stack 835. The DNE supports the TCP/IP and UDP protocols and various adaptor types. In essence, this forms a virtual network adaptor in device installations. This means that various configurations for each virtual community can be provided for each DNE. This
25 provides the advantage that a number of members or users can utilize the same device, with the device installing a different virtual adaptor using plug-ins for the deterministic network enhancer and each user does not need to reconfigure the

network settings of the machine to join each community. Each plug-in is constructed in accordance with standards promulgated by the DNE provider.

As shown in Fig. 8, user applications interact directly with the IP stack of the virtual adapter. Each adapter provides its own stack to the device's applications. To the applications, each stack appears separate, and no separate routing of the application is required. For example, the IKE user application 825 can interact with the domain name plug-in, the IPsec plug-in, the virtual area management communicator 856, and the security policy manager 860. The Adapter Manager 856 allows parallel stacks for each VCN to be implemented and used on each machine. This means a user and device can belong to several VCNs without needing to re-configure IP settings to access each VCN.

VCN DEFINITION

Fig. 9 shows the steps which occur at the VCN Manager to define and establish a virtual community. At step 902, an administrator sets up a virtual community by providing information to the VCN Manager via a user interface (not shown). It will be understood that the user interface and the method of providing information to the VCN Manager is not critical to the system of the present invention. One particularly advantageous interface is implemented in a World Wide Web browser. The interface may be implemented using HTML, XML, Java Applets, Java Server, Active Server Pager or any of a number of well-known Web technologies. The particular information required to set up the community network is illustrated in Fig. 10. Next, at step 904, users who are designated by the administrator as being allowed access to the virtual community defined in step 902 are notified by any number of appropriate means. In one implementation, the users are notified by e-mail, although other

forms of notification, such as verbal or personal notification, may be used. The e-mail may contain an invitation to join the community, community authentication information, a link to a location to download the Member Agent, and/or a link to the Group Agent. Next, at step 906, using information contained in the e-mail, users register with the VCN Manager. Registration in this context means registering a machine using a Member Agent or a Group Agent with the VCN Manager. Users may be required to install the Member Agent software. The link in the notification e-mail may provide the user with a location for downloading the Member Agent software as well as instructions for installing the software. Other information, such as system password information, is provided in the e-mail. Finally, at step 908, management of the community is handled by the VCN Manager. This includes monitoring which registered users have joined and left the system, answering DNS requests, and applying security policies, as described herein. This may include notifying new users and registering those users as the definition of the VCN changes.

Fig. 10 is a flowchart illustrating the process of setting up a virtual community which is performed by an Administrator. Initially, the Administrator sets up a virtual domain name and address domain at step 1002. This information is used by the VCN Manager and Route Directors to allow members to communicate. Next, users are defined at step 1004. In one embodiment, the users are defined by providing the domain names of each of the users who will be invited to participate in the VCN. At step 1006, default passwords are set. This is the password a user first uses to access the system. The user may be forced to change the password for security reasons at a later date. Finally, at step 1008, policies may be defined at the domain level, the user level, or for individual machines in the domain. Policies are used to allow or deny access to individual machines, services, or other users.

MEMBER REGISTRATION

The registration process is the first step that a user and machine go through with the VCN Manager before becoming a member of a virtual community. There are two phases to member registration: a registration request
5 and a registration file request. Registration happens outside of the IPsec tunnels because at registration time no IPsec tunnel exists for the user registering.

In one implementation, all traffic between Member Agents and the VCN Manager (with the exception of Registration and Join function traffic is
10 encapsulated using UDP encapsulation, represented by lines 511a, 513a, 523a, 519, 521, 527a, 527c, 537, 523c, 527e, 541, 543a, 533a of Fig. 5B). This encapsulated traffic will carry management traffic between the members and the VCN Manager. A service port is reserved at the VCN Manager in the virtual network for the establishment of a TCP connection between a member and the
15 VCN Manager. A member that joins a VCN is informed of the service port as part of the join protocol. A DNS port is also open on the virtual side of the VCN Manager. In one embodiment, the VCN Manager virtual ports are TCP Port 9001 and DNS UDP Port 53. The packets used for the initial Registration and the subsequent Join operations use TCP port 80 outside the virtual network.
20 This is represented in Fig. 5 by the solid lines 513b, 511b, 523b and 543b.

VCN system protocol packets that are sent outside the system tunneling are HTTP wrapped and sent to the VCN Manager on TCP port 80 to facilitate NAT traversal. More information about NAT traversal will be provided below. Each packet includes a header and payload. For compatibility with firewalls, the
25 HTTP wrapper makes the packet a SOAP-compatible XML document. Including a binary data portion after XML is consistent with Direct Internet Message Encapsulation (DIME), a proposed lightweight, binary message format that can

be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct.

The format of the HTTP wrapper from the Member Agent to the VCN Manager is shown in Fig. 11. The wrapper includes an HTTP HEADER, XML
5 HEADER and P-LENGTH fields. The HTTP header includes a POST HTTP field, an Identity field, a Content Type field, and a Content Length field. The XML header includes version information and packet type information. The Header includes error codes and explanations, as well as the content type and length.

10 The Registration exchange between the member agent and the VCN Manager is shown in Fig. 12A. When a Member Agent 565 attempts to register at step 1200, Member Agent 565 will send a registration request packet 1202 to the VCN Manager 510 to start registration. The packet is included in an HTTP wrapper as illustrated at 1204. The registration packet will carry the client Fully
15 Qualified Domain Name (FQDN) and a Diffie-Hellman Key Exchange request to the VCN Manager. The packet further includes packet version information, type and length information, a user authenticator, the length of FQDN in octets, a VCN name offset, the member's FQDN in DNS format, the length of Diffie-Hellman value in octets, and the member's initial Diffie-Hellman value.

20 An Initial Password is passed to the user through an outside channel, such as e-mail (or other channel). In a setting where security is a concern, an alternative method such as personal communication or encrypted e-mail may be used.

The registration authenticator is computed using the first sixteen bytes of
25 the HMAC-SHA-1 applied to the packet data with the password hash as the key. (Normally, the HMAC-SHA-1 algorithm generates a 20-byte result; in one

embodiment of the system only the first (leftmost) 16 octets are used in the MAC.) The formulas are as follows:

$$\text{HMAC-Key-Field} = \text{SHA-1}(\text{Initial Password})$$

$$5 \quad \text{Authenticator} = \text{HMAC-SHA-1}_{16}(\text{HMAC-Key-Field}, \text{Data})$$

The VCN Manager will respond in one of three ways 1206, 1208, 1212, to the registration packet 1202. VCN Manager 510 will acknowledge (ACK) the packet at step 1212 with the Registration Acknowledge (ACK) packet 1214 if the member belongs to a community but its status is "not registered." The VCN Manager also sends a phase-2 confirmation code to the member's e-mail address and changes the member status to "registering." The packet will transfer a "Time To Live" value to the member which is a timeout period in seconds for hearing back from the member with the confirmation code. Phase two of registration must be completed in this time period.

If the packet is abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, the member does not exist in the database, or the VCN server is not running, the VCN Manager drops the packet in step 1206. The packet will be not-acknowledged (NACK) 1210 if the member is already in the "registered" state, the send e-mail operation fails, the process of updating the member to the "registering" state fails, or the random generator fails in attempting to generate a confirmation code in step 208.

Upon receiving the Registration ACK 1214, the user will send Registration File Request Packet 1220 to the VCN Manager 510 to start registration. This packet will transfer the following information to the VCN Manager: a registration file User Authenticator, the length of FQDN in octets, a VCN name Offset, and the member's FQDN in DNS format.

-37-

The registration file user Authenticator contained in the File Request packet 1220 is slightly different from the Registration Request Authenticator in packet 1202, in that the Initial Password, passed to the user through an outside channel (e-mail for example), and the Confirmation Code, a temporary code sent in the second e-mail with a timeout to the user, are used:

$$\text{HMAC-Key-Field} = \text{SHA-1}(\text{Initial Password})$$
$$\text{User Authenticator} = \text{HMAC-SHA-116}(\text{HMAC-Key-Field}, \text{SHA-1}(\text{Confirmation Code}) + \text{Data})$$

10

The VCN Manager will send a Registration File acknowledge Packet 1230 to the member 565 in response to the Registration File Request packet 1220 in step 1228 if it is determined that the member belongs to a community. The Acknowledge Packet 1230 will transfer the following information to the member:

15

- *Crypto Type* — a code indicating how the rest of the packet is encrypted. This is provided in a crypto type field preceding the registration file.
- *Registration File* — a structure with a number of fields containing the information required by the member to successfully perform a join. It is sent encrypted using the key generated via the Diffie-Hellman key exchange.

20

A table representing the Registration File structure is shown in Fig. 12B. As shown therein, the Registration File contains an Authentication Type, a File Type, a File Length definition, a Token Key, a Key Timestamp, a Key Type, a Key Length, a High Availability (HA) Version, a HA Number, Server Information and Padding. The Token key is the shared secret with the server. The Token

25

Key is identified by the Key Type, which is normally a Diffie-Hellman type in one embodiment. The VCN Manager also changes the member status to "registered."

If at step 1224, the member agent status is not set at "registering," or the
5 timeout for phase 2 has expired, a NACK packet 1226 is sent. If the packet is
abnormal (in size, FQDN length, bad type, etc.), the authenticator check fails, or
the user does not exist in the database, or the VCN server is not running, the
packet is dropped in step 1222. While current encrypting method for the file is to
generate a key/IV pair from the combined Diffie-Hellman value using a Key
10 Derivation Function, any number of suitable substitutes may be used.

In addition to the registration authentication described above, the system
uses a packet authenticator to verify communications between the VCN
Manager and Agents. The Authenticator is a cryptographically strong hash of
the packet keyed by a shared secret between the source and destination. The
15 authenticator is calculated over the entire packet using the HMAC-SHA-1
algorithm. The inputs to this Authenticator are not available until after
Registration. As illustrated above, during registration an Authenticator based on
the user password is used. The fields used in the calculation are a *Diffie-
Hellman Key* comprising a multi-octet random string that is the result of the
20 Diffie-Hellman key exchange protocol, and the entire packet data, with the
Authentication field zeroed out.

The Authorization Key, AuthKey, described above, is derived from Diffie-
Hellman using the KDF2 function, and used for general packet Authentication.
AuthKey = KDF2 (Diffie-Hellman Key)MAC = HMAC-SHA-116(AuthKey, Data).
25 The *AuthKey* need be calculated only once per registration from the KDF2 of the
DH key and then stored for later use. It is known as the Authentication key and
is 20 octets long.

MEMBER JOIN/LEAVE

Once a user is registered, the user can join the VCN. Once joined, the user is a member of the VCN. Joining allows the user to let the VCN Manager and other members know that the user/member is on-line and available to communicate. The Join protocol runs between a Member Agent and the VCN Manager to establish a session key with the Manager, authenticate to the Manager, and make use of connections via the Route Directors in the community.

The Member Join process is illustrated in Fig 13. There are two phases to the Join operation: phase one is an Initialize Request and phase two is the actual Join. At join time, the IPSec tunnel for secure communication is not established, so the first few join packets are sent outside the IPSec tunnel.

Initially, at 1302, the Member Agent 565 will send an Init Request Packet 1304 to the VCN Manager 510 to start authentication. The packet will carry the following information to the VCN Manager:

- *Version Variant Mask* – used to indicate optional variations of the protocol from the member to the VCN;
- *Token Timestamp* – identifying when a Token Key was created (in seconds);
- *Member seed* – a random number to thwart so called “man-in-the-middle” attacks;
- *Member Local IP* – the member’s Local LAN IP address; and
- *Client FQDN* – the client’s fully qualified domain name.

Again, three responses 1306, 1308, 1312 are possible. At step 1306, if the packet is abnormal, it will be dropped. Similarly, if the member fails authentication, at step 1308 a NACK packet 1310 will be sent.

-40-

If the member passes authentication at 1312, the Manager will send an acknowledgement packet 1314 to Member 565. An AuthKey is also transmitted as part of the INIT Request Packet, and the Manager authenticates the packet by checking this against a secure key digest. The acknowledgement packet

5 1314 packet will transfer the following information to the member:

- *Version Variant Mask* – version information;
- *Member Seed* – from the Init Request to protect against playback attacks;
- 10 • *Manager Seed* – a unique seed used to thwart man in the middle attacks;
- *Session AH Key* – used in IPsec;
- *Session ESP Key* – used in IPsec;
- *Init ACK Time* – a time stamp used to tie this packet to the following Join Request. There is a timeout if the Join is delayed too long;
- 15 • *Authentication Method* – the method used for authentication;
- *Route Director Private IP* – if member is in a private network, this is the private IP address of the Private Route Director. The value is zero if no Route Director is used;
- *Route Public Public IP* – if member is in a private network, this is the
- 20 public IP address of the Private Route Director. The value is zero if no Route Director is used;
- *Tunneling Port* – used for UDP encapsulation *Route Director Flags*. Only Bits 0 and 1 currently used to direct the agent to a Private Route Director, Network Route Director with UDP, or a Network Route Director with TCP.

25

At step 1312 of the join process, the VCN Manager will also determine whether the Member Agent attempting to join is behind a NAT device. The

method by which this occurs is discussed below with respect to Fig. 21 and the results of this determination may force the Agent to negotiate a session with a Network Route Director which will provide a pseudo address value used as the Agent's local IP value in the Join request, discussed below. This process is
5 discussed in depth with respect to Fig. 21.

Following receipt of the acknowledgement packet, at step 1316, the member will send Join Request Packet 1318. The packet's payload includes a manager seed, the initial ACK time, join flags, the member machine's local IP address (or pseudo address), the Route Director's private IP address, the Route
10 Director's public IP, the member AH SPI and ESP SPI, the member listen port, a token timestamp, a GUID identifying the current client run, NetBIOS name support, a password hash, version information for high availability and security policy information.

In step 1320, the VCN Manager will drop this packet if it is abnormal. In
15 step 1322, the VCN Manager will send a NACK packet 1324 if the member is not in the registered state, the timeout for Join from INIT ACK has expired, or updating the member to the Joined state fails.

If the join action succeeds, then in step 1326 the VCN Manager will send an acknowledge packet 1328. The acknowledge packet payload includes the
20 RMI Port at the VCN Manager, the Tunneling Port, VCN Manager Authentication Header (AH), Security Parameters Index (SPI) for IPsec, VCN Manager Encapsulating Security Payload (ESP) SPI for IPsec, the UTC Time (in seconds) when the member joined, VCN Manager Heartbeat interval (in seconds), the Member Heartbeat interval (in seconds), the VCN Manager's Virtual IP address,
25 the Manager Subnet Prefix Length, the VCN Member Subnet Prefix Length, the Route Director's private IP address, the Route Director's public IP address, an indication of the updates that follow, an update of the Token Key, an update of

-42-

the Security Policies, an update of High Availability indication, and padding. The member has now joined the community at 1330. Once the member has joined, all communications can be encrypted using IPsec.

The system of the present invention also includes RADIUS authentication support. Generally, if a member attempts to authenticate using a RADIUS server, the VCN Manager will perform the same steps as when it receives the Join Request packet except for having a RADIUS server authenticate the member. The payload for this packet is similar to the Join Request packet except that it has an additional field for RADIUS password that is used by the RADIUS server to authenticate the member.

Fig. 14 shows the sequence for leaving a VCN. Initially, at step 1410 when a Member Agent is prepared to leave the community, a Leave Request Packet 1412 will be sent to the VCN Manager 510 to start the leave process. The Leave Request Packet will carry a Leave Flag, the FQDN Length, FQDN VCN Offset and Member FQDN. Unless dropped at step 1414 or a problem exists at 1416 which would generate a NACK packet 1418, the VCN Manager will send the Leave ACK Packet 1430 to the member in step 1420. This packet has no payload. At step 1440, the member has successfully left the community.

20 DNS/ LOOKUPS

For one member to communicate with another member, the initiating member's agent will perform a query or DNS lookup (step 654 in Fig. 7) to determine the address of the other member, and then establish a secure communication channel between them.

25 The Member Agent utilizes the VCN Manager to perform lookups of other virtual members in the virtual community using DNS. The DNS operation is conducted using the DNS protocol with the VCN Manager. The member

software sends a DNS query to the VCN Manager, and the manager returns information about the target member. Besides the target member's virtual IP address, the DNS response also contains additional information about the target member. While the VCN Manager accepts all DNS requests, it will only
5 acknowledge the DNS requests of type A, which are targeted to virtual domain names in the secure virtual communities of the VCN Manager. The VCN Manager is the authoritative name server for those virtual domain names; other requests will simply be responded to with a "Server Failure."

The DNS query and response sequence is illustrated in Fig. 15. At step
10 1510, a member will request a DNS lookup by sending a DNS request 1520 to port 53 of the VCN Manager. The DNS request 1520 will result in a normal DNS response 1575 unless any of a number of failure conditions are met, shown at steps 1522, 1540, 1550, and 1560.

If the Manager receives a query on port 53 that is not a DNS query, then
15 at step 1522, it is dropped. If, at step 1524, the query is not a standard query, such as a DNS STATUS (a status lookup) or IQUERY (inverse DNS), or the class of the DNS query indicates an Internet (IN) query, or if the TYPE value of the request is a pointer (PTR) or host address (A), then, a "Not implemented" DNS response 1530 is sent over the virtual link to the Member Agent 565.

20 At step 1540, the VCN checks to see if the source IP address is for a member of the VCN. If the source IP address is not for a member of the VCN, the virtual IP look up fails or the type PTR query does not match, a "server failed" response 1545 is returned. At step 1550, if there is no DNS Question section or there is another type of format error with the packet, a "format error"
25 response 1555 is sent. The VCN determines whether the member has joined the VCN, at step 1560. If not, a name error response is sent at 1565.

If the name is a successful lookup (step 1570), then the VCN Manager will send a DNS Response Packet 1575 to the member 565. The response includes the following information: the target member FQDN; the target member virtual IP address; a source Route Director flag, the source member virtual IP address; the target member join time; the target member agent version; the target member private IP address; the target Route Director public IP address; the target member NetBIOS name; the shared key, shared by the two members; a target Ticket length; a target member Ticket encrypted for target member only and containing a Ticket issue time, Ticket expiration time, and shared key; the target member virtual IP address, the source member virtual IP address, the source member private IP address; the source Route Director public IP address, the source member FQDN; and padding (to obtain a multiple of 16 octets). The Ticket provided by the DNS request is detailed further in the description of Figure 16B.

The target member's virtual IP address will be presented using an A-type resource record in the answer section of the normal DNS response packet. All the remaining information will be transferred using a TXT-type resource record in an additional section of the DNS Response.

20 ENCAPSULATION

Traffic between Member Agents in the VCN is encapsulated using UDP encapsulation. Encapsulated traffic between members can carry any IP traffic from any standard IPv4 compliant application. However, one port is set aside in the virtual network at the application layer to establish a connection between two members in the community. In one embodiment, this is UDP port 500, which is set aside for Internet Key Exchange (IKE), allowing negotiation of an IPsec tunnel between the two members.

When an application on a member device wishes to open a connection to a peer on a target member device, a protocol is followed for the establishment of the IPsec session between the two. Member Agents are configured to listen on the UDP tunneling port (which defaults to port 20202) for virtual traffic. As an
5 accepted procedure non-IPsec traffic on the virtual IKE port 500 is accepted and passed to an IKE and Security Policy Module to allow for the possibility of initiating an IKE exchange and the establishment of an IPsec session between the two members.

IKE is fully described in RFC-2409. IKE provides a key exchange with a
10 peer and creates a security association (SA) for the IPsec module. IKE access between peers occurs in two phases: phase 1 establishes a secure, authenticated, channel with which to communicate, and phase 2, which negotiates a Security Association on behalf of IPsec. Phase 1 is generally referred to as the ISAKMP Security Association (SA) and includes a "Main
15 Mode" and "Aggressive Mode." In one implementation, Aggressive Mode is used for phase 1. One of the allowed phase 2 exchanges is "Quick Mode" and in one implementation, Quick Mode is used in the system for phase 2.

Fig. 16B shows the aggressive mode IKE phase one exchange utilized in the present invention. Fig. 16A shows the standard aggressive mode IKE phase
20 one exchange for comparison. In these figures, in accordance with standard IKE parlance, one device is considered an exchange "initiator" and the other a "responder".

In general, in phase one of the IKE exchange, peers are authenticated, an IKE Security Association (SA) policy between peers is established, a Diffie-
25 Hellman exchange is performed to produce matching shared secret keys and a secure tunnel to negotiate IKE phase two parameters is established.

In Fig. 16A, an initiator exchanges a header (HDR), SA negotiation payload, Key Exchange (KE), nonce payload (Ni, where "i" indicates an "initiator" payload) and identity of the party (IDii). The key exchange payload contains the public information exchanged in a Diffie-Hellman exchange. The responder
5 returns the HDR, SA, KE, a responder nonce payload (Nr), its identity (IDir) and the HASH responder (HASH_R) payload, which is generally a hash of the ID payload and is used to authenticate the exchange. The initiator returns the HDR and HASH initiator (HASH_I) payload, and the initial secure tunnel is established.

10 In accordance with the present invention, Fig. 16B illustrates the use of an extension to aggressive mode exchange. This is performed by adding a ticket payload (TKT*) to distribute a shared-key to remote peers.

The Ticket is the means by which one Agent can identify whether another Agent is a trusted member of the virtual community. Essentially, the Ticket
15 includes information identifying the initiating member to the receiving member.

The ticket is issued by the VCN Manager and encrypted for the receiving member with a member-server shared secret; only the receiving member can open it. The ticket contains a time-stamp, a sequence number and a shared-secret used for IPSEC between the two members. To communicate with the
20 receiving member, the initiating member obtains the ticket from the VCN Manager (through, for example, the DNS sequence, described above) and passes it to the receiving member in a payload that can ride on an IKE packet. The receiving member receives the Ticket, decrypts the Ticket using the member-server shared secret, and uses the information in the Ticket to establish
25 secure communication with the initiating member.

This payload, TKT, is formatted as shown in Fig. 17. The packet 1700 contains an IP header 1710, UDP header 1720, System shim 1730, and Virtual

IKE Phase 1 UDP/IP packet 1740. Fig. 18 illustrates the structure and data of an exemplary first packet 1740. The IKE Ticket Payload in the first IKE packet contains information on the payload and the payload data, including the type of payload following next and the ticket payload data 1756. The payload data 1750
 5 includes the size, number and item list 1766. The item list 1760 includes type, size and item information. The IKE ticket payload data 1740 contains the item types

The item types 1770 are shown in the last table of Fig. 18: "My FQDN" -- a null terminated FQDN in label dot format. (For example, a human readable
 10 FQDN "bob.system.com" is encoded as "bob.system.com\0x00.") My Ticket data which includes a Manager Current Time (UTC of Manager as known by initiator); and an Initiator Virtual IP (Obtained at Join time) Target Virtual IP (Obtained from Manager) and Padding. The Peer FQDN Format is a null terminated FQDN in label dot format. For example, a human readable FQDN
 15 "bob.system.com" is encoded as "bob.system.com\0x00". Finally, the Peer Ticket data includes: a Ticket Issue Time (UTC (seconds) on VCN Manager); a Ticket Expiration (UTC (seconds) for ticket expiration); a Shared Key used by the two Members for IKE; a Target Virtual IP Address; the Initiator NAT Port; the Initiator Subnet; the Initiator Virtual IP Address; Initiator Private IP Address, the
 20 Initiator Public IP Address, the Initiator FQDN and padding.

The Diffie-Hellman key exchange protocol is utilized in the Internet Key Exchange (IKE) protocol that precedes IPsec. The prime and generator value are taken from a well-known Internet Draft entitled, "More Diffie-Hellman groups for IKE," Kivinen et al., IP Security Protocol Working Group (IPSE) Internal Draft,
 25 Dec. 13, 2001, for proposed use within the Internet Key Exchange (IKE) protocol.

ADMINISTRATIVE FUNCTIONS

The system can simulate pings to any of the Route Directors (NRD or PRD). This ping is sent inside a packet generated from an application used to trouble-shoot the virtual network by touching the Route Directors and insuring
5 that they are alive.

An exemplary ping process is illustrated in Fig. 19. As shown therein a pinging application 1902 at step 1904 sends a ping request packet 1906 to the Route Director 560. The Route Director receives the ping at 1910 and generates a response at step 1912. The ping response packet 1914 is returned
10 to the application 902 at step 1916.

The ping request packet is sent and returned on the default tunneling UDP port (which in Fig. 5B is UDP Port 20202). The Ping Request 1906 packet is formatted as shown in Fig. 19, with the content of the shim and the ping packets exploded in further detail. In the shim 1930, the source and destination
15 Route Director public IP addresses (gIP) and private IP addresses (pIP) are all set to 0. In the system ping field 1960, the ping type field may be a ping request or a ping response. The Sequence field in the response is set to the same value as the Sequence field in the request packet.

Another function which may be performed is an Agent Query. Fig. 20
20 illustrates a query request from a Member Agent requiring system/status information of another member. The first Member Agent 565 at step 1802 will send a Query Request Packet 1810 to the VCN Manager 510. The Packet contains definitions for the Maximum Number of Records to return, a status Mask indicating whether the members are registered and/or joined, a platform
25 Mask, indicating the platform (desktop, server, laptop, mail server, etc) of the member, the FQDN Length, FQDN VCN Offset, Search String Length, Member

FQDN and a Search String for pattern matching. This packet is sent over the IPsec tunnel between the VCN Manager and the Member Agent.

If the packet is abnormal it is dropped at step 2012 if there is an error in the query authentication file or the member is not joined, NACK 2016 is sent in
5 step 2014. If the packet is not abnormal, no error is present, the member passes authentication and was joined, then the VCN Manager sends a query acknowledgement Packet 2030 to the member. The packet payload includes a number of records with the following fields: the status of the member, the platform type of the member, and the member's FQDN String. Note that the
10 FQDN is null-terminated and consistent with the FQDN in DNS format definitions. Here, a human readable FQDN "www.abcdefg.com" is encoded as "www.abcdefg.com\0x00".

Each joined member will periodically send a heartbeat packet to the VCN Manager so that the VCN Manager can determine if the member is alive. In
15 addition, the member's heartbeat packet is used to determine how long the member is actually joined. This information can be used to allow a provider of the infrastructure for the system to generate revenue from users on a per-use time basis. Conversely, the VCN Manager periodically sends its heartbeat packet to joined members so that the joined members can know if the Manager
20 is alive. This can be used by the member to determine if it should switch to a backup VCN Manager. Heartbeat packets are sent inside the system tunnel on the default tunneling port (UDP port 20202) and are IPsec protected.

ROUTE DIRECTORS

25 Route directors allow communication to a member that is in a private network. The PRD resides within a private network, behind the NAT device. The NRD resides on the public side of the NAT device. The NAT device can be

-50-

a Network Address Port Translation (NAPT) NAT device or a basic NAT where only addresses are translated.

Note that devices with public addresses do not require Route Directors (RDs). In the context of Fig. 5B, devices M_A and M_E do not require either a PRD or NRD, since they reside in the public address space. Likewise, M_X does not
5 require the PRD for its domain 540, since it has a public address (or is statically mapped to a public address at the NAT device 515).

The NRD implements a NAT traversal architecture which allows System packets to enter and exit a private network. The NRD maintains persistent
10 connections/sessions with members that are behind NAT devices. Member Agents initiate a TCP or UDP persistent connection/session with the NRD and use keep-alive messages to ensure that the NAT device does not drop the member's connection/session. The use of TCP or UDP is based on a bit set by the VCN Manager in the INIT ACK packet of the Join Protocol. Communication
15 to a member using a NRD tunnels between the NRD and the Member Agent through the persistent connection/session. More information about a suitable NAT traversal architecture is found in U.S. Patent Applications 10/233,289, "Accessing an Entity Inside a Private Network,;" and 10/233,288, "Communicating With An Entity Inside a Private Network Using an Existing
20 Connection to Initiate Communication," both of which are incorporated herein by reference.

When a member behind NAT attempts to join a virtual network by contacting the VCN Manager as discussed above, the VCN Manager will detect the presence of the NAT device, direct the member to a specific NRD and
25 indicate the use of TCP or UDP. The presence of the NAT device must be detected during the initialize Init message portion of the join sequence so the

-51-

VCN Manager can inform the member that it needs to setup a session with the assigned NRD prior to the Join message sequence.

In one embodiment, the NRD uses a pseudo address. The pseudo address is different than the virtual address and is used solely for NRD routing.

- 5 The pseudo address assigned by the NRD will allow the NRD to map a packet to the member's post-NAT IP address and UDP port.

- The process for establishing a session with a NRD and obtaining an address therefrom is shown in Fig 21. Initially (as described in Fig. 13), a member behind a firewall will send an init request 1304 to VCN Manager 510. In addition to the functions performed with respect to step 1306, 1308, and 1311 (of Fig. 13), the VCN Manager will detect that the member is behind a NAT device and whether it is served by a PRD in step 2120.
- 10

- The detection of a NAT device is accomplished using a field with the member's local IP address in the Init packet sent to the VCN Manager. The VCN Manager detects the fact that Agent 565 is behind a NAT device by comparing the member's private IP address in the INIT message payload with the source address in the TCP/IP headers. If the addresses differ, then a NAT device is present. At step 2120, the VCN Manager must next check if the member's NAT device is associated with a known PRD (Premises Route Director). If no PRD is found, then the VCN Manager will check if the member can use a known NRD. If an NRD is found then the INIT ACK 1314' will indicate that the member must establish a session with the NRD prior to joining the VCN. If the NRD can support TCP tunneling, the INIT ACK will also indicate to the member to start a TCP connection rather than a UDP connection. If neither a PRD nor an NRD is found for the private member, an Init NACK will be returned. The VCN Manager will find an available NRD and send an INIT ACK 1314' with
- 15
- 20
- 25

-52-

the NRD info data contained therein. The contents of an INIT ACK packet 1314 are discussed above with respect to Fig. 13.

At step 2132, the member will seek to establish a session with the NRD and will send address request 2130 to the NRD. The member sends the
5 Address Request Packet 2130 to the NRD. The packet includes an IP Header, UDP Header or TCP header, and Shim. In this case, the shim includes the NRD's public address. At step 2135, the NRD assigns the member a pseudo address. This is used as the member's private address in the Shim when external members send packets to the NRD for forwarding to the private
10 member. The NRD will store the association of the pseudo address with the Member's NAT device public address and port number. When other members of the VCN perform a DNS request on the member behind the NRD, as part of the DNS response, they will receive the public address of the NRD and they will receive the pseudo address as the private address for the member behind the
15 NRD. When sending a communication to the member behind the NRD, the outer packet will be addressed to the public address of the NRD. The NRD will access the shim to identify the pseudo address. The NRD uses the pseudo address as a handle to the persistent connection/session when sending packets through a NAT to the member. Once identifying the appropriate persistent
20 connection/session, the shim and virtual packet are encapsulated and sent to the destination, via the NAT device, using the identified persistent connection/session. When the NAT device receives the message, it will do the address and port translation, and forward the message to the member agent's real local address and port on the private network.

25 In one aspect, the pseudo address comprises portions of the public IP address space in IP version 4 that had been reserved for special purposes. This ensures that no machine within a private realm will have the same pseudo IP

address as the private address of a machine in any separate and distinct private realm. In order to prevent this from happening, the system of the present invention uses addresses that are otherwise not used or reserved. Examples include the 0.0.0.0, the 10.0.0.0, 14.0.0.0, 127.0.0.0, 169.2454.0.0, 172.16.0.0
5 and the like.

The NRD provides the pseudo address to the Agent 565 in a NAT Traversal Address Response Packet 2140. The packet includes a shim having an indicator that the response is a pseudo address response, as well as the source Route Director public IP address and Destination Route Director public
10 IP address, (which is set equal to the NRD address), the Source member private IP address (0) and the Destination member private IP address, which is the Virtual IP. Hence all communications for the Member Agent will be routed to the NRD 520. After acquiring the pseudo address from the NRD, the member designates that pseudo address to the VCN Manager as its local address in Join
15 packet 1318.

Note that there is an extra packet exchange 2145, 2150 when establishing a TCP connection that is not required when establishing a UDP connection with the NRD. This packet is the NRD Init Request Packet 2145. The previous TCP session for the Address Request and Address Response
20 must be closed and a new TCP session opened which will remain open for the duration of the tunnel session. The member sends the Init Request message to the NRD as the first message in this TCP session. This message only has a TCP header and System Shim preamble, and has no data following the Shim.

After receiving the pseudo address, the join process completes with the
25 join request packet 1318, and join ack packets 1328. After the join processing is complete, TCP/UDP encapsulated traffic flows between the member and the

NRD through the NAT. The member is now ready to establish connections with other members.

When outbound System traffic from a member behind a NAT device to the NRD is not frequent enough to keep the NAT device's mappings active, the member may to send keep alive messages to the NRD's TCP port 80 or UDP encapsulation port to ensure that the NAT device does not drop the TCP/UDP encapsulation session. The member sends this message to the NRD to ensure that the NAT device does not drop the TCP/UDP port mapping. The keep-alive messages do not need to be sent when other messages were sent out during the keep-alive interval.

The member sends this NAT Traversal Leave Packet message to the NRD to release the session and pseudo address when the member is leaving the VCN. The NAT traversal switch will verify that the receive-from socket address this message came from matches the lookup table entry before deleting the member's address.

GROUP AGENT

For some devices, member client software cannot be installed on the device or it is not desirable to install member client software on the device. For example, a printer or other networked devices may not be able to load software. For various reasons, some entities may not desire to add network software onto their machines. Additionally, some devices may use operating systems that do not support running the member agent software. For those devices that cannot or choose not to use member agent software, a Group Agent can be used. The Group Agent acts as a proxy for one or more members of a VCN without requiring installation of member agent software on the client devices. Thus, a

device can become a member of a VCN without changing any of the software on the device by using the Group Agent.

Fig. 22 is a block diagram depicting various components of the present invention utilizing a Group Agent. Note that some of the members of a VCN can use a Group Agent while other members do not use a Group Agent. Fig. 22 shows ten devices $M_1 - M_{10}$. Devices M_1, M_2, M_3, M_4 and M_{10} are devices that are participating in the VCN without using member agent software. Rather, they will use a Group Agent. Devices M_5, M_6, M_7, M_8 and M_9 are devices which include member agent software and, therefore, do not need to use a Group Agent. Fig. 22 shows some of the many varieties of permutations of using Group Agents, Network Route Directors and Private Route Directors. Other permutations can also be used with the present invention. Also note that Fig. 22 is more of a structural view of additional components of the present invention, as compared to Fig. 5B which is more of a symbolic/logical view.

Fig. 22 includes a first private network which connects to the Internet (or other network) via NAT device 2202. In addition to NAT 2202, the private network includes device M₁, device M₂ and Group Agent 2204. In one embodiment, the Group Agent runs on the same machine as a Private Route Director. Devices M₁ and M₂ do not include agent software. Rather, they participate in the VCN using Group Agent 2204.

A second private network allows devices to communicate to the Internet (or other network) via NAT device 2210. That private network also includes Group Agent 2212, device M₃ and device M₄. Note that Group Agent 2212 does not include a Private Route Director. Thus, for devices M₃ and M₄ to be reached by other members of the VCN, communication is performed via Network Route Director 520. In one embodiment, each of the private networks are different physical address realms. That is each uses a different set of private IP

addresses. The present invention will also work if the private networks have overlapping addresses. That is, one or more private IP addresses are used by more than one private network involved in a VCN.

A third private network, which includes devices M₅ and M₆, provides for communication on the Internet via NAT device 2220. A fourth private network, which includes devices M₇ and M₈, allows its components to communicate on the Internet (or other network) via NAT device 2230. This fourth private network includes Private Route Director 2232. Because devices M₇ and M₈ include member agent software, there is no need for a Group Agent on this network. Device M₉ has a public IP address and includes member agent software; therefore, it communicates and participates in the VCN as described above. Device M₁₀ has a public IP address; however, device M₁₀ does not include member agent software. For device M₁₀ to participate in the VCN, it must make use of Group Agent 2234, which has a public IP address.

In one embodiment, a Group Agent includes software running on a computing device, including (but not limited to) a server, router, personal computer, minicomputer, mainframe, mobile computing device, or other suitable computing device. In other embodiments, the Group Agent, or any other of the software components described above, can be performed by its special purpose computing device.

A Group Agent acts as a proxy for one or more members which do not have member agent software. For example, Group Agent 2204 is a proxy for devices M₁ and M₂; and Group Agent 2212 is a proxy for devices M₃ and M₄. Group Agent 2234 is a proxy for device M₁₀. Although Fig. 22 shows the Group Agents being proxies for one or two members, a Group Agent can be a proxy for more than two members.

Communication between two members of a VCN can pass through two NAT devices, one NAT device for each member. For example, communication between device M_1 and device M_4 will pass through NAT device 2202 and NAT device 2210. Additionally, communication between device M_1 and another entity
5 in a private network configured like the private network of device M_1 will require communication to pass through two NAT devices.

Note that a single Group Agent can participate in more than one VCN. For example, Group Agent 2204 can be used to allow device M_1 participate in a first VCN and concurrently (for all or part of the time) allow device M_2 to
10 participate in a second VCN. Because there can be multiple virtual community networks, the VCN Manager is able to create and maintain, the multiple virtual community networks. As described herein, the VCN Manager identifies which entities can communicate on each VCN by maintaining a list of domain names for each VCN. For example, one list may include the domain names for devices
15 $M_1 - M_{10}$.

The Group Agent requires initialization so it may know which members it is a proxy for. Group Agent initialization cannot occur until after the Group Agent has joined the VCN Manager as a member. The join prior to Group Agent initialization is for a pseudo-member so the proxy initialization messages can
20 use virtual IP addresses and the tunneling protocols described above to travel on an IPsec tunnel between VCN Manager 510 and the particular Group Agent. Separate member specific tunnels will be created when the Group Agent later joins for the proxied members. The Group Agent join will require the Group Agent to be registered with the VCN Manager. In one embodiment, this
25 registration will be done during the installation of the Group Agent.

Fig. 23 provides a flowchart describing one embodiment of the process for Group Agent initialization. In step 2302, the Group Agent joins as a pseudo-

-58-

member. This process of step 2302 is performed as described above. In step 2304, the Group Agent will send an initialization request to the VCN Manager. The initialization request is a packet that includes the fully qualified domain name for the Group Agent, a packet version indication, a packet type indicating that it is an initialization request, a packet length, and an authentication code. If the received initialization request is abnormal (step 2306), then the initialization request is dropped in step 2308. If the packet was normal but authentication failed (step 2312), then the VCN Manager sends a NACK to the Group Agent in step 2314. If authentication was successful and the initialization request was normal, then the VCN Manager sends an acknowledgement to the Group Agent in step 2320.

After completion of step 2320, the Group Agent is initialized and now must join each of the members it is proxying. To do so, the Group Agent will perform a loop where each iteration will include joining for one of the members that is being proxied. In step 2322, it is determined whether there are any more members being proxied that have to be joined. If there are more members to join, then the Group Agent will join for one member being proxied in step 2324 and the method will loop back to step 2322. When there are no more proxied members to be joined, the process of Fig. 23 is complete (step 2330). The process of joining for a proxy member is the same as the process of joining described above; however, the process is performed for the member by the Group Agent rather than by the member agent. The virtual IP address received by the Group Agent is for the member being proxied. The Group Agent stores that virtual IP address in a data structure for the member. In one embodiment, there is a separate data structure for each member being proxied. In another embodiment, there is one data structure which has separate records for each member being proxied. This data stored will include the member's virtual IP

address and private address in the local LAN, as well as other information that will be described below.

The acknowledgement sent from the VCN Manager to the Group Agent in step 2320 contains all of the member information required so the Group Agent
5 can send the appropriate join requests for each member being proxied. The following information is in the acknowledgement sent from the VCN Manager to the Group Agent: packet version indicating the version of the header, packet type indicating that it is a acknowledgement, packet length, authentication code, subnet IP address, subnet prefix, public IP address of the Private Route Director
10 (when the Group Agent also includes a Private Route Director), Private Route Director ping flag (1 if PRD responds to pings), the number of members being proxied, the number of permanent connections from proxied members to other members that the proxy must make, the member record list and the connect record list. The member record list is a set of records for each member being
15 proxied. The following information is stored in each record: member password (password SHA1 digest), member's local private IP address, the length of the member's fully qualified domain name, the member's fully qualified domain name, offset to the VCN name, authentication type (0=preshared 1=certificate), time stamp indicating when the token key was created, token length in bytes,
20 token key (member shared secret with VCN Manager), HA version number, number of HA records, HA record list and authentication key (generated by server for the proxy). Each HA record in the HA record list includes a VCN Manager IP address for the next VCN Manager, a join port for the next VCN Manager and a service port for the next VCN Manager in case the current VCN
25 Manager goes down. The connect record list includes the following three fields: proxy member index (zero based index into member list), DNS request length and a DNS request.

-60-

Once the Group Agent joins for all of its members, then any of its members can receive communication from other members of the VCN or can initiate communication to other members in the VCN. Members that are being proxied by a Group Agent can communicate with other members being proxied by the Group Agent, with other members proxied by a different Group Agent (regardless of whether they are in a private network or available on the public Internet), and members that do not use a Group Agent (regardless of whether those other members are in a private network or available on the Internet with a public IP address), as long as they are all members of the same VCN. From the point of view of an application on a member being proxied by the Group Agent, the VCN appears as a local subnet (or LAN) and all of the members of the VCN appear to be on the local subnet (or LAN). However, the VCN is not a local subnet (or LAN); rather it is a virtual subnet (or LAN). Each of the members of the VCN will have a Virtual IP Address on the virtual subnet.

Because members of a VCN register with the VCN Manager, the VCN Manager will know how to find the members (e.g. it will know its public and private addresses). Thus, a Group Agent acting as a proxy for a first member will be able to act as an intermediary for that first member when talking to a second member of a VCN even if the second member moves to a different or new private network and/or changes its IP address. That is, when the second member makes the move or change, the second member will so inform the VCN Manager. The VCN Manager will inform the Group Agent of the change so that the Group Agent can continue to act as an intermediary between the first member and the group member. More information about communicating with mobile entities can be found in U.S. Patent Application No. 10/233,289, "Accessing An Entity Inside a Private Network," filed on August 30, 2002; U.S. Patent Application No. 10/161,573, "Creating A Public Identity For An Entity On

A Network," filed on June 3, 2002; and U.S. Patent Application No. 10/233,288, "Communicating With An Entity Inside A Private Network Using An Existing Connection To Initiate Communication," filed on August 30, 2002, all three applications are incorporated herein by reference in their entirety.

5 Fig. 24 is a flowchart describing one embodiment of a process for initiating communication with a member that is being proxied by a Group Agent. In Fig. 24, the communication is being initiated by a member that is not being proxied by a Group Agent. That is, the member initiating communication is a member that has agent software loaded on it. That member is initiating
10 communication with a member that does not have agent software. Prior to the process of Fig. 24 being performed, the Group Agent has joined the member into the VCN and the member initiating communication has already joined the VCN. For example purposes, looking at Fig. 22, the process of Fig. 24 can be performed by M₅, M₆, M₇, M₈ or M₉ initiating communication with any of devices
15 M₁, M₂, M₃, M₄ or M₁₀. Assume, for example purposes, that device M₉ is initiating communication with device M₁. The destination device is also assumed to be served by a Private Route Director.

 In step 2402, an application on the source device (e.g., device M₉) is intending to send a message to an application on the destination device (e.g.,
20 device M₁). In step 2404, the application on the source device sends a DNS request to the VCN Manager using the domain name of the destination. For example, the application on M₉ will send a DNS request using the domain name for M₁. In step 2406, the VCN Manager returns a response to the DNS request. This response includes the public IP address for private Route Director 2204,
25 the private IP address for member M₁ and the virtual IP address for member M₁. In some embodiments, the DNS response also includes a token key (as described above). The Agent on the source device (e.g., M₉) stores the

information it received from the VCN Manager. In step 2410, the Agent on the source device returns the virtual IP address for the destination to the application which initiated the DNS request. In step 2412, the application on the source device initiates the sending of a message to M_1 using the virtual IP address.

5 That is, a virtual IP packet is created where the source address is the virtual IP address for the source machine (M_9) and the destination address in the virtual IP packet is the virtual IP address for the destination device (device M_1). The virtual IP packet is created in step 2414 and subject to IPsec (or other security means). In step 2416, the virtual IP packet is encapsulated. Encapsulation

10 includes adding a shim, a UDP header and an IP header, all as described above. The shim includes the public IP address for the Private Route Director associated with the destination member (e.g., PRD 2204) and the private IP address for destination (e.g. member M_1). If the source, the member initiating communication was in a private network, then the shim would also include the

15 public IP address for the Route Director associated with the source and the private IP address for the source. In step 2418, the encapsulated packet is sent to the NAT for the destination's private network. That is, in the example above, the newly created packet is sent to NAT 2202 via the Internet (or other network). In step 2420, the encapsulated packet is sent from the NAT (e.g., NAT 2202) to

20 the Route Director for the destination (e.g., PRD 2204).

In step 2422 of Fig. 24, the Route Director removes the virtual IP packet and the shim from the encapsulation and presents both the virtual IP address and the shim to the Group Agent (e.g., Group Agent 2204). The Group Agent stores the information from the shim, as described above with respect to the

25 member agent software. In one embodiment, the Group Agent includes the necessary logic to received the communication so that no route director is necessary. In step 2426, the Group Agent extracts the virtual IP packet from

IPsec. In step 2428, the Group Agent chooses a private IP address for the source entity. In the above example, the source entity is device M₉. Group Agent 2204 will pick a private IP address that is routable in the private network associated with device M₁ and NAT 2202. This private address will be used by
5 device M₁ to identify M₉. In step 2430, the Group Agent will change the source address in the virtual packet. That is, the virtual packet originally had a source address equal to the virtual IP address for the source device (e.g., M₉) and a destination address equal to the virtual IP address for the destination device (e.g., M₁). In step 2430, the source address in the virtual IP packet is changed
10 to be equal to the private IP address chosen by the Group Agent for M₉ in step 2428. In step 2432, the Group Agent changes the destination address in the virtual IP packet to be equal to the private IP address in the local LAN for M₁. In step 2434, the packet is sent by the Group Agent to the destination machine (e.g., sent to M₁).

15 The above discussion of Fig. 24 was made with respect to the example that the communication has been initiated by device M₉ which is a member having a public IP address and member agent software. The process of Fig. 24 can also be performed by a member which does not have a public IP address, including members using a Private Route Director and/or a Network Route
20 Director. When the process of Fig. 24 is being performed by members using Route Directors, the shim that is added to the encapsulated packet in step 2416 includes the private IP address for the member and the public IP address for the Route Director. The example used in discussing Fig. 24 also assumes that the destination was a device in a private network where the private network included
25 a Group Agent and a Private Route Director. The process of Fig. 24 can also be adapted to work with a member using a Group Agent where the member has a

public IP address and/or a member in a private network that uses a Network Route Director.

When sending communication to an entity with a public IP address that uses a Group Agent, the shim will include the public IP address for the Group Agent and the public IP address for the member in step 2416. The packet will not be sent to a NAT or to a Route Director. Rather, the packet will be sent directly to the Group Agent. The Group Agent will access the virtual IP packet in step 2426. Rather than choosing a private IP address to identify the source, the Group Agent will choose a public IP address for the destination to use to refer to the source. The virtual IP packet will be changed so that the source address is equal to the public IP address chosen by the Group Agent to represent the source and the destination address will become the public IP address for the destination. The virtual IP packet (which is no longer virtual) will be sent to the destination.

If the destination member participates in a VCN using a Network Route Director (e.g., device M_3 using NRD 520), then the encapsulated packet is sent to the Network Route Director in step 2418. The Network Route Director will communicate the shim and virtual IP packet to the Group Agent (e.g., Group Agent 2212) via a persistent connection as described above in Fig. 7, steps 673-675, 677, except that the packet is forwarded to the Group Agent rather than the NAT device. The Group Agent will then perform steps 2424 – 2434, as described above.

Fig. 25 is a flowchart describing one embodiment of a process for the destination device responding to the initiation of communication from the source device. In the example discussed above, this process would include device M_1 responding to device M_9 . In step 2502, the application on device M_1 attempts to send a communication. A packet is then created using the private addresses.

The packet would include a source address equal to the private IP address in the LAN for device M_1 . The destination address would be equal to the private IP address in the LAN that is used to identify device M_9 . That packet is sent to the Group Agent in step 2504. In step 2506, the Group Agent changes the packet
5 by replacing the private addresses with virtual addresses. The source address is replaced with the virtual IP address in the VCN used to identify device M_1 . The destination address in the packet is replaced with the virtual IP address in the VCN used to identify device M_9 . In step 2508, this packet is subject to IPsec, and encapsulated as described above.

10 In step 2512 of Fig. 25, the Group Agent sends the packet. In the example above, the Group Agent would send the encapsulated packet to device M_9 using the public IP address for device M_9 . If the Group Agent is sending the packet to a member that is in a private network, then the encapsulated packet would be sent to the Group Agent/Private Route Director for the member or to
15 the Network Route Director for that member. If the responding device (e.g. M_1) is using a Network Route Director, then the Group Agent can still send the reply packet directly to the original source without going through the Network Route Director. If the replying device (e.g. M_1) has a public IP address, then the packet sent to the Group Agent would include the public IP addresses for the
20 responding device and the public IP address that the Group Agent told the replying device to use to identify the original source device. In one embodiment, when the member using the Group Agent has a public IP address, an IPsec tunnel can be created between the Group Agent and the member device.

25 Fig. 24 contemplates communication being initiated by a device that has member software loaded on it. Fig. 26, on the other hand, describes a process that is performed when communication is initiated by a device that does not have member software and, therefore, uses Group Agent software. In step

2602, the application on the initiating member will send a DNS request. This DNS request will be sent to the Group Agent. The Group Agent receives the DNS request in step 2604. In step 2606, the Group Agent sends its own DNS request for the same domain name to the VCN Manager. In step 2608, the
5 Group Agent receives a response from the VCN Manager. This response will include the virtual IP address for the target, the public IP address of the Route Director for the target (if any) and the private IP address for the target (if any). If the target has a public IP address, then the public IP address will be returned. In step 2610, the Group Agent will choose a private IP address in the local LAN
10 to be used to identify the target. The virtual IP address returned from the DNS request will be mapped to this private IP address in the local LAN. In step 2612, the Group Agent will return that chosen private IP address to the application as a response to the application's DNS response. In step 2614, the application will initiate the communication. In one embodiment, the process of 2614 includes
15 performing the steps of Fig. 25. Note that if the member who is initiating the communication in the process of Fig. 26 has a public IP address, rather than being in a private network, then in step 2610 the Group Agent will map the virtual IP address to a public IP address that the Group Agent and member will use to identify the target. It is this mapped public IP address that is returned to
20 the application in response to the DNS request. The mapped public IP address is routable to the Group Agent.

Although the Group Agent is described above with respect to use with a VCN, the technology of the Group Agent is broader than a VCN. Thus, the Group Agent can be used to allow entities to participate in other types of
25 networks, communities, groups, organizations, communications, etc.

Note that in one embodiment, the member being serviced by the Group Agent must be in the same physical address realm as the Group Agent. In this

-67-

manner, the Group Agent is used to bridge that physical address realm with the virtual space. The Group Agent contains the functionality to allow the member to participate in the virtual community; however, all the protocols of the virtual community terminate at the Group Agent. This way, the member receives a normal IP packet. From the point of view of the member, the Group Agent works like a router which connects the member to the subnet of virtual nodes.

The foregoing detailed description of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, any number of VCN Managers may be used. Any combination of NRDs and PRDs may be used to improve network efficiency. Any combination of Member Agents and Group Agents may be used, and the Virtual Community may be of any size. Additionally, while the above description provided an example using the protocols and addressing currently used on the Internet, the present invention can be used with other protocols and addressing schemes. The described embodiments were chosen in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto.

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.app

Express Mail No: EV 251 363 937 US

CLAIMS

We claim:

- 5 1. A virtual community network system, comprising:
 a virtual network manager including at least one virtual community
definition comprising at least a domain name and a user set; and
 at least one route director capable of communicating with users in the
user set.
- 10 2. The system of claim 1 wherein each user communicates with the
virtual network manager and other users in the user set via at least one agent.
3. The system of claim 2 wherein the agent is installed on a
15 processing device.
4. The system of claim 2 wherein the agent is installed on a proxy
device.
- 20 5. The system of claim 2 wherein the virtual network manager
includes a NAT device detector for agents installed on a processing device
behind a NAT device.
6. The system of claim 1 wherein the manager comprises a device
25 coupled to a public network and having a public network address.

7. The system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device.

5

8. The system of claim 7 wherein each said device includes at least one virtual address in the community and at least one physical address.

9. The system of claim 8 wherein the physical address is dynamic.

10

10. The system of claim 8 wherein the physical address is static.

11. The system of claim 8 wherein the physical address is private.

15

12. The system of claim 8 wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device.

13. The system of claim 12 wherein the physical address is dynamic.

20

14. The system of claim 12 wherein the physical address is static.

15. The system of claim 12 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

25

16. The system of claim 15 wherein said second device includes at least one virtual address in the realm and at least one private physical address.

-70-

17. The system of claim 15 wherein the physical address is dynamic.

18. The system of claim 15 wherein the physical address is static.

5 19. The system of claim 15 wherein said at least first private network
and said at least second private network share at least one network address.

20. The system of claim 1 wherein the route director includes a
pseudo address assignment for at least one user in the user set.
10

21. The system of claim 1 wherein the route director includes a
translator for virtual address information for a virtual user in a private network
realm.

15 22. The system of claim 1 wherein the virtual community manager is
coupled to a public network and includes a public network address.

23. The system of claim 22 wherein the route director is coupled to
said public network and includes a public network address.
20

24. The system of claim 22 wherein the route director is coupled to a
first private network and said route director includes a private network address.

25 25. The system of claim 1 wherein communications between users in
the user set are encapsulated.

-71-

26. The system of claim 1 wherein communications between users in the user set are encrypted.

27. The system of claim 26 wherein said encryption uses IPSEC.

5

28. The system of claim 26 wherein said encryption uses DES.

29. The system of claim 26 wherein said encryption uses triple DES.

10

30. The system of claim 1 wherein the manager includes at least a second virtual domain definition.

31. The system of claim 1 further including at least a first public route director and a second private route director.

15

32. A system, comprising:

a management device including network interface coupled to a public address realm and having a public address;

a virtual community network traffic router; and

20

router data including at least one association of a logical identifier with public routing information for a member.

33. The system of claim 32 wherein the network traffic router includes a network interface accessible by a public address in the public address realm.

25

34. The system of claim 32 wherein the management device includes a UDP port capable of receiving virtual community network traffic.

-72-

35. The system of claim 32 wherein the management device includes a TCP port capable of communicating virtual community network traffic.

36. The system of claim 32 wherein a member accesses a physical
5 network via a processing device and the system further includes at least one agent installed on the processing device.

37. The system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router
10 includes a transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent.

38. The system of claim 32 further including at least one proxy agent on a private physical network communicating with a member and the network
15 traffic router.

39. The system of claim 38 wherein the member accesses other members using a device coupled to a private physical network.

40. The system of claim 32 wherein the manager includes a member
20 register module.

41. The system of claim 40 wherein the manager includes a member
join module.
25

42. The system of claim 41 wherein the join module provides a virtual address to a registered member.

-73-

43. The system of claim 41 wherein the manager maintains data on an association between at least one virtual address with at least one member.

44. The system of claim 40 wherein the manager includes a DNS
5 server for the virtual community.

45. The system of claim 32 further including a virtual community network communication agent for a device, comprising a virtual network adapter interfacing with the device and applications on the device to route traffic to
10 members of the virtual community via their virtual address.

46. The system of claim 45 wherein the agent includes a domain name routing plugin.

15 47. The system of claim 45 wherein the agent includes a separate IP stack for each user in the user set accessing the device.

48. The system of claim 45 wherein the adapter is a deterministic network enhancer.
20

49. The system of claim 45 wherein the adapter includes a DNS plugin.

50. The system of claim 45 wherein the adapter includes an IPSEC
25 plugin.

-74-

51. The system of claim 45 wherein the adapter includes a domain name routing plugin.

52. The system of claim 45 wherein the agent includes a community
5 registration module.

53. A virtual community network system, comprising:
a virtual community network manager;
a route director;
10 at least a first virtual community agent associated with a first community member; and
at least a second virtual community agent associated with at least a second community member.

15 54. The system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address.

55. The system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private
20 physical network address.

56. The system of claim 53 wherein the first or second virtual community network agent is installed on a device used by a member to access a network.
25

57. The system of claim 56 wherein the device is in a private physical network.

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.app

Express Mail No: EV 251 363 937 US

-75-

58. The system of claim 56 wherein the device is coupled to a public physical network.

59. The system of claim 53 wherein the first or second virtual
5 community network agent is a proxy agent.

60. The system of claim 53 wherein the first and second members
access the virtual community via devices coupled to separate private address
physical realms.

10

61. The system of claim 53 wherein the virtual community network
manager includes at least a first community definition and a second community
definition.

15 62. The system of claim 53 wherein the community network manager
includes a member authenticator.

63. The system of claim 62 wherein the community network manager
includes a DNS server providing authoritative responses for DNS queries in the
20 virtual community.

64. A method for providing a secure virtual network, comprising:
providing a virtual network manager coupled to a public network;
defining a member set of users entitled to communicate in the virtual
25 network;
registering members with the manager;

-76-

assigning members a virtual address; and
routing network traffic between the members in the virtual community.

65. The method of claim 64 further including the step of providing
5 users in said member set with a communication agent.

66. The method of claim 65 wherein said step of providing users with a
communication agent includes providing a proxy agent.

10 67. The method of claim 65 wherein said step of providing users with a
communication agent includes providing an agent installed on a device used by
the member to couple to a network.

68. The method of claim 65 wherein the step of registering comprises
15 authenticating members with the member set.

69. The method of claim 64 wherein the step of defining a member set
includes the step of assigning a domain name for the community.

20 70. The method of claim 64 wherein the step of defining a member set
includes defining at least two member sets having at least one different member.

71. The method of claim 64 wherein the step of assigning a virtual
address includes assigning an IPV4 compliant address.

25 72. The method of claim 71 wherein the step of assigning a virtual
address includes assigning a non-routable IPV4 compliant address.

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.app

Express Mail No: EV 251 363 937 US

73. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address with a second member accessing the public network on a second device having a different public address.

5

74. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address with a second member accessing the public network on a second device having a public address.

10

75. The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address with a second member accessing the public network on a device in a private physical network having a second private physical address.

15

76. The method of claim 75 wherein the first private physical address and the second private physical address are identical.

20

77. The method of claim 64 further including the step of responding to DNS requests for members in the virtual network.

78. The method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network.

25

79. The method of claim 64 further including applying a group policy to members of the virtual community.

80. One or more processor readable storage devices having processor
5 readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

managing a virtual community network realm;
defining a member set of users entitled to communicate in the virtual
10 community;
registering users with the virtual community;
assigning each user a virtual address; and
routing network traffic between the users in the virtual community.

15 81. One or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent.

20 82. One or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent.

25 83. One or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community.

84. One or more processor readable storage devices as defined in claim 80 wherein the step of assigning a virtual address includes a non-routable IPV4 compliant address.

5 85. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device having a public address with a second member accessing the public address realm on a second device having a different public address.

10

 86. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address with a second member accessing the public address realm on a second device having a public address.

15

 87. One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address with a second member accessing the public address realm on a device in a private physical network having a second private physical address.

20

 88. One or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device.

25

-80-

89. One or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical.

5 90. One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic.

91. One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic.

10

92. One or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community.

15

93. A virtual community network system, comprising:

a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set, the network being assessable by users in the user set and users outside the user set, the manager exchanging virtual community network information with users in the user set.

20

94. The system of claim 93 wherein the virtual network manager includes a member register module.

25

95. The system of claim 93 wherein the virtual network manager includes a member join module.

96. The system of claim 95 wherein the join module provides a virtual address to a registered member.

97. The system of claim 93 wherein the virtual network manager
5 maintains data on an association between at least one virtual address with at least one member.

98. The system of claim 93 wherein the virtual network manager
includes a DNS server for the virtual community.
10

99. The system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device.

100. The system of claim 93 wherein the virtual network manager
15 includes at least a second virtual domain definition.

101. The system of claim 93 wherein the virtual network manager includes at least a first virtual community definition and a second virtual
20 community definition.

102. The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. The system of claim 93 wherein the virtual network manager
25 includes a DNS server providing authoritative responses for DNS queries form users in the virtual community.

-82-

104. The system of claim 93 wherein the system further includes at least one route director capable of communicating with users in the user set.

105. The system of claim 93 wherein each user communicates with the
5 virtual network manager and other users in the user set via at least one agent.

106. The system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses
10 other users in the community using at least a second processing device, wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device.

107. The system of claim 106 wherein said first device is coupled to
15 said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. The system of claim 93 wherein communications between users in the user set are encrypted.
20

109. The system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications.
25

-83-

ABSTRACT

A private virtual dynamic network is provided for computing devices coupled to public networks or private networks. This enables computing devices anywhere in the world to join into private enterprise intranets and communicate with each other. In one embodiment, the present invention provides a separate
5 private virtual address realm, seen to each user as a private network, while seamlessly crossing public and private network boundaries. One implementation of the present invention uses an agent to enable an entity to participate in the network without requiring the member to add new hardware or software.

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.app

Express Mail No: EV 251 363 937 US

10403319-053103

Fig. 1

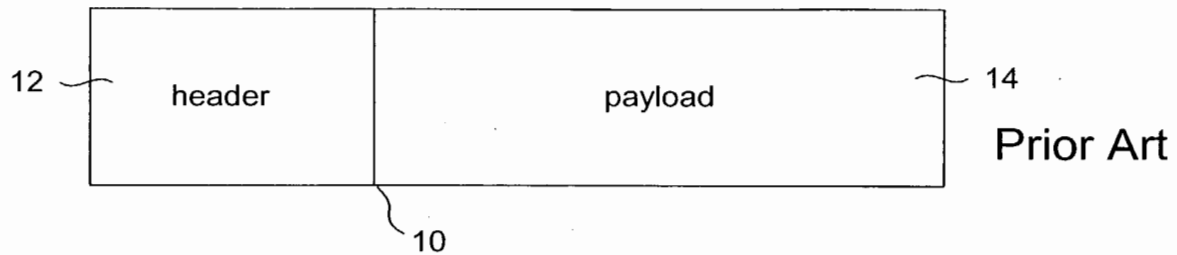


Fig. 2A

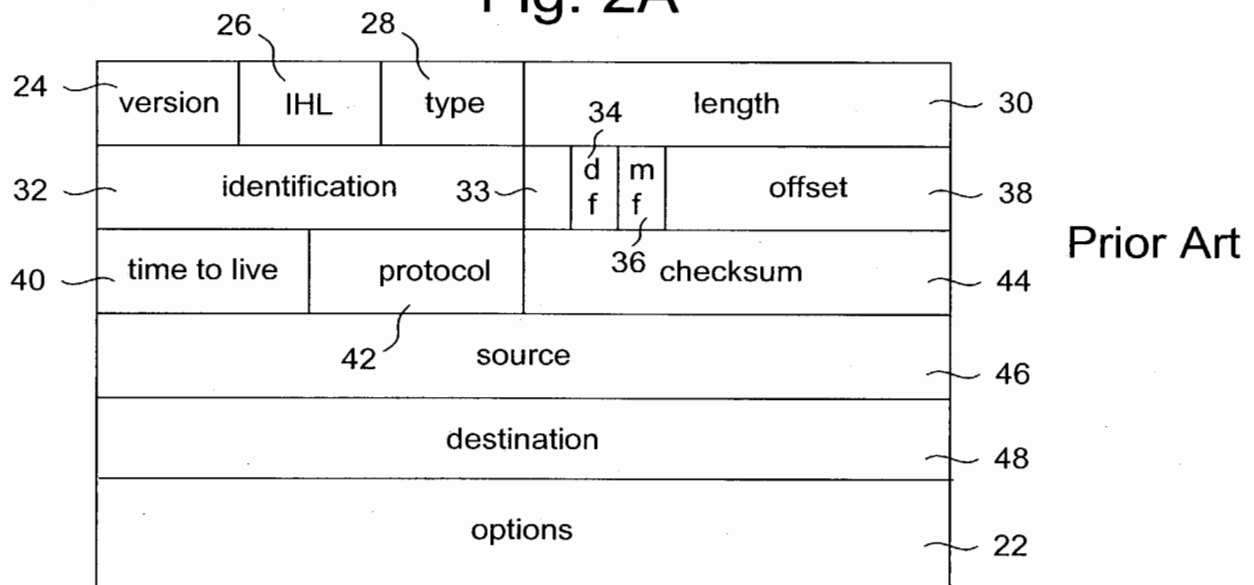
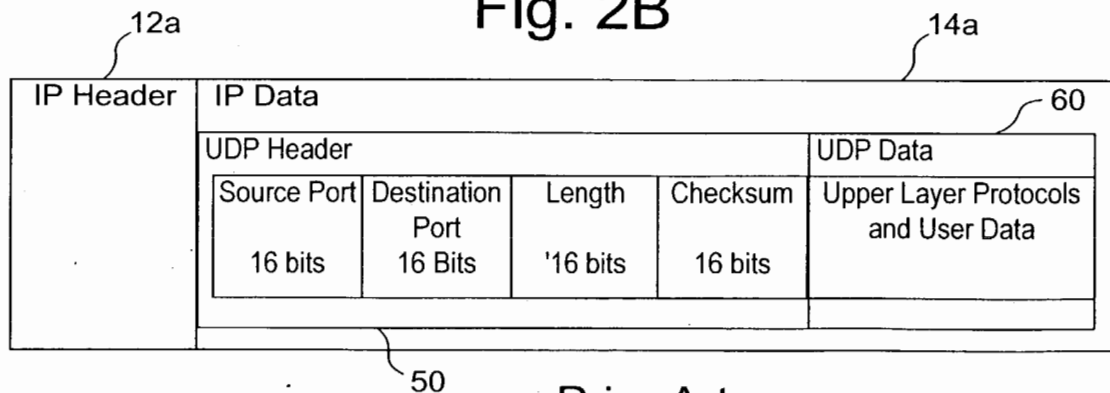


Fig. 2B



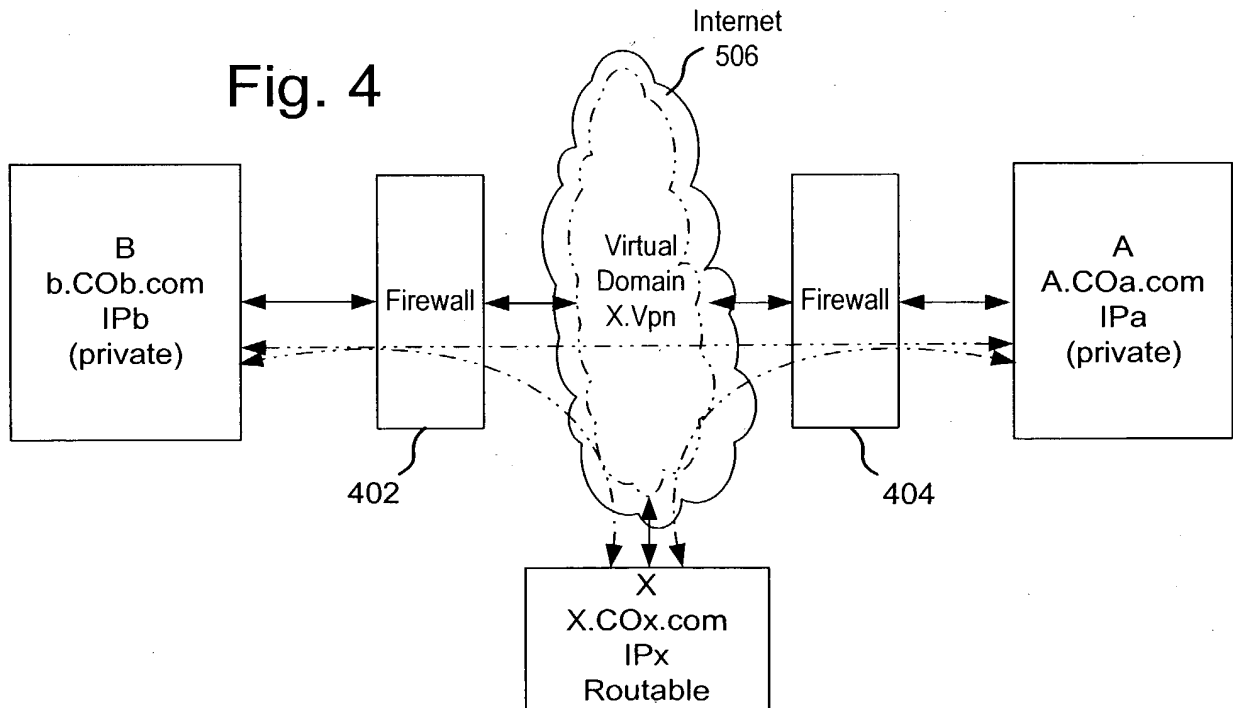
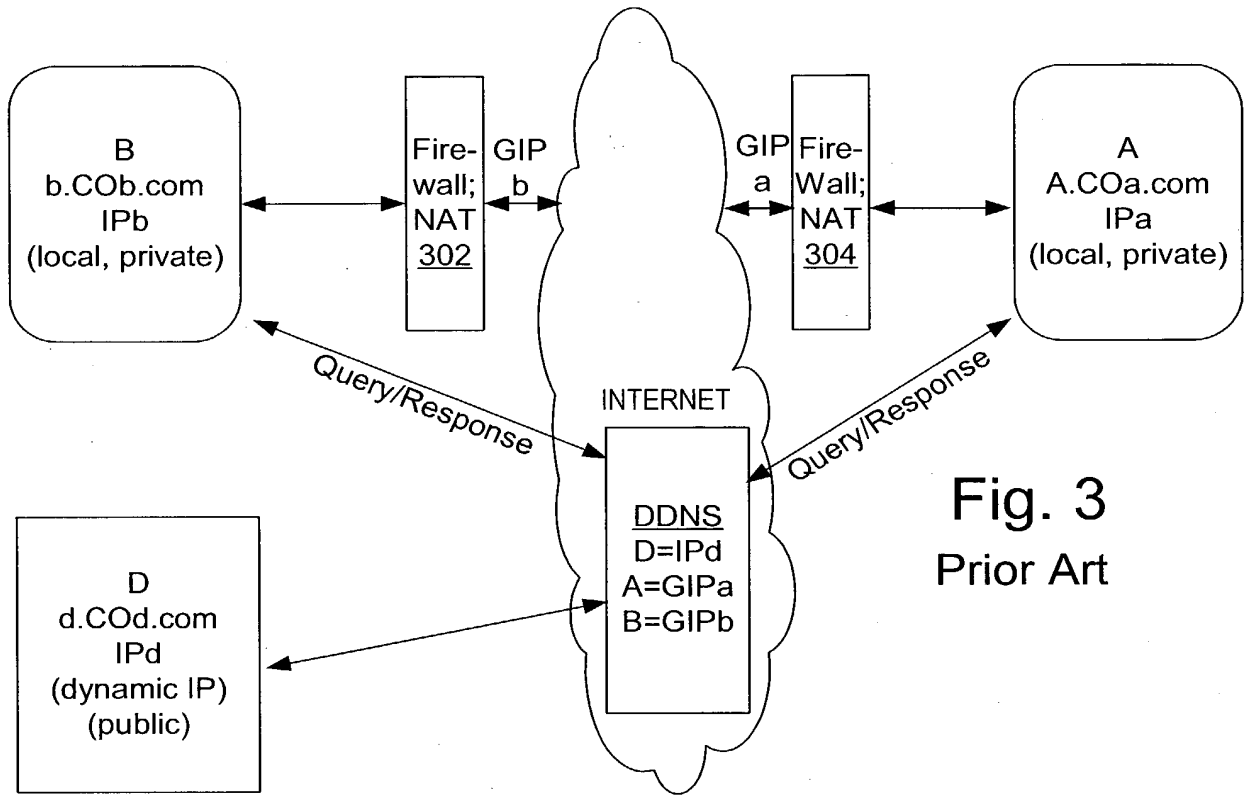
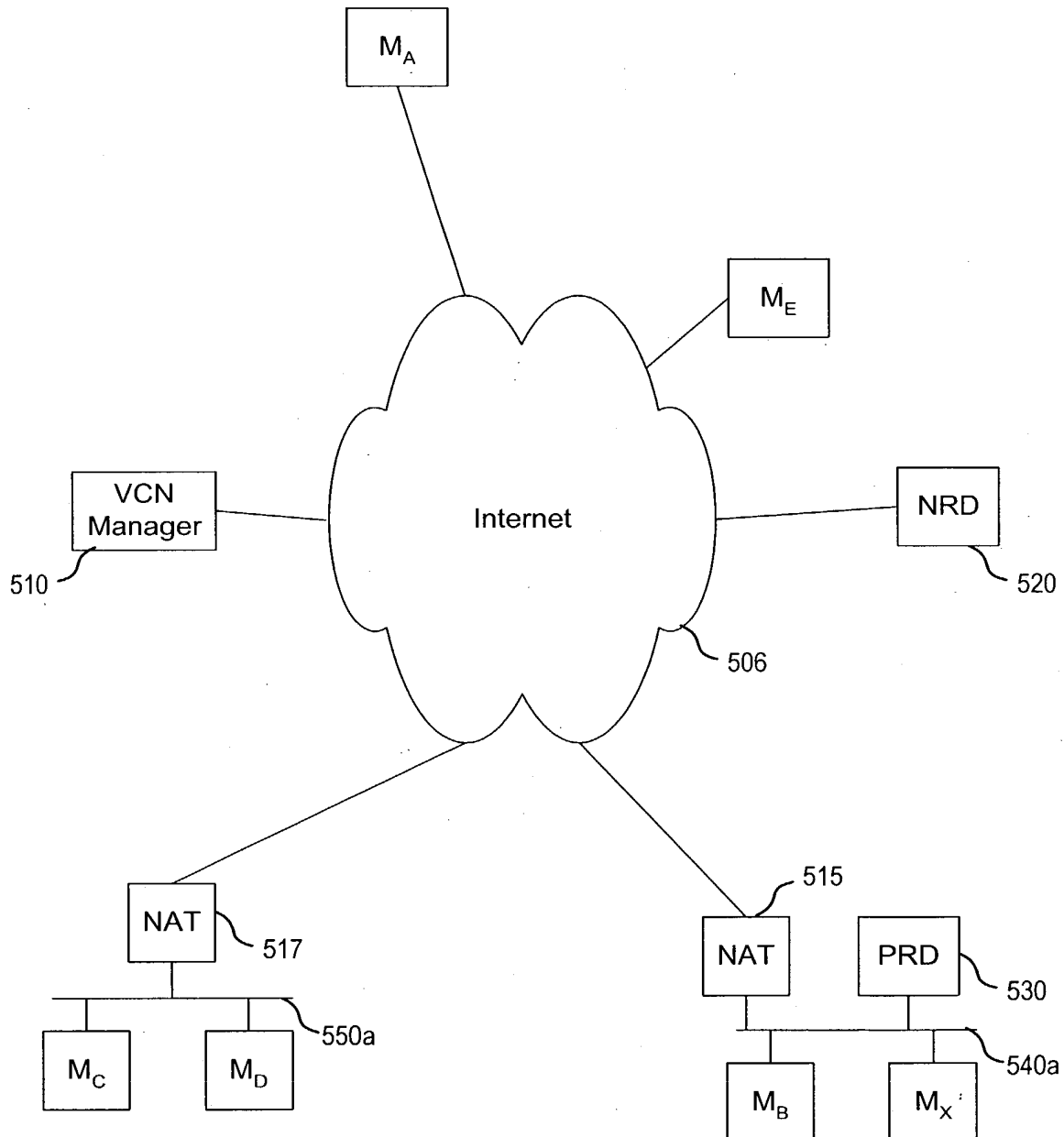
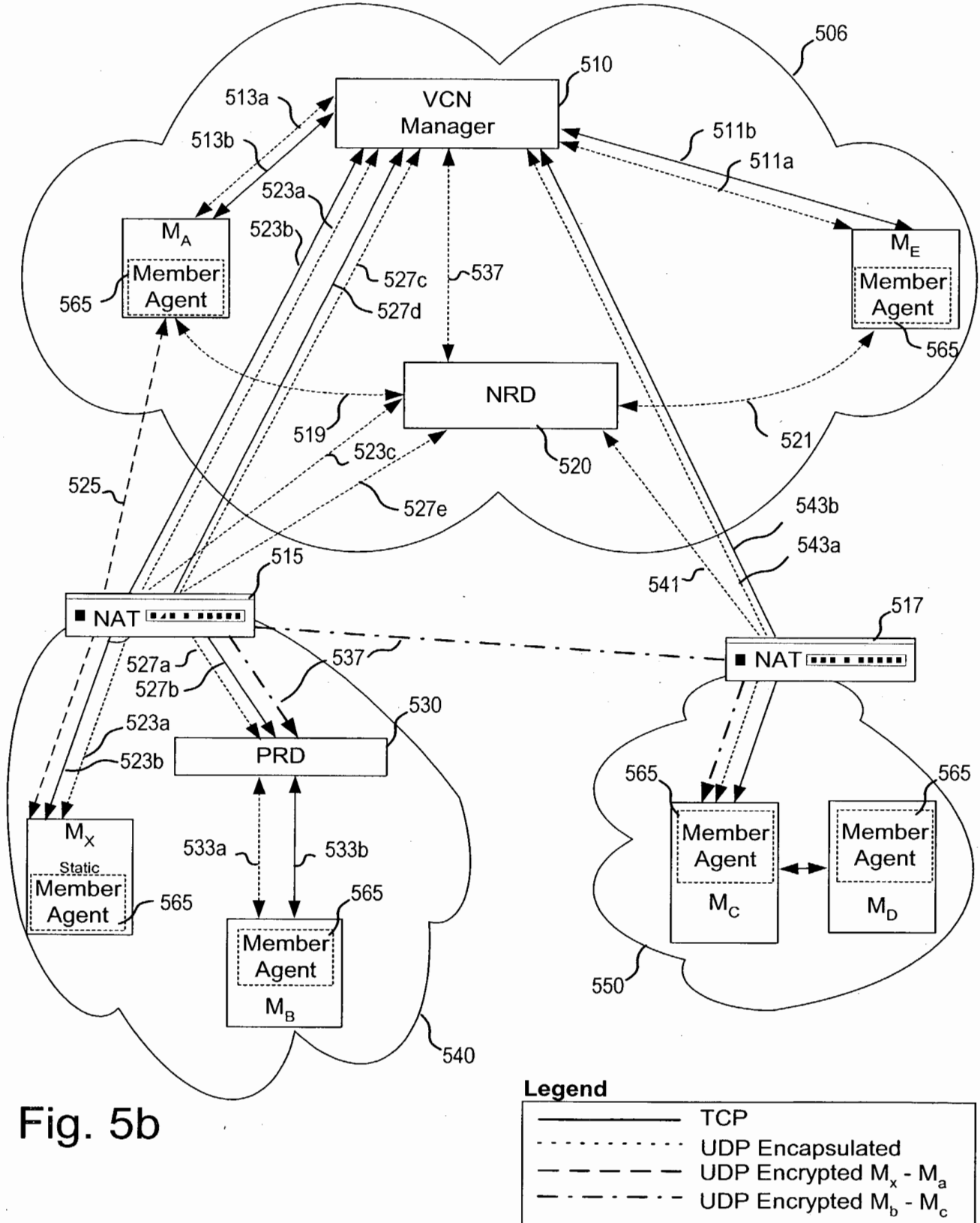


Fig. 5a





Legend

—	TCP
...	UDP Encapsulated
- - - -	UDP Encrypted $M_x - M_a$
- - - -	UDP Encrypted $M_b - M_c$

Fig. 6A

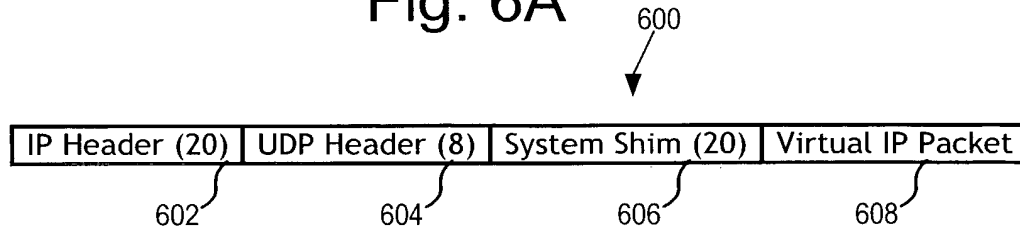


Fig. 6B

606

Field Name	Description
Protocol Version	Version information
Data Type	Type of data following Shim
Header Option Flags	Option Flag Information
Source RD Public IP	Source Route Director gIP
Dest RD Public IP	Destination Route Director gIP
Source Member pIP	Source Member Private IP
Dest Member pIP	Destination Member Private IP

Fig. 7

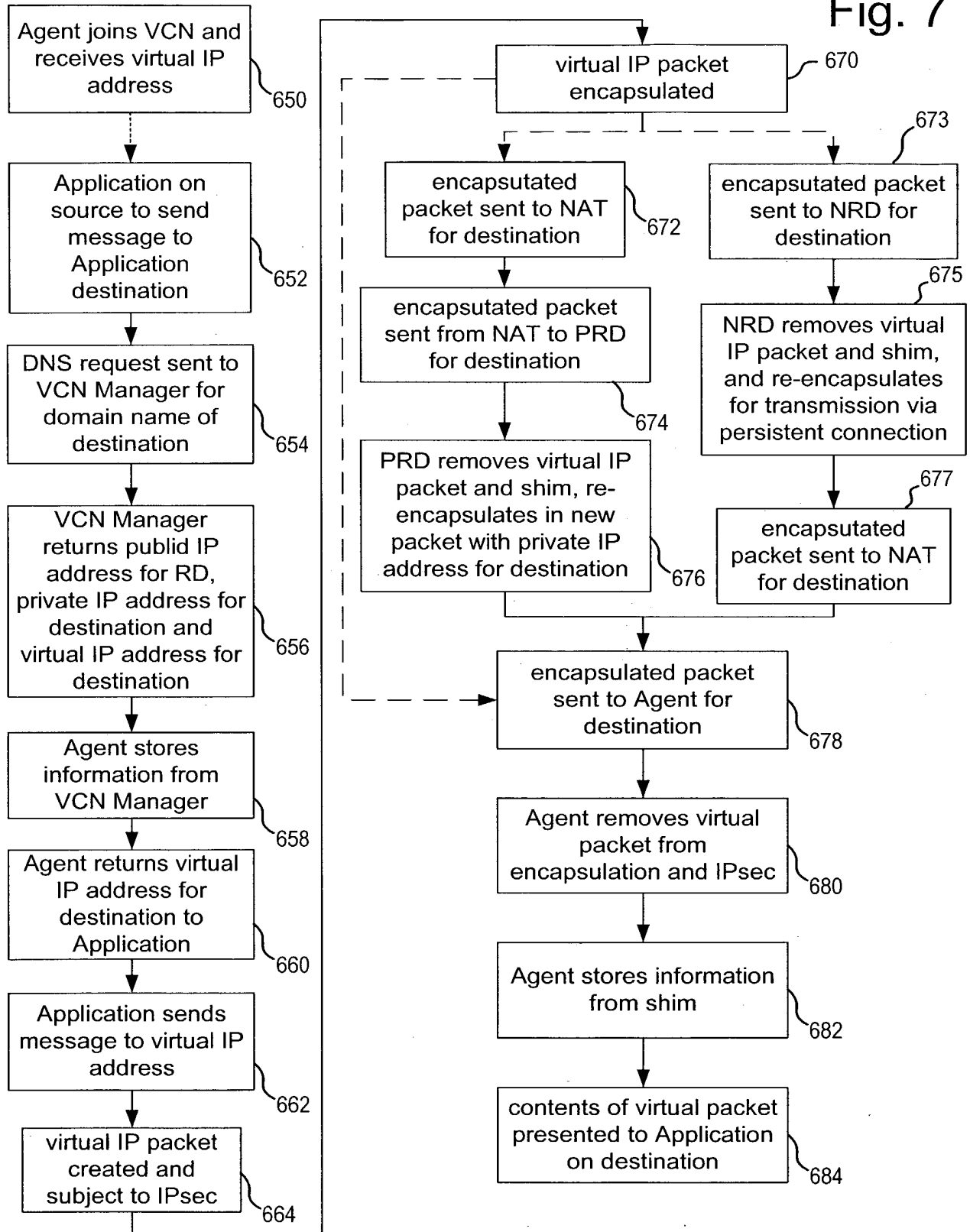
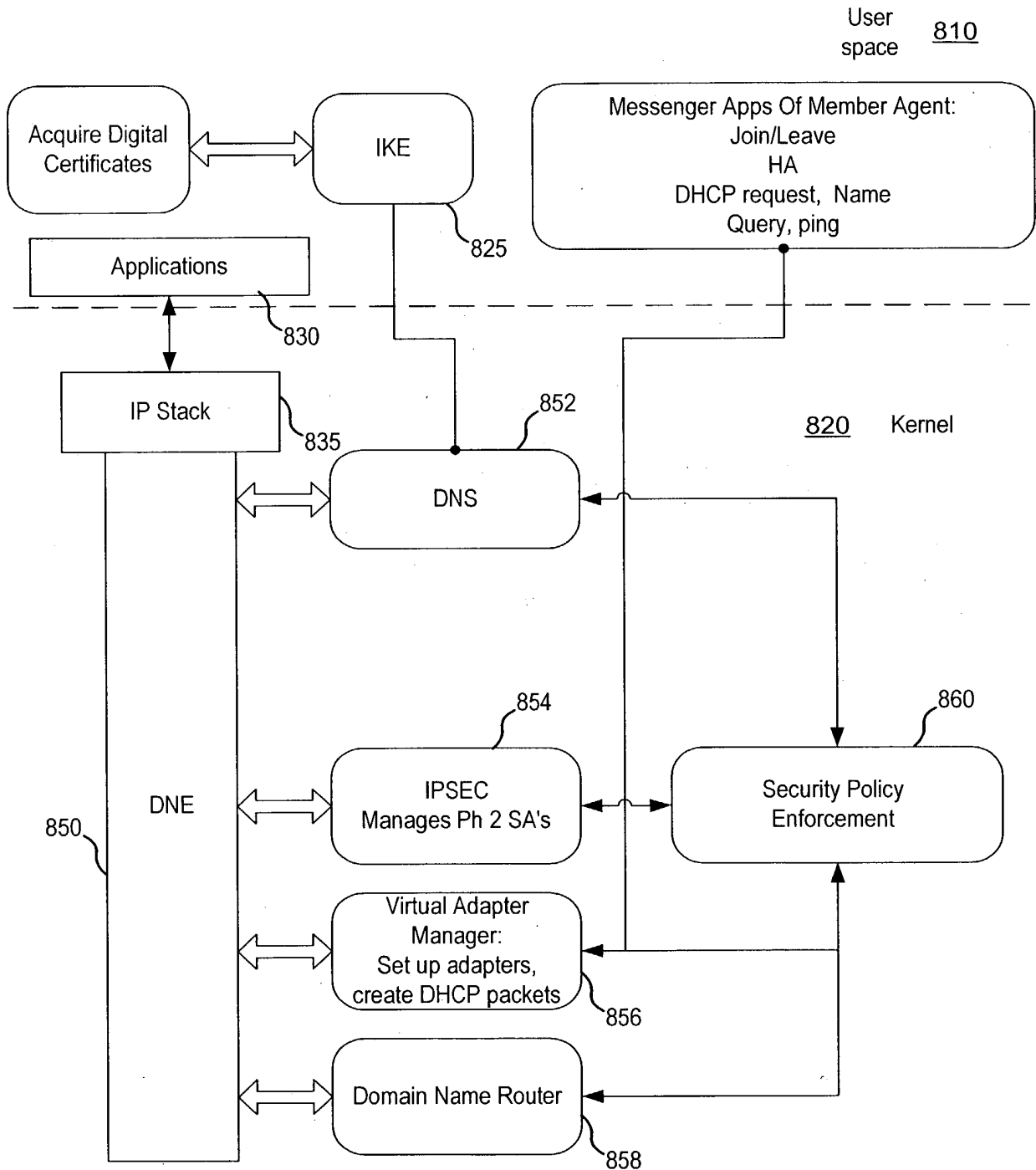


Fig. 8



Title: SECURE VIRTUAL COMMUNITY NETWORK SYSTEM
Applicant: Hasan S. Alkhatib et al.
Appl. No.: Unknown
Filing Date: March 31, 2003
Express Mail No.: EV 251 363 937 US

Docket: TTCC-01021U
Atty: Burt Magen, Esq.
Phone: (415) 369-9660

Fig. 9

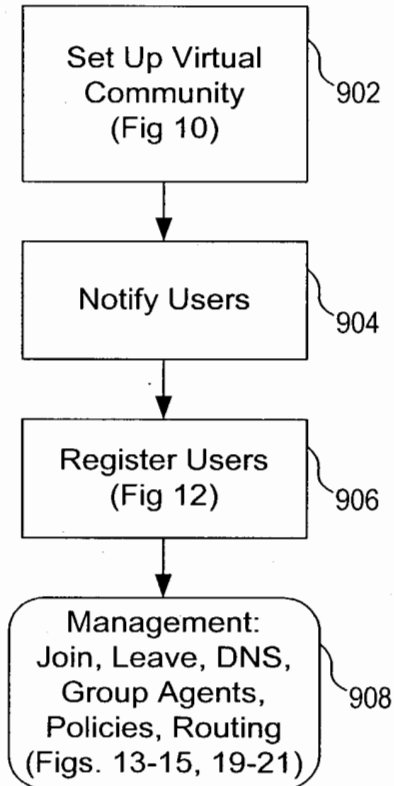


Fig. 10

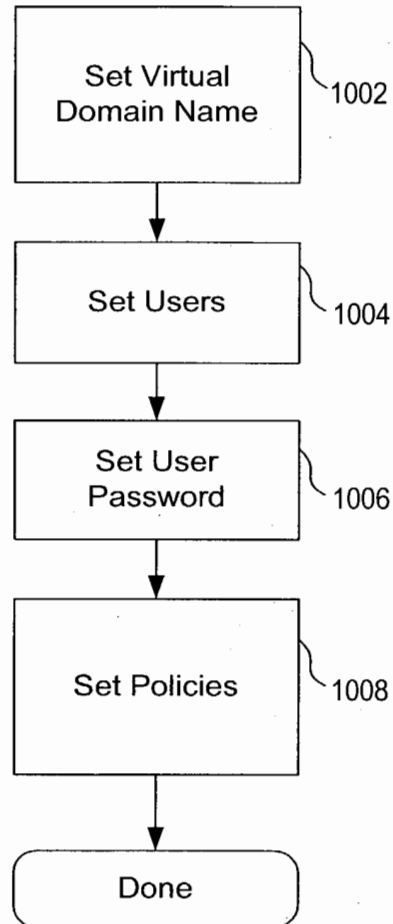


Fig. 11

<HTTP Header><XML Header><P-Length>

Fig. 12A

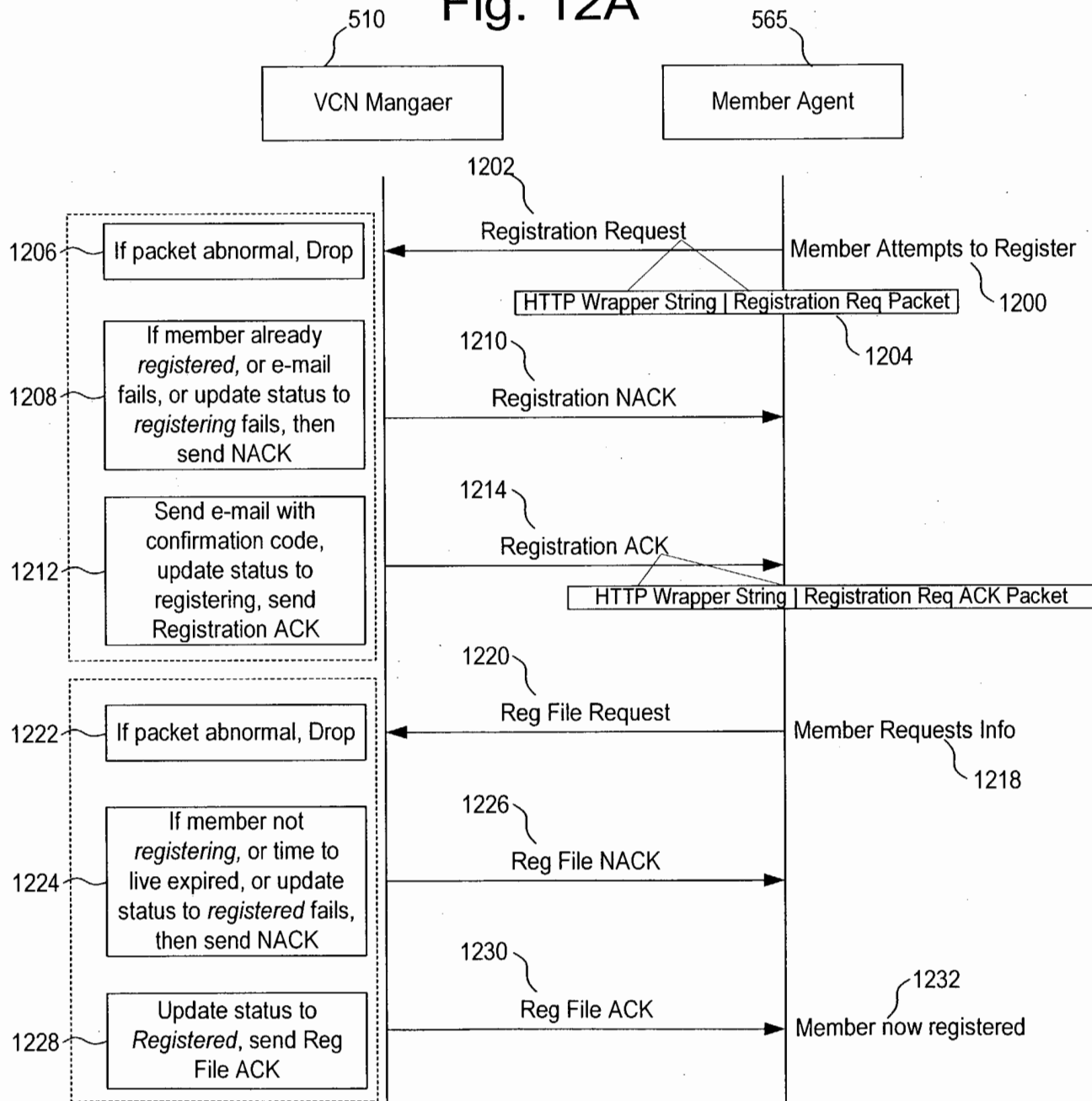


Fig. 12B

Field Name	Type	Description
Manager Seed	Array (32)	From Init Ack
Init Ack Time	Uint (8)	From Init Ack
Join Flags	Uint (2)	Indicates if rejoin and/or Group
Member Local IP	Uint (4)	The machine's local IP address
RD Local IP	Uint (4)	The Route Director local IP address
RD Global IP	Uint (4)	The Route Director Global IP
<Unused>	Uint (4)	
Member AH SPI	Uint (4)	For IPsec
Member ESP SPI	Uint (4)	For IPsec
Member Listen Port	Uint (2)	For Heartbeat Protocol
Token Timestamp	Uint (8)	The UTC time Token Key was created
Member Run ID	Array (16)	GUID Identifying current client run
Member Netbios Name	Array (16)	Microsoft NetBios support
SP Version	Uint (4)	Security Policy version
HA Version	Uint (4)	High availability version
Password Hash	Uint (20)	SHA1 of the user password string
Padding	Uint (.)	End on a multiple of 16 octets

Fig. 13

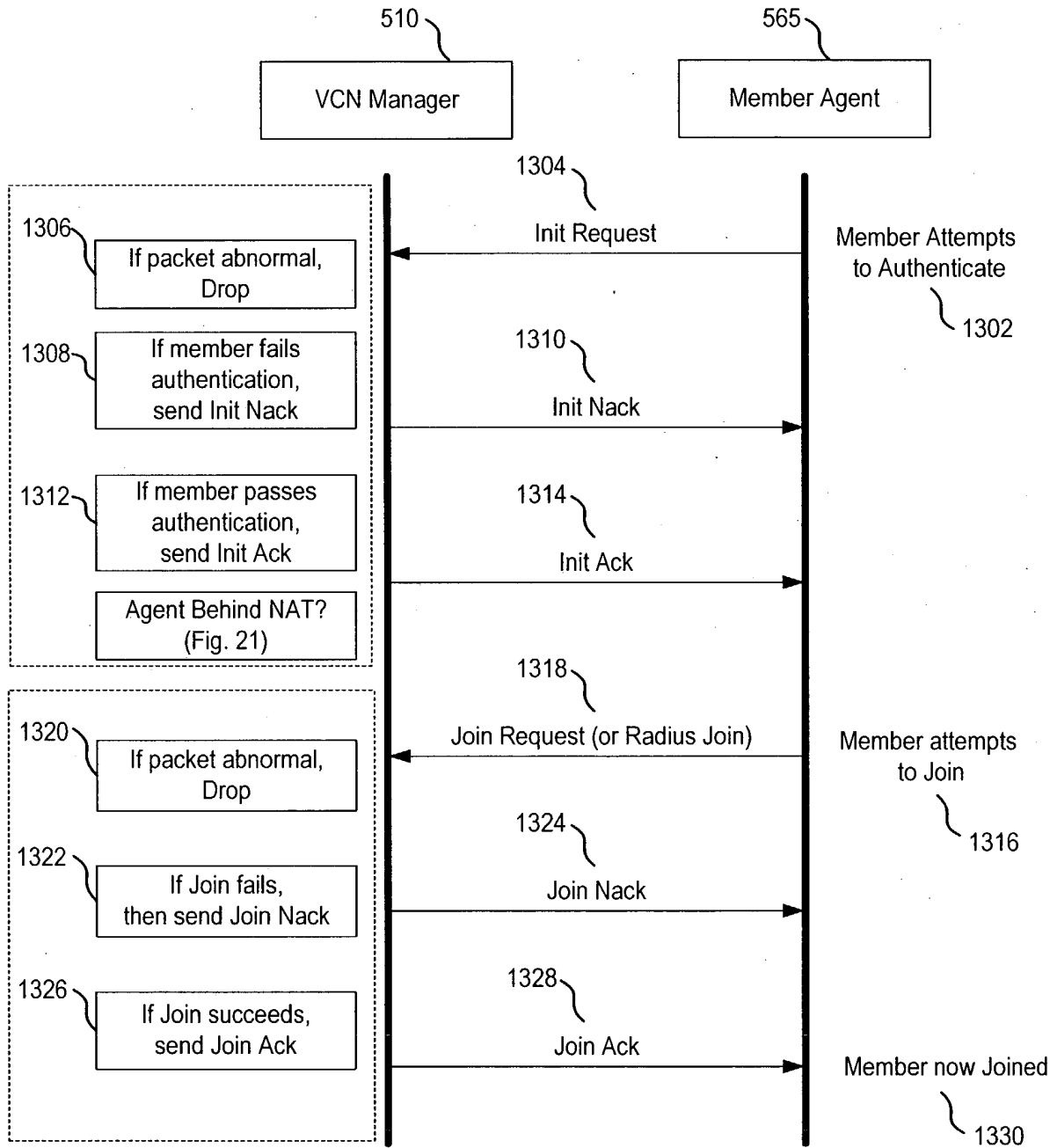


Fig. 14

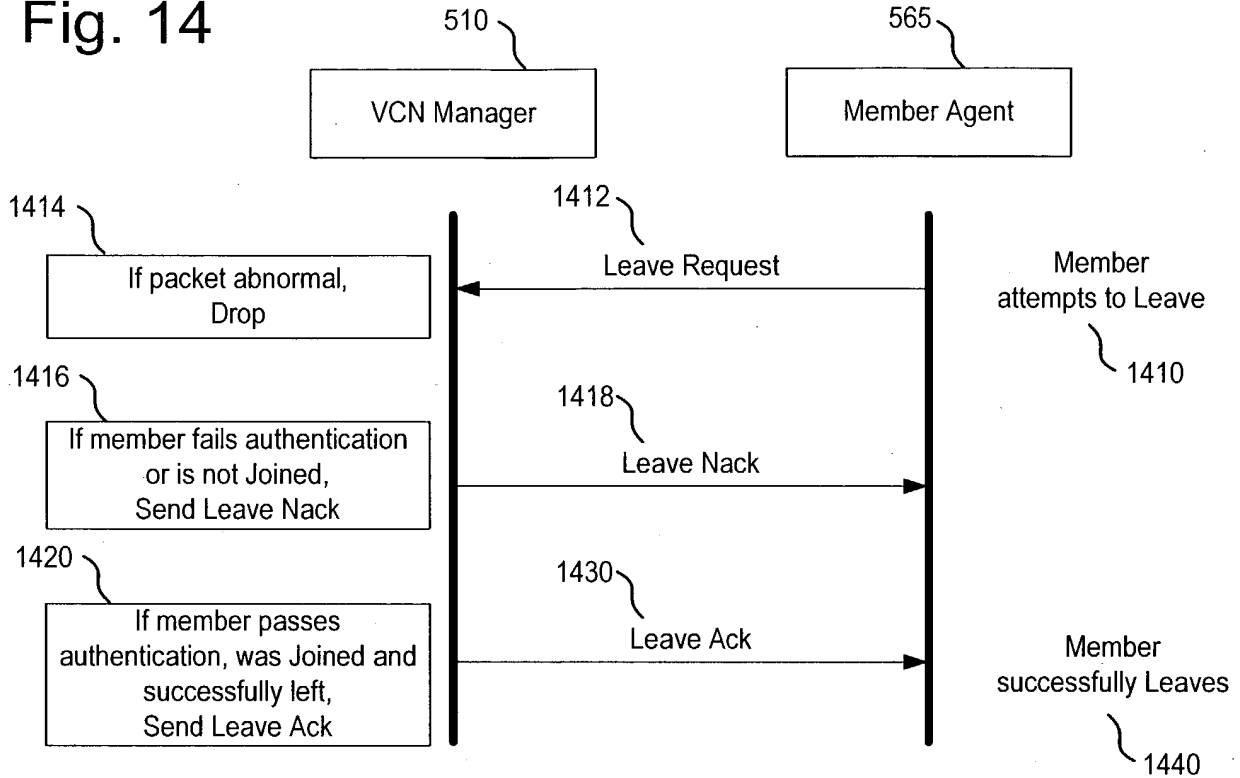


Fig. 20

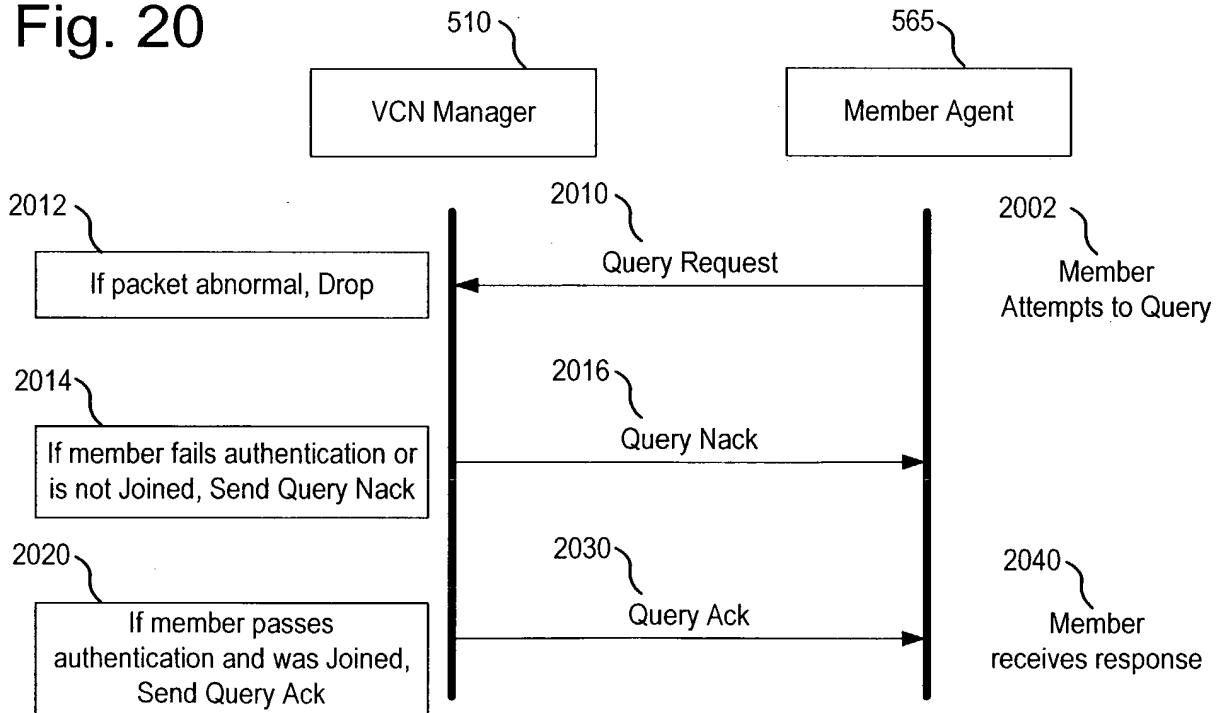


Fig. 15

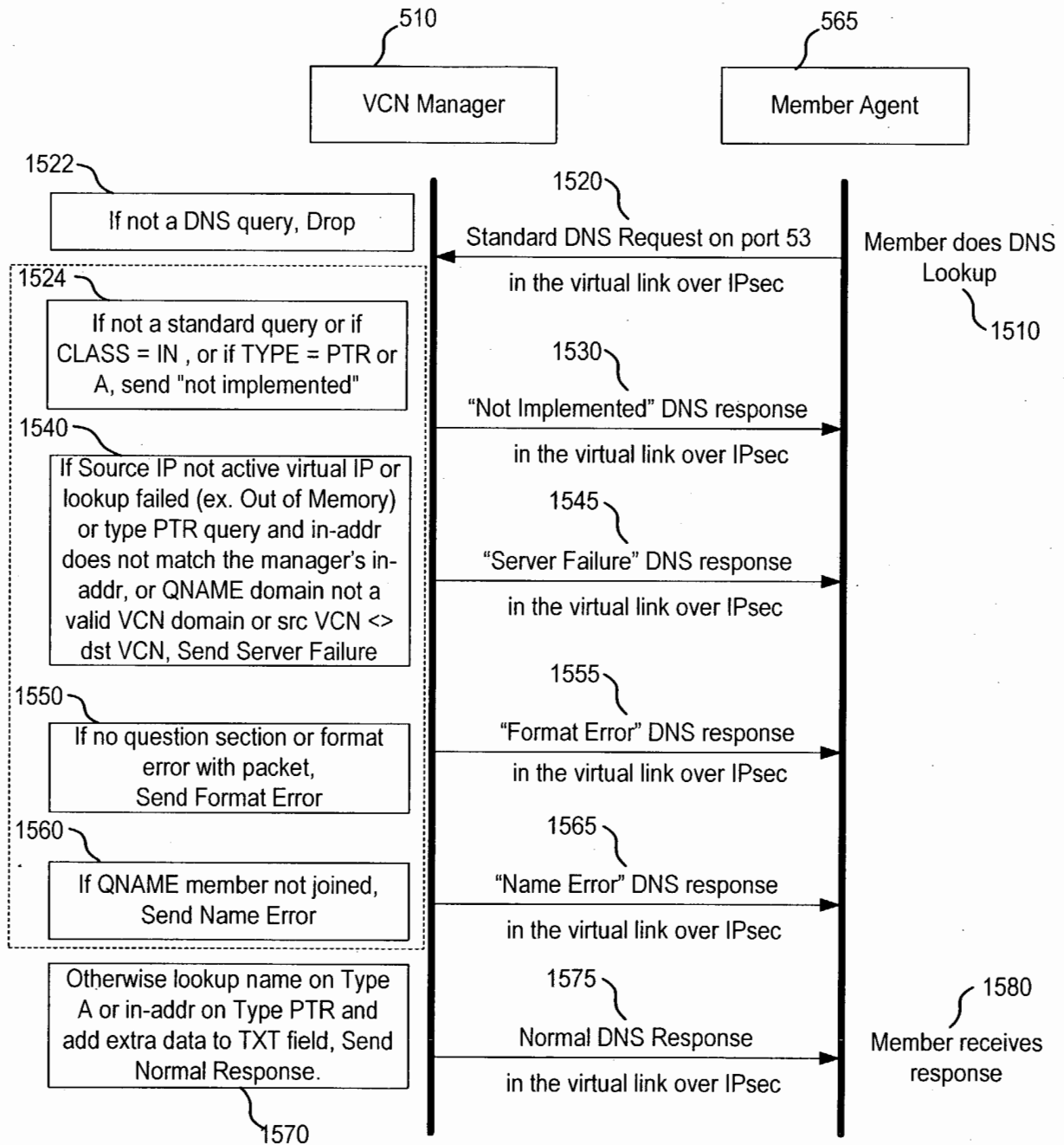


Fig. 16A

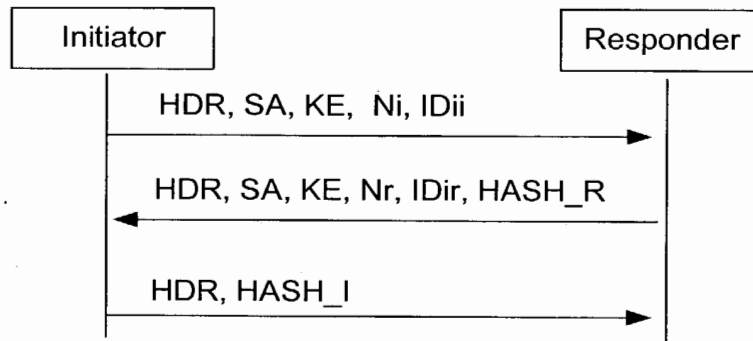


Fig. 16B

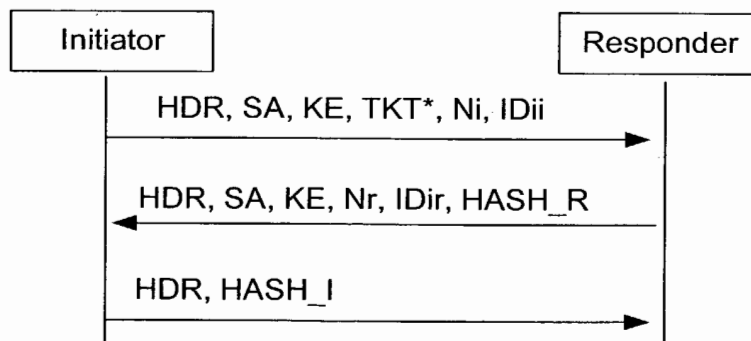


Fig. 17

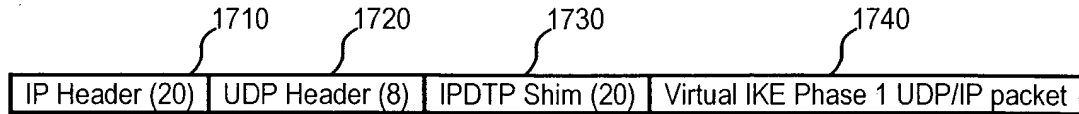


Fig. 18

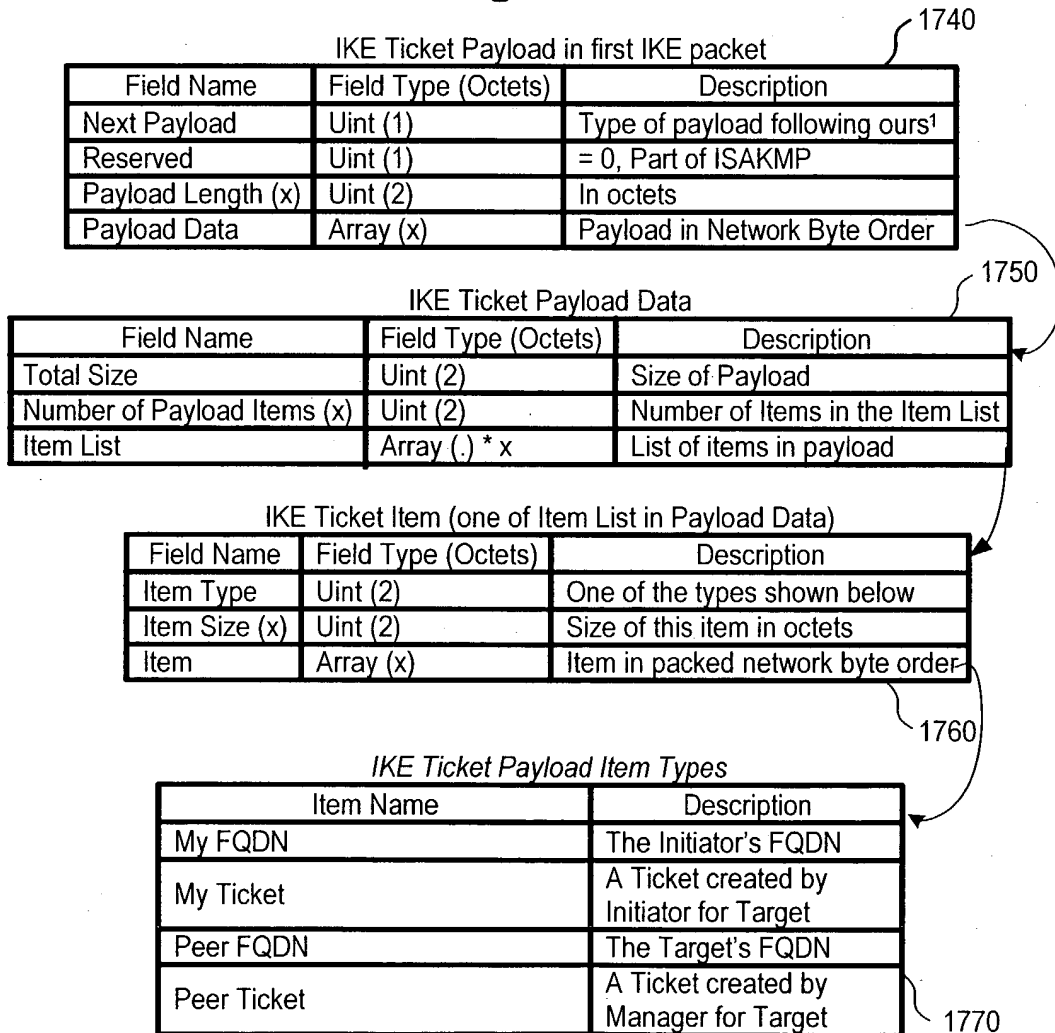


Fig. 19

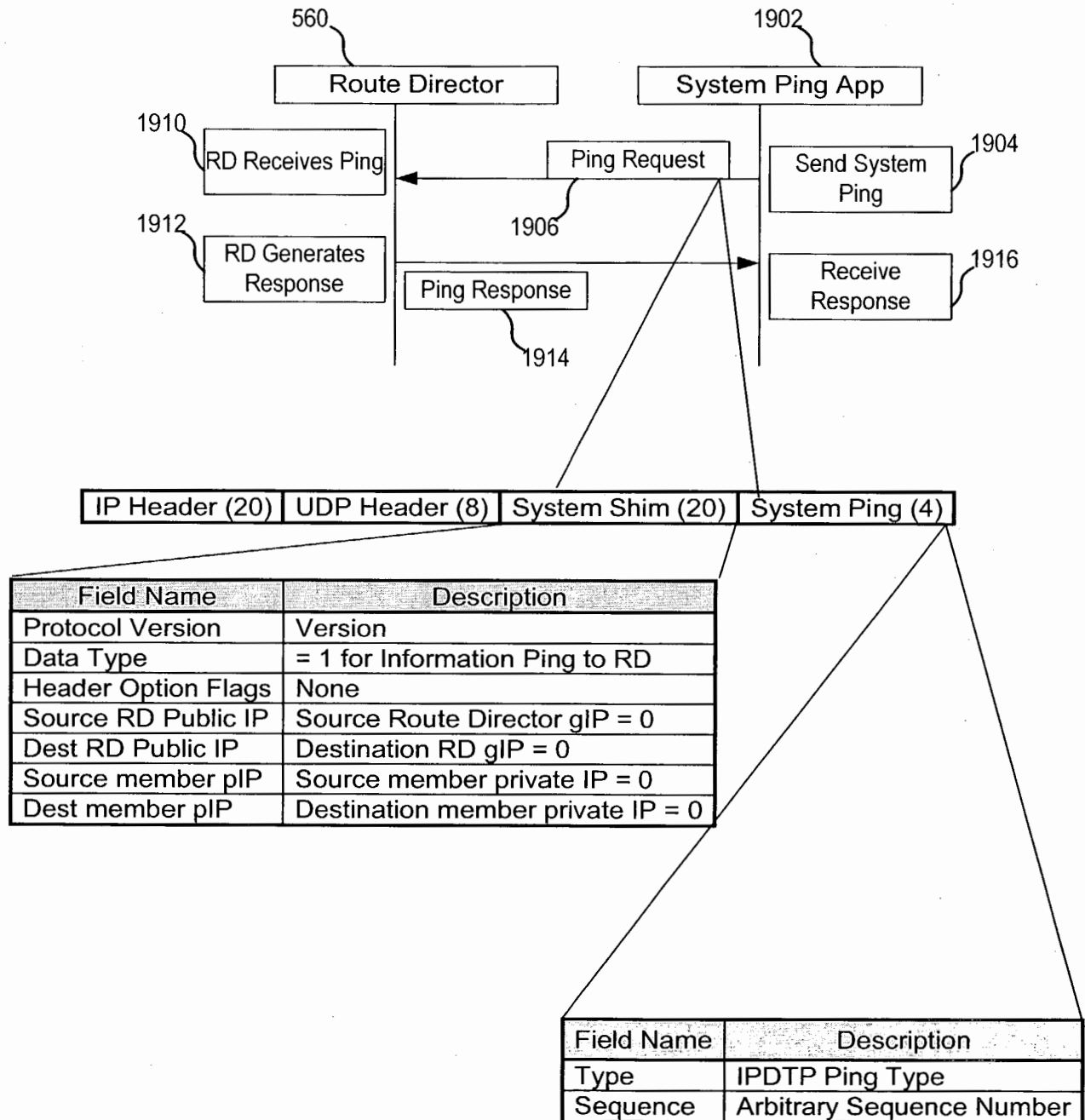


Fig. 21

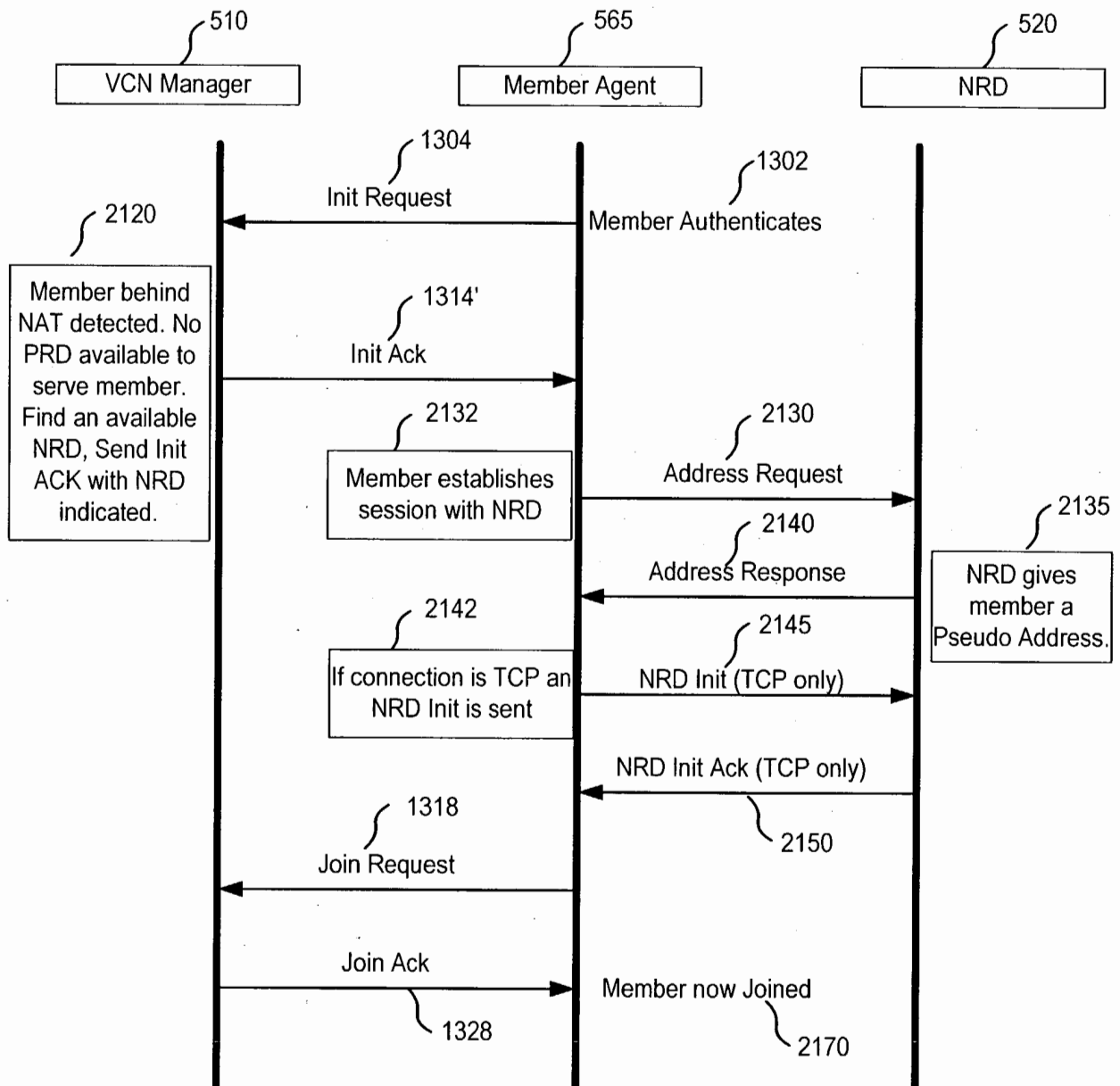


Fig. 22

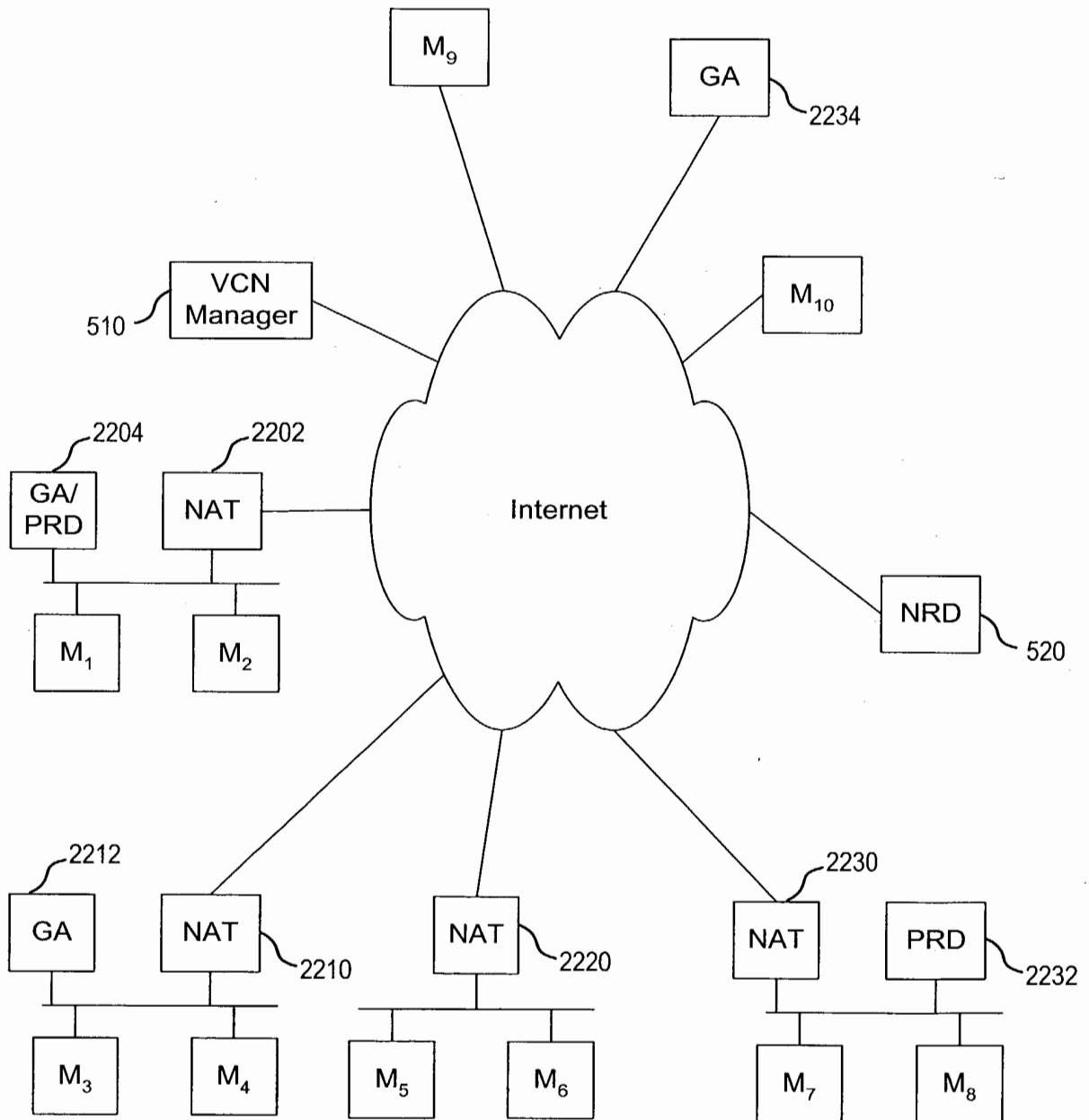


Fig. 23

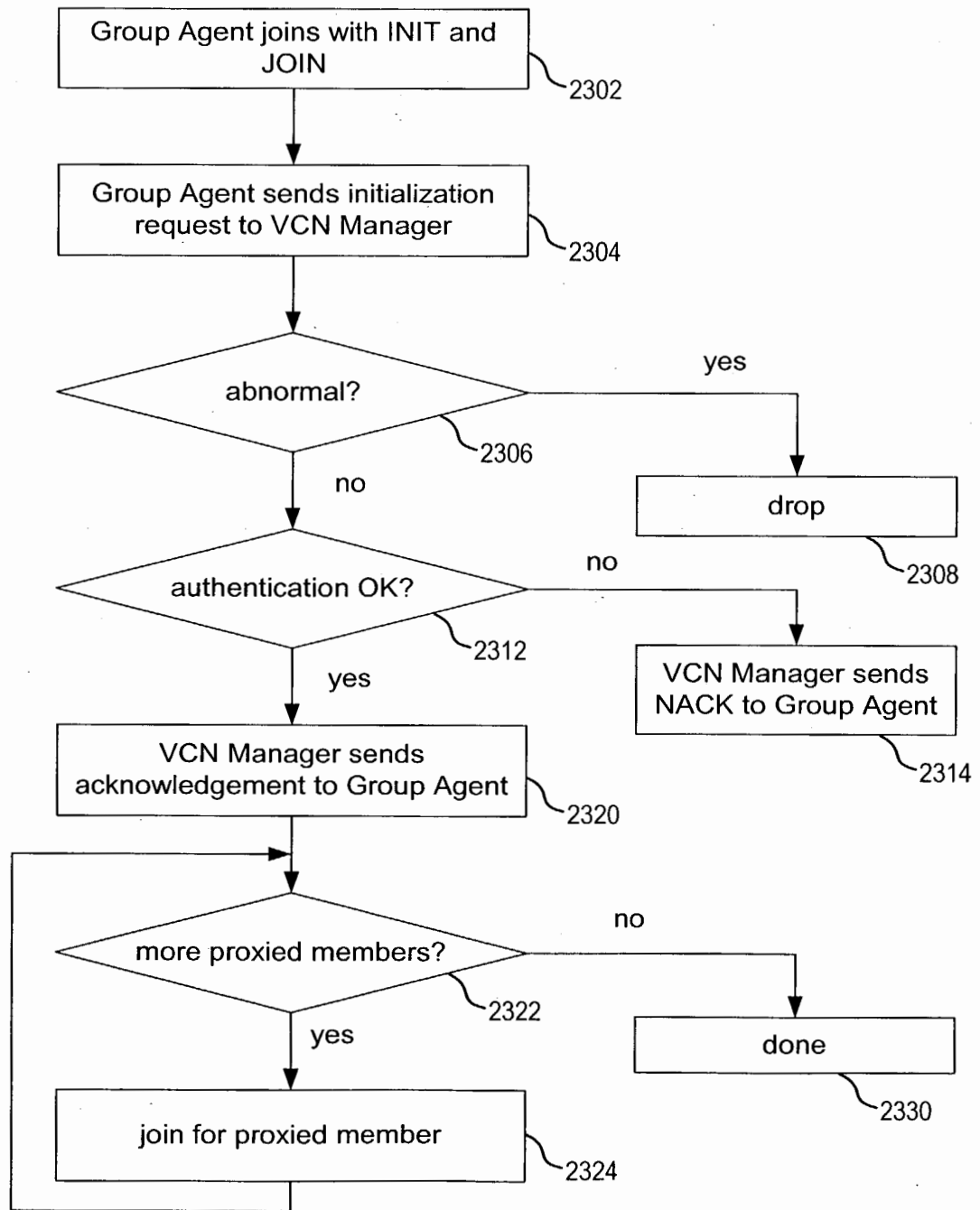


Fig. 24

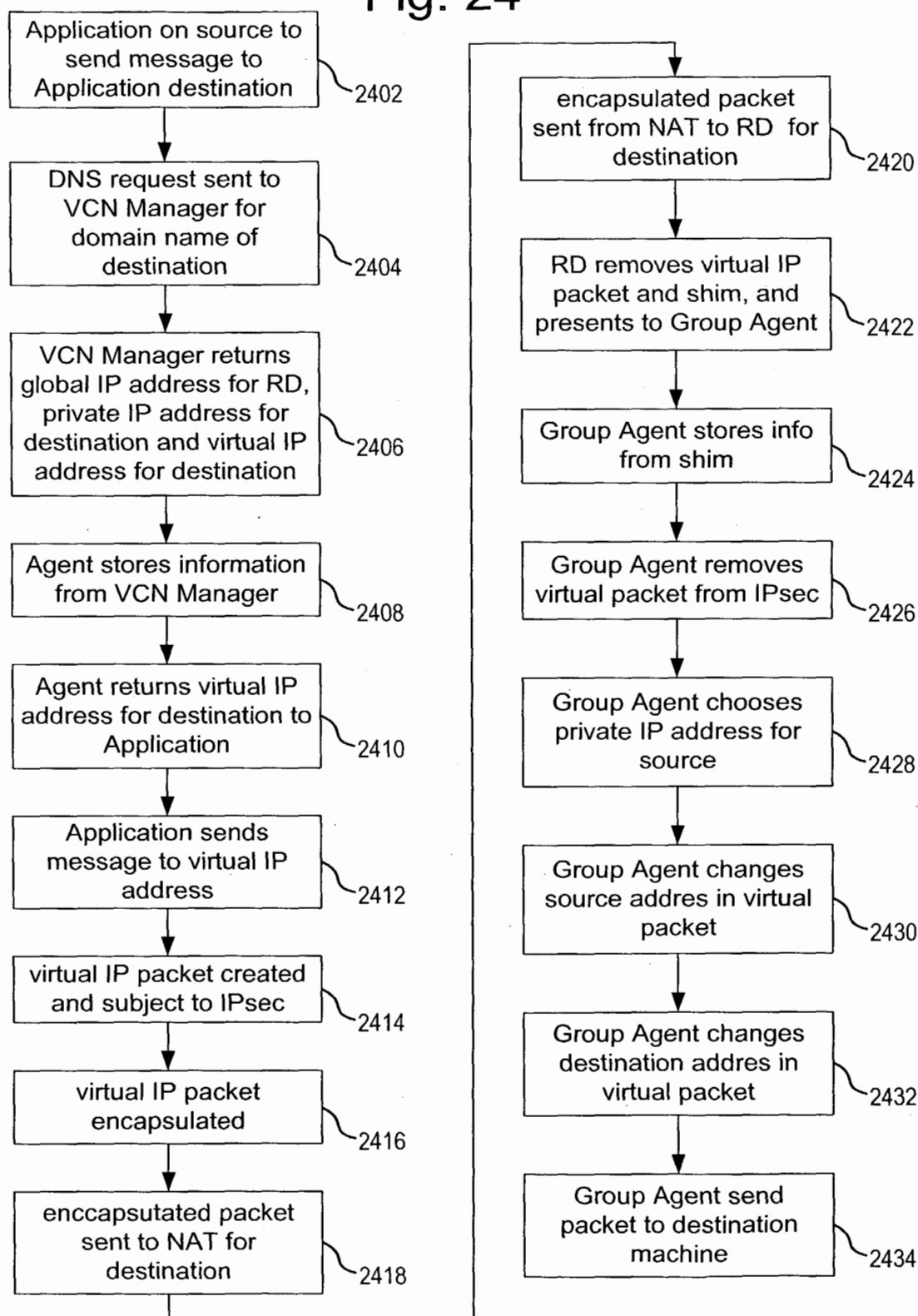


Fig. 25

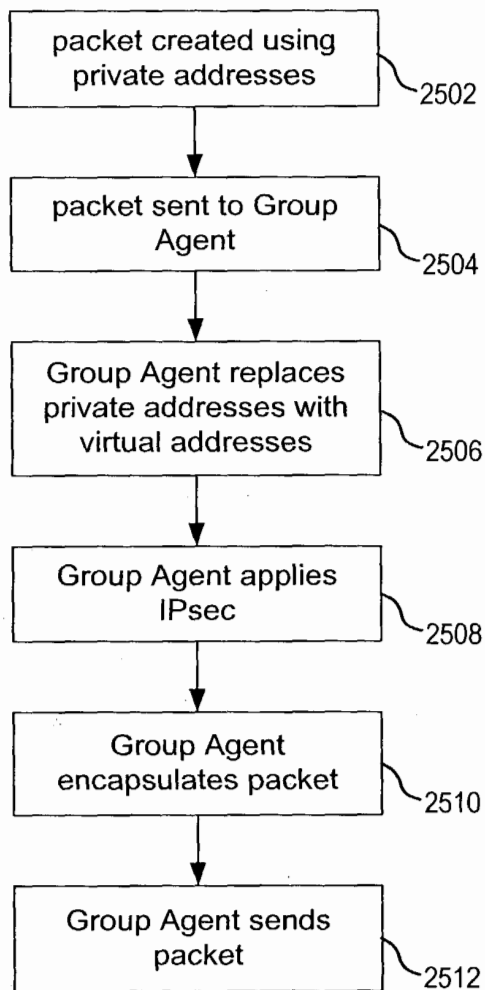
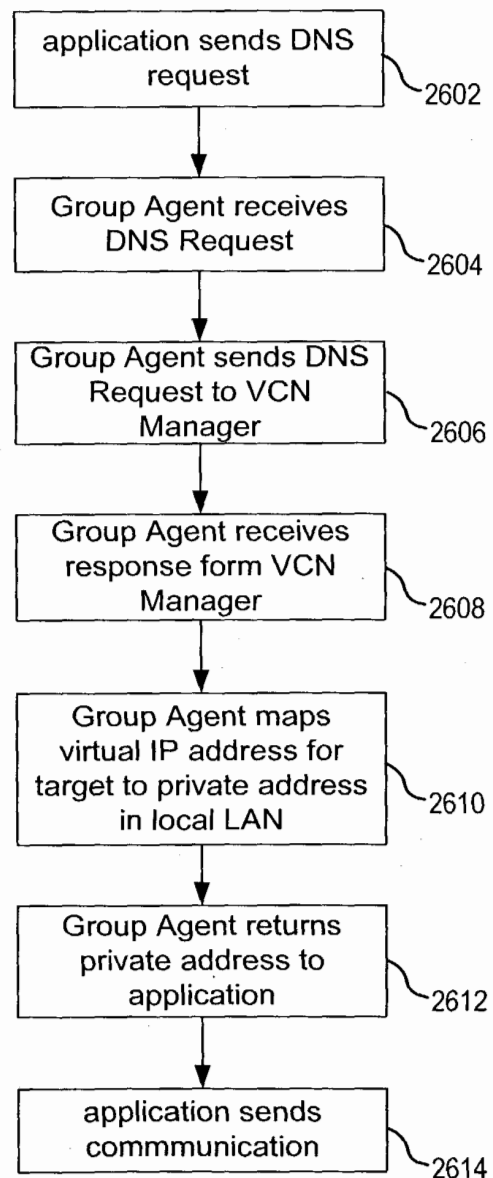


Fig. 26



PATENT APPLICATION FEE DETERMINATION RECORD

Effective January 1, 2003

Application or Docket Number

CLAIMS AS FILED - PART I

(Column 1) (Column 2)

TOTAL CLAIMS	109	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	109 minus 20 =	* 89
INDEPENDENT CLAIMS	6 minus 3 =	* 3
MULTIPLE DEPENDENT CLAIM PRESENT ☐		

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

(Column 1) (Column 2) (Column 3)

AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**
	Independent	*	Minus	***
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

1,32,53,24,20,13

(Column 1) (Column 2) (Column 3)

AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**
	Independent	*	Minus	***
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

(Column 1) (Column 2) (Column 3)

AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**
	Independent	*	Minus	***
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SMALL ENTITY TYPE

☐

OR

OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	375.00
X\$ 9=	
X42=	
+140=	
TOTAL	

RATE	FEE
BASIC FEE	750.00
X\$18=	1602
X84=	252
+280=	
TOTAL	2604

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL	

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL	

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL	



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 NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0

CONFIRMATION NO. 2698

28554
 VIERRA MAGEN MARCUS HARMON & DENIRO LLP
 685 MARKET STREET, SUITE 540
 SAN FRANCISCO, CA 94105

FORMALITIES LETTER



OC000000010381185

Date Mailed: 07/03/2003

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
Applicant must submit \$ 750 to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).
- The oath or declaration is missing.
A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.

Items Required To Avoid Processing Delays:

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- Additional claim fees of **\$1854** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

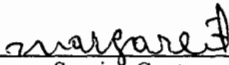
SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$2734** for a Large Entity

- **\$750** Statutory basic filing fee.

- **\$130** Late oath or declaration Surcharge.
- Total additional claim fee(s) for this application is **\$1854**
 - **\$1602** for **89** total claims over 20 .
 - **\$252** for **3** independent claims over 3 .

A copy of this notice MUST be returned with the reply.



Customer Service Center

Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY



#7

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application	)	<u>PATENT APPLICATION</u>
	)	
Inventors: Alkhatib, et al.	)	
	)	
Application No.: 10/403,818	)	
	)	
Filed: March 31, 2003	)	
	)	
Title: SECURE VIRTUAL COMMUNITY	)	
NETWORK SYSTEM	)	<u>Customer No. 28554</u>
	)	

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

the specification of which (check applicable ones):

_____ is filed herewith;

 X was filed with the above-identified "Filed" date and "Application No."

_____ was amended on (or amended through) _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to the examination of the application in accordance with Title 37, Code of Federal Regulations, §1.56.

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 were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of 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.

(1) Full name of sole
or first inventor: Hasan S. Alkhatib

(1) Residence: 15725 Apollo Heights Court
Saratoga, California 95070

(1) Post Office Address: same

(1) Citizenship: United States

(1) Inventor's signature: Hasan S. Alkhatib

(1) Date: 7/13/2003

(2) Full name of second
joint inventor: Fouad A. Tobagi

(2) Residence: 1183 Laureles Drive
Los Altos, California 94022

(2) Post Office Address: same

(2) Citizenship: United States

(2) Inventor's signature: F. Tobagi

(2) Date: 7/14/2003

(3) Full name of third
joint inventor: Farid F. Elwailly

(3) Residence: 1691 Tupolo Drive
San Jose, California 95124

(3) Post Office Address: same

(3) Citizenship: United States

(3) Inventor's signature: Farid F. Elwailly

(3) Date: 7/29/03

Title 37, Code of Federal Regulations, §1.56

**SECTION 1.56. DUTY TO DISCLOSE INFORMATION
MATERIAL TO PATENTABILITY**

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98.* However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

- (i) Opposing an argument of unpatentability relied on by the Office; or
- (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
- (2) Each attorney or agent who prepares or prosecutes the application; and
- (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

* §§1.97(b)-(d) and 1.98 relate to the timing and manner in which information is to be submitted to the Office.



1FW/2157

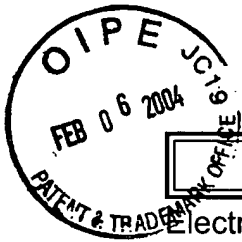
Electronic Filing System (EFS) Data
Electronic Patent Application Submission
USPTO Use Only

EFS ID: 55006
Application ID: 10403818
Title of Invention: SECURE VIRTUAL COMMUNITY
NETWORK SYSTEM
First Named Inventor: HASAN ALKHATIB
Domestic/Foreign Application: Domestic Application
Filing Date: 2004-02-06
Effective Receipt Date: 2004-02-06
Submission Type: Information Disclosure
Statement
Filing Type:
Confirmation number: 2698
Attorney Docket Number: TTCC-01021US0



Total Fees Authorized:

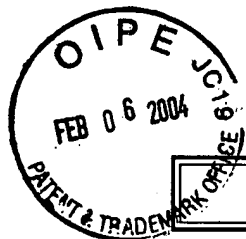
Digital Certificate Holder: cn=Burt Magen,ou=Registered Attorneys,ou=Patent and Trademark
Office,ou=Department of Commerce,o=U.S. Government,c=US
Certificate Message Digest: 70b06882d44d71aa8c86fbbd5f97d28dae130381



TRANSMITTAL

Electronic Version v1.1
Stylesheet Version v1.1.0

Title of Invention	SECURE VIRTUAL COMMUNITY NETWORK SYSTEM									
Application Number: 10/403818 										
Date: 2004-02-06										
First Named Applicant: HASAN S. ALKHATIB										
Confirmation Number: 2698										
Attorney Docket Number: TTCC-01021US0										
I hereby certify that the use of this system is for OFFICIAL correspondence between patent applicants or their representatives and the USPTO. Fraudulent or other use besides the filing of official correspondence by authorized parties is strictly prohibited, and subject to a fine and/or imprisonment under applicable law. I, the undersigned, certify that I have viewed a display of document(s) being electronically submitted to the United States Patent and Trademark Office, using either the USPTO provided style sheet or software, and that this is the document(s) I intend for initiation or further prosecution of a patent application noted in the submission. This document(s) will become part of the official electronic record at the USPTO.										
<table border="1"><thead><tr><th>Submitted by:</th><th>Elec. Sign.</th><th>Sign. Capacity</th></tr></thead><tbody><tr><td>BURT MAGEN Registered Number: 37,175</td><td>/BURT MAGEN/</td><td>Attorney</td></tr></tbody></table>			Submitted by:	Elec. Sign.	Sign. Capacity	BURT MAGEN Registered Number: 37,175	/BURT MAGEN/	Attorney		
Submitted by:	Elec. Sign.	Sign. Capacity								
BURT MAGEN Registered Number: 37,175	/BURT MAGEN/	Attorney								
<table><tr><td>Documents being submitted</td><td>Files</td></tr><tr><td>us-ids</td><td>1021.ids-001-usidst.xml</td></tr><tr><td></td><td>us-ids.dtd</td></tr><tr><td></td><td>us-ids.xsl</td></tr></table>			Documents being submitted	Files	us-ids	1021.ids-001-usidst.xml		us-ids.dtd		us-ids.xsl
Documents being submitted	Files									
us-ids	1021.ids-001-usidst.xml									
	us-ids.dtd									
	us-ids.xsl									
Comments										



ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	SECURE VIRTUAL COMMUNITY NETWORK SYSTEM																																																																																																																													
Application Number: 10/403818  Confirmation Number: 2698 First Named Applicant: HASAN ALKHATIB Attorney Docket Number: TTCC-01021US0 Art Unit: 2157 Search string: (5361256 or 5623605 or 5717687 or 5751961 or 5777989 or 5781550 or 5790548 or 5805818 or 5805820 or 5856974 or 5867667 or 5884246 or 5889953 or 5913210 or 5937162 or 5937163 or 6003084 or 6055575 or 5793763 or 6119171 or 6061738 or 6047325 or 6032196 or 5815664 or 5764906 or 6006272 or 6557037 or 6591306 or 5734651 or 5701427 or 5563878).pn. US Patent Documents Note: Applicant is not required to submit a paper copy of cited US Patent Documents <table border="1"><thead><tr><th>init</th><th>Cite.No.</th><th>Patent No.</th><th>Date</th><th>Patentee</th><th>Kind</th><th>Class</th><th>Subclass</th></tr></thead><tbody><tr><td></td><td>1</td><td>5361256</td><td>1994-11-01</td><td>Doeringer</td><td></td><td></td><td></td></tr><tr><td></td><td>2</td><td>5623605</td><td>1997-04-22</td><td>Keshav</td><td></td><td></td><td></td></tr><tr><td></td><td>3</td><td>5717687</td><td>1998-02-10</td><td>Minot</td><td></td><td></td><td></td></tr><tr><td></td><td>4</td><td>5751961</td><td>1998-05-12</td><td>Smyk</td><td></td><td></td><td></td></tr><tr><td></td><td>5</td><td>5777989</td><td>1998-07-07</td><td>McGarvey</td><td></td><td></td><td></td></tr><tr><td></td><td>6</td><td>5781550</td><td>1998-07-14</td><td>Templin</td><td></td><td></td><td></td></tr><tr><td></td><td>7</td><td>5790548</td><td>1998-08-04</td><td>Sistainizadeh</td><td></td><td></td><td></td></tr><tr><td></td><td>8</td><td>5805818</td><td>1998-09-08</td><td>Perlman</td><td></td><td></td><td></td></tr><tr><td></td><td>9</td><td>5805820</td><td>1998-09-08</td><td>Bellovin</td><td></td><td></td><td></td></tr><tr><td></td><td>10</td><td>5856974</td><td>1999-01-05</td><td>Gervais</td><td></td><td></td><td></td></tr><tr><td></td><td>11</td><td>5867667</td><td>1999-02-02</td><td>Butman</td><td></td><td></td><td></td></tr><tr><td></td><td>12</td><td>5884246</td><td>1999-03-16</td><td>Boucher</td><td></td><td></td><td></td></tr><tr><td></td><td>13</td><td>5889953</td><td>1999-03-30</td><td>Thebaut</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>							init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass		1	5361256	1994-11-01	Doeringer					2	5623605	1997-04-22	Keshav					3	5717687	1998-02-10	Minot					4	5751961	1998-05-12	Smyk					5	5777989	1998-07-07	McGarvey					6	5781550	1998-07-14	Templin					7	5790548	1998-08-04	Sistainizadeh					8	5805818	1998-09-08	Perlman					9	5805820	1998-09-08	Bellovin					10	5856974	1999-01-05	Gervais					11	5867667	1999-02-02	Butman					12	5884246	1999-03-16	Boucher					13	5889953	1999-03-30	Thebaut											
init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass																																																																																																																							
	1	5361256	1994-11-01	Doeringer																																																																																																																										
	2	5623605	1997-04-22	Keshav																																																																																																																										
	3	5717687	1998-02-10	Minot																																																																																																																										
	4	5751961	1998-05-12	Smyk																																																																																																																										
	5	5777989	1998-07-07	McGarvey																																																																																																																										
	6	5781550	1998-07-14	Templin																																																																																																																										
	7	5790548	1998-08-04	Sistainizadeh																																																																																																																										
	8	5805818	1998-09-08	Perlman																																																																																																																										
	9	5805820	1998-09-08	Bellovin																																																																																																																										
	10	5856974	1999-01-05	Gervais																																																																																																																										
	11	5867667	1999-02-02	Butman																																																																																																																										
	12	5884246	1999-03-16	Boucher																																																																																																																										
	13	5889953	1999-03-30	Thebaut																																																																																																																										

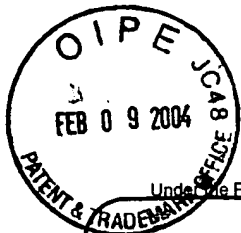
APP_ID=10403818

page 1 of 2

	14	5913210	1999-06-15	Call
	15	5937162	1999-04-10	Funk
	16	5937163	1999-04-10	Lee
	17	6003084	1999-12-14	Green
	18	6055575	2000-04-25	Paulsen
	19	5793763	1998-08-11	Mayes
	20	6119171	2000-09-12	Alkhatib
	21	6061738	2000-05-09	Osaku
	22	6047325	2000-04-04	Jain
	23	6032196	2000-02-29	Monier
	24	5815664	1998-09-29	Asano
	25	5764906	1998-06-09	Edelstein.
	26	6006272	1999-12-21	Aravamudan
	27	6557037	2003-04-29	Provino
	28	6591306	2003-07-08	Redlich
	29	5734651	1998-03-31	Blakeley
	30	5701427	1997-12-23	Lathrop
	31	5563878	1996-10-08	Blakeley

Signature

Examiner Name	Date



2157

PTO/SB/21 (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

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

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

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	10/403,818
Filing Date	March 31, 2003
First Named Inventor	Alkhatib
Art Unit	2157
Examiner Name	
Attorney Docket Number	TTCC-01021US0

ENCLOSURES (Check all that apply)

- | | | |
|--|---|--|
| ☐ Fee Transmittal Form | ☐ Drawing(s) | ☐ After Allowance communication to Group |
| ☐ Fee Attached | ☐ Licensing-related Papers | ☐ Appeal Communication to Board of Appeals and Interferences |
| ☐ Amendment/Reply | ☐ Petition | ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) |
| ☐ After Final | ☐ Petition to Convert to a Provisional Application | ☐ Proprietary Information |
| ☐ Affidavits/declaration(s) | ☐ Power of Attorney, Revocation | ☐ Status Letter |
| ☐ Extension of Time Request | ☐ Change of Correspondence Address | ☒ Other Enclosure(s) (please identify below): |
| ☐ Express Abandonment Request | ☐ Terminal Disclaimer | 10 references for IDS |
| ☒ Information Disclosure Statement | ☐ Request for Refund | |
| ☐ Certified Copy of Priority Document(s) | ☐ CD, Number of CD(s) _____ | |
| ☐ Response to Missing Parts/Incomplete Application | Remarks | |
| ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53 | | |

RECEIVED

FEB 12 2004

Technology Center 2100

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Burt Magen, Vierra Magen Marcus Harmon & DeNiro LLR
Signature	
Date	FEB 6, 2004

CERTIFICATE OF TRANSMISSION/MAILING

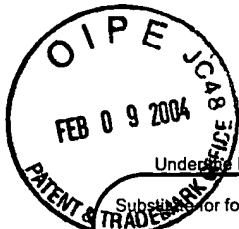
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Burt Magen, Reg. No. 37,175
-----------------------	-----------------------------

Signature		Date	FEB 6, 2004
-----------	--	------	-------------

This collection of information is required by 37 CFR 1.5. 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



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

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number 10/403,818

Filing Date March 31, 2003

First Named Inventor Alkhatib

Art Unit 2157

Examiner Name

Attorney Docket Number TTCC-01021US0

RECEIVED

FEB 12 2004

Technology Center 2100

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		VENTERS, Demystifying Protocols: A comparison of Protocols Suitable for IP Telephony, Sonus Networks, pp. 1-11, 2000.	
		TSUCHIYA, ET AL., Extending the IP Internet Through Address Reuse, ACM SIGCOMM Computer Communication Review, pp. 16-33, JANUARY 1993.	
		FRANCIS, ET AL., IPNL: A NAT-Extended Internet Architecture, SIGCOMM'01, 8/27-31, 2001, pp. 69-79.	
		YALAGANDULA, ET AL., Transparent Mobility with Minimal Infrastructure, University of Texas at Austin, pp. 1-14, JULY 2001.	
		TERAOKA, ET AL., VIP: A Protocol Providing Host Mobility, Communications of the ACM, August 1994/Vol. 37, No. 8, pp. 67-75, 113.	
		EDEVANG, ET AL., The IP Network Address Translator (NAT), Network Working Group, RFC 1631, May 1994, pp. 1-10.	
		CHATEL, Classical Versus Transparent IP Proxies, Network Working Group, RFC 1919, March 1996, pp. 1-35.	
		FINSETH, An Access Control Protocol, Sometimes Called TACACS, Network Working Group, July 1993, pp. 1-18.	
		Computer Networks, Third Edition, by Andrew S. Tanenbaum, 1996, pp. 643-670, 685-691.	
		PERKINS, Mobile IP, IEEE Communications Magazine, May 1997, pp. 84-99	

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 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

*1 = COPY NOT SUBMITTED BECAUSE IT WAS SUBMITTED IN PRIOR APPLICATION NO. 09/492,565, filed 1/27/2000, which is a continuation of Application No. 09/015,840, filed 1/29/1998.

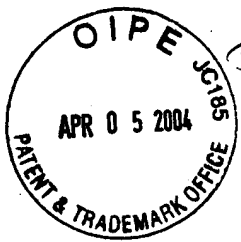


Image
2157

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application	)	<u>PATENT APPLICATION</u>
Inventors:	)	
Alkhatib, et al.	)	
Application No.:	)	
10/403,818	)	
Filed Date:	)	
March 31, 2003	)	
Title:	)	
SECURE VIRTUAL COMMUNITY	)	
NETWORK SYSTEM	)	Customer No.: 28554

POWER OF ATTORNEY

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

Sir:

I hereby revoke all previous powers of attorney or authorizations of agents given in the above-identified application.

I hereby appoint CROMER, David E. (Reg. No. 54,768), DeNIRO, Kirk J. (Reg. No. 35,854), MAGEN, Burt (Reg. No. 37,175), MARCUS, Brian J. (Reg. No. 34,511), and VIERRA, Larry E. (Reg. No. 33,809), as our attorneys or agents to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please recognize or change the correspondence address for the above-identified application to the address associated with **Customer Number 28554**.

Please direct any telephone calls to Burt Magen at (415) 369-9660.

IP Dynamics, Inc. is the assignee of the entire right, title and interest in the above-identified patent application. I, the undersigned, declare that I have reviewed copies of the documentary evidence establishing chain of title to the patent application identified above from the inventors to the assignee which was recorded at Reel 014340, Frames 0968-0972.

The undersigned is authorized to sign this document on behalf of the assignee.

Signature: Hasan S. Alkhatib
Date: 3/23/2004
Name: Hasan S. Alkhatib
Title: Chief Executive Officer

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.power



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
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0

28554
 VIERRA MAGEN MARCUS HARMON & DENIRO LLP
 685 MARKET STREET, SUITE 540
 SAN FRANCISCO, CA 94105

CONFIRMATION NO. 2698

OC000000012589397

OC000000012589397

Date Mailed: 05/11/2004

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/05/2004.

- 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).

SUSAN K FORD
 2100 (703) 308-9045

OFFICE COPY

BEST AVAILABLE 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
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0

28554
 VIERRA MAGEN MARCUS HARMON & DENIRO LLP
 685 MARKET STREET, SUITE 540
 SAN FRANCISCO, CA 94105

CONFIRMATION NO. 2698
 OC000000012589438
 OC000000012589438

Date Mailed: 05/11/2004

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

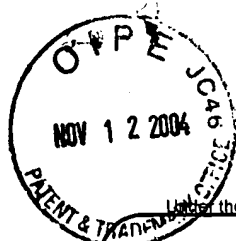
This is in response to the Power of Attorney filed 04/05/2004.

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.

SUSAN K FORD
 2100 (703) 308-9045

OFFICE COPY

BEST AVAILABLE COPY

2157
Jh

PTO/SB/21 (04-04)

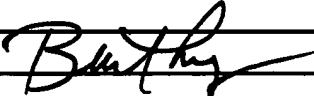
Approved for use through 07/31/2006. OMB 0651-0031

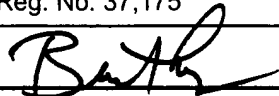
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	10/403,818
	Filing Date	March 31, 2003
	First Named Inventor	Alkhatib
	Art Unit	2157
	Examiner Name	
Total Number of Pages in This Submission	Attorney Docket Number	TTCC-01021US0

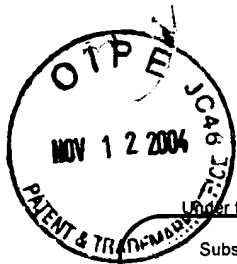
ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☐ Amendment/Reply ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☒ Information Disclosure Statement ☐ Certified Copy of Priority Document(s) ☐ Response to Missing Parts/Incomplete Application ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Attorney, Revocation ☐ Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____	☐ After Allowance communication to Technology Center (TC) ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☒ Other Enclosure(s) (please identify below): 1 REFERENCE FOR IDS
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Burt Magen, Vierra Magen Marcus Harmon & DeNiro LLP
Signature	
Date	11/9/04

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.			
Typed or printed name	Burt Magen, Reg. No. 37,175		
Signature		Date	11/9/04

This collection of information is required by 37 CFR 1.5. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



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

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known

Application Number	10/403,818
Filing Date	March 31, 2003
First Named Inventor	Alkhatib
Art Unit	2157
Examiner Name	
Attorney Docket Number	TTCC-01021US0

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

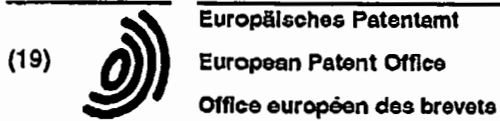
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)				
		EP 0 817 444 A2	01/07/1998	Sun Microsystems, Inc.		

Examiner
SignatureDate
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.uspto.gov or MPEP 901.04. 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.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



(11) **EP 0 817 444 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
07.01.1998 Bulletin 1998/02

(51) Int Cl.⁶: **H04L 29/06**

(21) Application number: **97304597.2**

(22) Date of filing: **30.06.1997**

(84) Designated Contracting States:
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
 NL PT SE**

(72) Inventor: **Ebrahim, Zahir**
Mountain View, California 94043 (US)

(30) Priority: **01.07.1996 US 674561**

(74) Representative: **Turner, James Arthur et al**
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

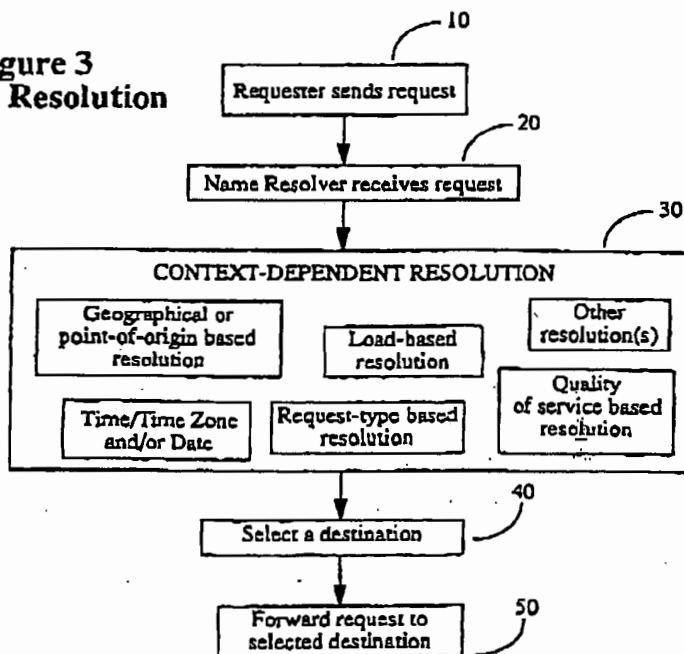
(71) Applicant: **SUN MICROSYSTEMS, INC.**
Mountain View, California 94043-1100 (US)

(54) **System for context-dependent name resolution**

(57) A context-dependent, multiply binding name resolution system. A name resolver is provided, connected to either a requester's system or a receiver's system, or both. Requests to a given service or domain name are resolved to the appropriate IP address. The intended recipient of the request is resolved based upon a combination of one or more predetermined criteria, including: information about the sender (e.g. geographical

location, specific requester identity, etc.); information about the intended recipient (e.g. load balance at the receiver, type of service, etc.); information contained within the request itself (e.g. type of service requested); or other information (time of day, date, random selection of recipient, e.g.). The system is implemented in hardware and/or software, and the resolution criteria can be made interdependent or independent.

Figure 3
Service Resolution



Description

This invention relates to systems for context-dependent name resolution.

In a network (either Intranet or Internet) system, when a host wants to communicate with another host or locate a service or another host on the network, the address is typically resolved in an absolute manner; that is, the naming service of the network resolves a given name to a single IP (Internet Protocol) address. For instance, a domain name service (DNS) call resolves a name to a single IP address or host name on the Internet.

When there are many connections to a given host or service, the resulting congestion degrades the overall performance. The service provider may upgrade the service, e.g. to increase its capacity. In this case, in order to keep the modification of the service transparent to requesting hosts, a demultiplexer may be used, as illustrated by way of example in Figures 1-2. For instance, in Figure 1 a call to Service 3 will be uniquely resolved to that service's IP address and transmitted there accordingly, because there is only a single binding in the DNS name resolver to the host of Service 3. In general, in a conventional system such as that illustrated in Figures 1, 2 and 2A, there will be a single binding between a name and an IP address.

Yet another alternative is for a special type of demultiplexer, which may monitor the traffic, and from the different IP addresses can collect statistics such as response time and/or the load on the corresponding IP hosts, and use this information for load balancing by binding a requested name to an IP address for a host which is less heavily loaded.

If Service 3 is upgraded to include Services 3.1 through 3.Y, then the demultiplexer is added (see Figure 2); the requesting or DNS resolving host resolves the request as usual and sends it out over the (Inter- or Intra-)network, but the demultiplexer is interposed between the network and the service(s), to route the incoming requests to one of the services. Note that in this case, there is still a single binding between the DNS and the demultiplexer.

A problem with this approach is that the demultiplexer acts as a limiting factor on throughput, and additionally represents a single source of failure for all of the services that it serves. A mechanism is needed whereby such a critical point and bottleneck can be avoided, while still providing access to the services for remote users.

An alternative approach to decreasing congestion is through DNS spoofing, where the name resolver is fooled into giving out a different name binding, by keeping the name resolver updated frequently with a new name resolution binding based on some criteria such as load distribution on target servers. An example of DNS spoofing is shown in Figure 2A, in which a requester 2 issues a request using the name "sun.com", and a DNS

lookup 4 looks it up. The host (1, 2 or 3) to which the names is bound will depend upon criteria employed at the destination domain, as determined by DNS spoofing service 6. Such criteria may include load on the hosts, their availability, etc. The DNS spoofing service 6 polls the hosts 1-3 periodically or at demand, and binds one of them at a time to the DNS lookup name resolver for the name "sun.com".

In a spoofing service, the criteria used to achieve the binding are not related to the context of the requester; they rely only upon information at the destination. Thus, much information that could be important in making a binding is not utilized. In none of the known systems is caller context used.

It would accordingly be advantageous to have a system which takes into account the context of the requester in the process of name resolution.

Various respective aspects and features of the invention are defined in the appended claims.

A context-dependent name resolution system is presented, which implements predetermined criteria for static or dynamic binding of a "name" to any one of several "objects" of the same type. Which "object" is selected for the binding is determined by a "name resolver" using context information that is explicitly specified by the requestor in a name resolution lookup call to the "name resolver". The "name resolver", which is implemented as a server program, stores a lookup table comprising bindings of a "name" to several different instances of an object, along with "policy" information which defines the criteria for selecting an instance of the object. For instance, the name may be an internet URL of the form "www.sun.com", and the resolved to object may be an IP address of the type 192.146.85.82. Thus the "name resolver" will store the tuple: <www.sun.com> <IP_address_1> <IP_address_2>..., and will store policies on which IP address to bind to www.sun.com when a lookup request specifying "www.sun.com" is received by it.

By enabling multiple binding support in the "name resolver", several advantages are realized. First, the system enables new resources to be added transparently to the caller. When a new server is added to distribute the load for one or more hosts corresponding to the name "sun.com", for instance, the IP address for the new server is simply added to the tuple in the name resolver, along with any desired policy criteria, e.g. to use only between 9 a.m. and 5 p.m.

Secondly, the fundamental limit to scaling which is inherent in today's single binding systems is removed, by enabling multiple destination servers providing the same service to be referenced by the same "name" handle by the caller (for example "sun.com"), and the name to be resolved by the name resolver to different physical computers servers, depending upon caller context. Many instances of the name resolver may be running on different physical computers, and many instances of the services may be running, and the requester will ac-

cess the name resolver closest to him; and the resolved object that is closest to the requester or that can best serve the request (based upon some selected or predetermined criteria) will be bound to the request, all transparently to the requester. Another advantage of the system of the invention is that it allows resources to be easily replicated transparently to the user, eliminating any single point of failure in the network or at the service end point. If one valid destination fails, is not responding or is overloaded, the name resolver is already capable of binding a "name" to multiple destinations, and the unavailable destination can be disabled in the name resolver's internal tables, using administrative means.

The context that may be used as a basis for the binding is variable; it may include information about the requester (e.g. requester IP address, domain name or inferred geographical region), about the destination (with similar alternatives), about the request itself (e.g. type or quality of service requested), or about independent information (e.g. time of day or time zone of the point of origin of the request).

The system may be implemented (eg as part of a computer apparatus) using hardware, software, or combinations thereof.

The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

Figures 1-2A are diagrams of present network systems used for destination addresses for requests.

Figure 3 is a flow chart illustrating a method according to an embodiment of the present invention.

Figures 4 and 5 are diagrams of network systems incorporating features of embodiments of the present invention.

Figure 6 is an illustration of the operation of an embodiment of the invention using geography-based resolution criteria.

Figure 7 is a diagram depicting zones in which domain name service resolvers and service location resolvers of the invention may be located.

A method according to the invention is illustrated in Figure 3, and Figures 4-5 shows a suitable systems implementable on the Internet or WorldWide Web, the Internet or an Intranet, incorporating features of the name resolution system.

Name resolution can include any kind of name resolution lookup for binding one object to another. This includes binding the name of a service to a host computer (or its IP address) that provides that service, and binding the type of service to the name of a service providing that type of service. It also includes resolving a name in one domain to another name in the same domain, and to another name in a different domain. For the purposes of this invention, the terms "service" and "host" can be considered synonymous, as can "service location" and "host location".

The system includes three fundamental features

that can be implemented singly or in any combination with one another: multiple binding of destination addresses to names; caller context name resolution in connection with such multiple binding; and name resolution policy considerations, i.e. independent criteria upon which such resolution is based.

Name Resolution: An Example

An example of name resolution occurs, for instance, when a user wishes to view video, e.g. a movie, on his or her computer. An application running on the computer is used to make a procedure call to the name resolver to determine which server can serve a movie, e.g.

`service_handle = name_service_lookup("movie")`
where the string "movie" is passed to a server, which then returns the name of the service providing that movie (or it may return a linked list of services providing movie services, from which the user may be prompted to select one).

The server may, by way of example, return a single service name (e.g. "quicktime") in the variable called "service_handle". Next, the application must determine which server host can provide this service to this client; to do this, it makes another name resolution call:

`host_handle = name_hostname_lookup(service_handle)`
and passes it the variable "service_handle" returned by the previous call. This call returns it the name of a server which is listed as offering this service.

The network location of this server must now be determined, so that the user's computer or workstation can connect to it to get the movie service, and so it makes the call:

`host_IP_address = name_hostaddress_lookup(host_handle)`
and finally obtains an IP address of an appropriate host that can provide the movie service to the user.

Further calls to this quicktime server may determine a list of movies that are available. Alternatively, a design may be had in which the caller simply specifies the name of the movie he wants to see, and the name lookup returns to the caller the IP address of a host that is currently able to serve the requested movie to the caller.

All of or some of the above steps may be combined in more integrated calls to the name resolver.

In the present invention, in addition to the above, an additional parameter is passed to the `name_hostaddress_lookup()` function above (or to all the functions above); this parameter may be called the `caller_context`. This `caller_context` is used by the name resolver to help it decide which IP address to use. Thus, the calls would look like:

`host_IP_address = name_hostaddress_lookup(host_handle, caller_context)`. `Caller_context` is a cookie (or structure) that may include information such as the caller's IP address, its point of origin, the quality of the requested service, or any other context that might be

relevant. These contexts must be well specified and their format(s) standardized, so that many different name resolvers can interoperate properly. The particular caller_context formats and contents selected are not themselves crucial,

The present embodiment uses requester context-dependent intelligence to determine which of several destination hosts should be utilized, or in other words, which of several IP addresses should be used to resolve a given "name" request. The context-dependent intelligence, implemented as hardware or software or a combination of both, allows the "name" resolution to be based upon some context information from the requester, and/or upon the "name" being resolved in a context-free manner, but optionally dependent upon criteria such as load balancing on the destination.

As shown in Figure 4, a requesters 100-120, of which there may be an arbitrary number, each comprise computers or workstations on a local network, served by a server 150. The requesters will typically be conventional workstations, personal computers, or any networkable computing device, with local processors (130, etc.), memory (140, etc.), mass storage (not shown) and network connections. The server 150 also includes a conventional processor 160, memory 170, mass storage and necessary connections and control hardware and software.

A name resolver 180 forms part of the server 150, or may be a separate unit. It may be implemented entirely in software, i.e. as program modules stored in mass storage and/or the memory 170, or it may be a stand-alone device, with its own logic or processor and memory, as desired.

The server 150 is connected to a broader network 170, such as the Internet, an Intranet or WAN (wide-area network), or the WorldWide Web, via a network connection (e.g. a T-line) 260. On this network 170 is optionally another name resolver 200, which may be implemented in the same fashion or differently from the name resolver 180. Name resolvers 180 and 200 may both be used, or either may be used by itself. (See discussion of Figure 7, below.)

Destination hosts 210-230 may also be conventional computers or workstations with processors (such as 240), memory (such as 250), mass storage (not shown), network connections, etc., as needed to implement conventional network functions in addition to the features of the present invention.

Referring to the flow chart of Figure 3, when a requester (such as 100-120) sends a name resolution request to a name resolver 180, instead of the single binding of conventional systems, the name resolver 180 includes multiple binding tables and/or functions (implemented by appropriate logic or program modules) to resolve the request to an appropriate IP address for a destination host (such as 210-230 in Figure 4).

An example of such a multiple binding would be the binding of multiple, geographically disparate destina-

tions to a single domain name. If, for instance, a user in Germany wishes to access www.sun.com (the WWW server for Sun Microsystems, Inc.), he or she can simply use the Uniform Resource Locator (URL) "http://www.sun.com". Thus, the user sends the request from requester 310 (see Figure 6), and the name resolver 320 determines that the requester is in Germany. (See step 20 in Figure 3). The selected destination may either be in the United States or elsewhere in Europe, since Sun Microsystems in this example has two "sun.com" locations. Since there is a valid European local destination 330, the name resolver 320 resolves the destination address to sun.com (Europe), as indicated at box 30 of Figure 3. This resolved destination is then selected for the request packet(s) (box 40 of Figure 3), and the request is forwarded to sun.com (Europe) (box 50 of Figure 3).

Following are lists of context-dependent resolution criteria applicable to the invention and usable at box 30 of Figure 3, where resolution may be based upon requester information, destination information, request contents, or other information:

A. Resolution Based Upon Requester Information

Examples of manners in which the resolution dependent upon requester information may be carried out include:

1. resolution based upon the domain name of the sender;
2. resolution based upon the inferred (looked-up) actual geographic region of the sender;
3. resolution based upon other geography-related information of the sender:
4. either directly ascertainable from the request (city/country info, e.g.); and/or
5. indirectly ascertainable (area code, address, etc.);
6. resolution based upon quality of service desired by the requester; and
7. resolution based upon requester's time of day or time zone.

B. Resolution Based Upon Destination Information

Examples of manners in which the resolution dependent upon a specified or intended destination or receiver information may be carried out include:

1. resolution based upon the load at the receiver;
2. resolution based upon the inferred (looked-up) actual geographic region of the receiver;
3. resolution based upon other geography-related information of the receiver:

4. either directly ascertainable from the request (city/country info, e.g.); and/or
5. indirectly ascertainable (area code, address, etc.).

Criterion B.1 can be resolved either based upon information as perceived at the sender end or based upon information as it exists at the receiver end, and resolved at the sender end. For example, the sender might frequently send requests to a particular server, service, geographical region or organization. In this case, it may be advantageous to regularly poll one or more often-used destinations to determine their level(s) of activity. Alternatively, such polling could automatically be carried out for any destinations for which the sender determines that its number of requests exceeds a certain threshold, or for a top predetermined percentage of requests sent by the requester (e.g. all destinations for which the number of requests exceeds N1%, or the top N2 destinations to which the sender makes requests, where N1 and N2 are appropriate predetermined numbers). Polling can be implemented as program modules integral to the name resolver(s), either entirely in one or in more than one location (e.g. partially in a local name resolver and partially in the destination server).

Alternatively or in addition, criterion B.1 may be based upon information at the receiver end at the time of sending the request, and resolved at the receiver.

C. Resolution Based Upon Request Contents

1. type of service requested;
2. specific information (or type of information) requested;
3. any other implicit information inferred from the request; and/or
4. any other explicit information obtained from the request.

D. Resolution Dependent Upon Other Factors

1. randomly generated selection of destination based upon qualified list; and/or
2. other independently developed information.

These resolution criteria can be used singly or in any desired combination with one another, as specified by the requester or the administrator of the destination (e.g. server owner or service provider). For instance, in the example of Figure 6 the resolution of the destination address to sun.com (Europe) could be modified if the load of sun.com (Europe) is larger by some predetermined threshold amount than the load at sun.com (USA) -- in which case the sun.com (USA) resolution could override the default sun.com (Europe) resolution for requesters in Europe, either at all times or only during peak European hours, which correspond to off-peak hours in the United States.

An extension of this system is in the resolution of services provided at the receiver network of a request. For instance, a given organization may have many database servers, and request for access to given information may in conventional systems be routed to the same server, because of the single binding nature of destination resolution. With multiple address resolution binding, multiple database servers (or other destination hosts) such as 210, 270, 280, etc. (see Figure 5) may be made available under a single name, in which case a local service resolution server, such as server 300 in Figure 5, is provided. The server 300 includes tables, program modules or the like as desired to resolve a request to any one of several to many IP addresses. The selection of a given server to receive a request can depend upon, for example, load at each of the servers.

In general, the resolution systems or subsystems will be in one of three "zones" (see Figure 7): the sender's zone 1 (up to, e.g., the sender's firewall or Internet server); the name resolver system's zone 2 (which may be at a server on the Internet, or any place outside zone 1 which is not in the receiver's system; and the receiver's zone 3. Service location name resolvers may be in any of zones 1-3; typically, destination lookup name resolvers, which may comprise multiple-binding domain name services (DNS's), will be in either zone 1 or zone 2. It will be understood that zones, for the purpose of this application, are administrative boundaries, and need not correlate to actual network boundaries.

The present embodiment can interact with existing systems in a number of ways. For instance, in secure systems where the source address is stripped from the request by a firewall (and only, e.g., the domain name remains), then the entire source address would not be used to resolve the destination; the name resolver is provided with the program instructions or circuitry to implement this. Note also that the DNS name resolution may be a distinct operation from service location, and thus the destination can be selected due to a combination of considerations including source address, requested destination address, and request contents, including the type of request made or service requested.

The multiple binding feature of the invention allows a single name, Internet address (e.g. URL address such as <http://www.sun.com>) or the like to represent as many actual servers (or services) as desired. This has a distinct advantage of allowing modifications, upgrades or replications to be made to the destination server(s) without modification of the destination address or service name as used by the requester. Such modifications may include adding servers or services, or establishing a mirror site at a location geographically near a large source of requests, etc.

There may be security and consistency implications of multiple bindings, with concomitant solutions. If a destination address can be multiply bound, a name resolver may be configured to bind to an incorrect address, either deliberately or otherwise. While this may also be a prob-

lem with existing single binding, multiple binding may complicate detection of the problem. Thus, the system of the invention may be combined with programs and tables for verification that a given binding is valid. Very secure systems may wish to limit their multiple binding to a predetermined, fixed number of resolution possibilities, or even maintain the current system of single binding as far as Internet or Web transmission is concerned, and implement multiple binding only behind a firewall. Alternatively or in addition, encryption and digital signatures may be used to ensure validity of bindings, and of modifications or additions to the bindings.

Variations may be had by designating a given name resolution as a default resolution, and utilizing alternative resolutions only upon the request meeting predetermined criteria (such as load imbalance, geographical distance, specific sources of the request, etc.).

Additional bindings (i.e. additional addresses to which a request may resolve) may be added without the requester being aware of it, and indeed substitutions may be made at any time, again transparently to the requester.

F. Service Selection Based Upon Caller Context

The system of the invention may be applied more generally to the use of caller context for name resolution. Context about the requesting user (e.g. in a variable called "caller_context") can be passed to appropriate functions, such as:

```
service_handle = name_service_lookup("movie",
caller_context)
host_handle = name_hostname_lookup
(service_handle, caller_context)
```

Here, the function service_handle executes a service name lookup based upon the input "movie", as well as the information in the variable caller_context, outputting the value service_handle. Given this output as input, along with (again) caller_context, the function host_handle then returns an appropriate host name.

An example of a possible such situation could result when a user desires an encryption service, and several encryption policies are available. The service_handle function can be configured to return different encryption algorithm services based upon the specified destination (which is specified in caller_context), or there may be an effective override in the caller_context by which the user can select a higher level of security.

In general, as noted above, the invention may be implemented at the sender's system or at the destination system, or indeed at points in between (e.g. at proxy servers). Note that single points of failure and bottlenecks are removed using the present system, and a truly distributed, multiply binding name resolution system is achieved.

Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Features of the dependent claims may be

combined with those of the independent claims as appropriate and in combinations other than those explicitly set out in the claims.

Claims

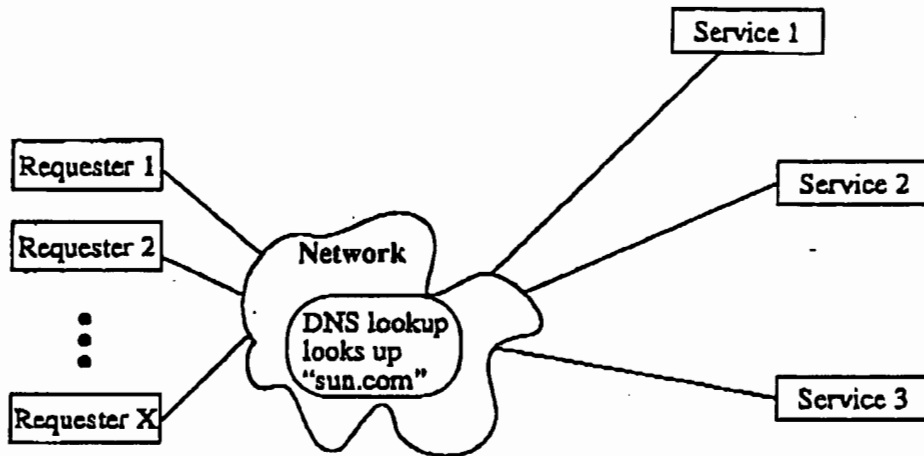
1. A system for name resolution of at least one request directed to a destination name of a receiver and issued from a requester system, including:
a name resolver connected to the requester service and including

predetermined information correlating a plurality of destination addresses with said destination name;
a criteria selection subsystem configured to provide a selection of at least one said destination address based upon at least one predetermined criterion; and
a destination address binder configured to bind said destination name with said selected destination address.

2. The system of claim 1, wherein said at least one predetermined criterion includes a criterion based upon information explicitly contained within said request.
3. The system of claim 2, wherein said information includes an address of said requester.
4. The system of claim 2, wherein said information is based upon at least a portion of contents of said request.
5. The system of claim 4, wherein said portion of said contents includes at least one of:
a type of service requested by said request; and
a quality of service requested by said request.
6. The system of claim 1, wherein said at least one predetermined criterion includes a criterion based upon information not explicitly contained within said request.
7. The system of claim 6, wherein said information pertains to a geographical region of said requester.
8. The system of claim 6, wherein said information pertains to a geographical region of said receiver.
9. The system of claim 6, wherein said information includes load information relating to said receiver.
10. The system of claim 6, wherein said information includes at least one of time and date information.

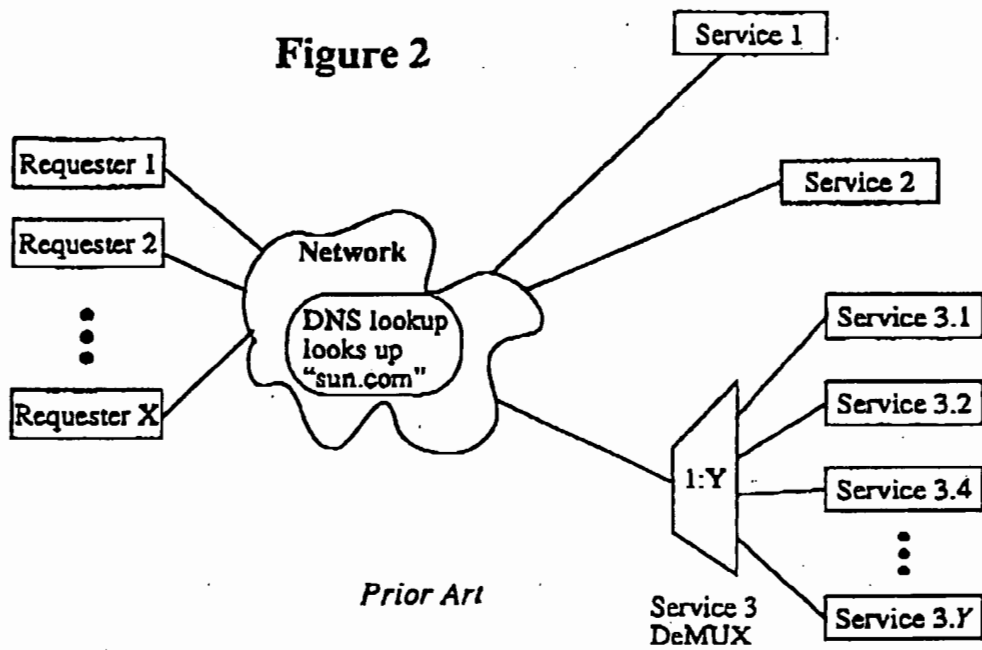
11. The system of claim 1, wherein said binding is to a port at said destination address.
12. The system of claim 1, wherein said binding is based at least in part upon a random selection of one said destination address.
13. A method for context-dependent binding of a destination name to a destination address in a name resolver having a predetermined set of binding criteria and predetermined correlations of destination names with destination addresses, wherein at least one said correlation is a multiple correlation correlating a plurality of said destination addresses with a single destination name, including the steps of:
- (1) receiving said request at said name resolver; and
 - (2) based upon said multiple correlation, retrieving at least one said destination address from said plurality of destination addresses.
14. The method of claim 13, further including after step 2, the step of:
- (3) binding said retrieved destination address to said destination name.
15. The method of claim 14, further including after step 3, the step of:
- (4) transmitting said request with said destination address.
16. The method of claim 13, wherein said multiple correlation is based upon information explicitly contained within said request.
17. The system of claim 13, wherein said multiple correlation is based upon at least a portion of contents of said request.
18. The system of claim 13, wherein said multiple correlation is based upon at least one of:
- an address of said requester; and
 - a type of service requested by said request; and
 - a quality of service requested by said request.
19. The system of claim 1, wherein said multiple correlation is based upon information not explicitly contained within said request.
20. The system of claim 19, wherein said multiple correlation is based upon at least one of:
- a geographical region of said receiver;
 - load information relating to said receiver;
 - time information;
 - date information; and
- a random factor generated by said name resolver.
21. A system for name resolution of at least one request directed to a destination name of a receiver and issued from a requester system, the request information relating to caller context, the system including:
- a name resolver connected to the requester service and including
 - predetermined information correlating a plurality of service names with said caller context;
 - a service selection subsystem configured to provide a selection of at least one said service name based upon said caller context; and
 - a host name selection subsystem configured to return a host name based corresponding to said selected service name.
22. The system of claim 1, wherein said at least one predetermined criterion includes:
- a first criterion based upon information explicitly contained within said request; and
 - a second criterion based upon information not explicitly contained within said request.
23. The system of claim 22, wherein said second criterion corresponds to a predetermined policy used by said name resolver.
24. The system of claim 23, wherein said first criterion corresponds to information relating specifically to said requester system.

Figure 1



Prior Art

Figure 2



Prior Art

Figure 2A

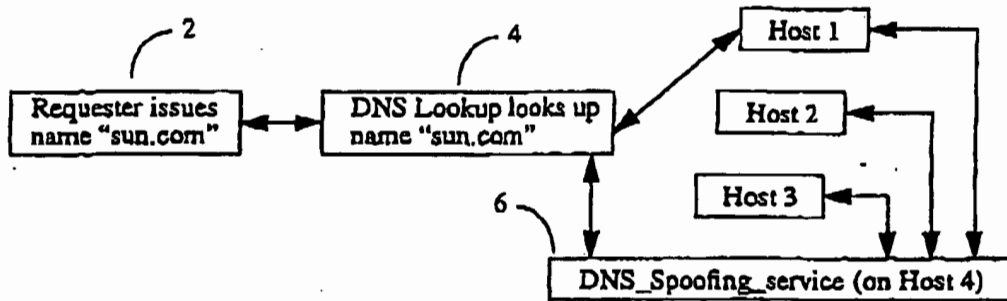
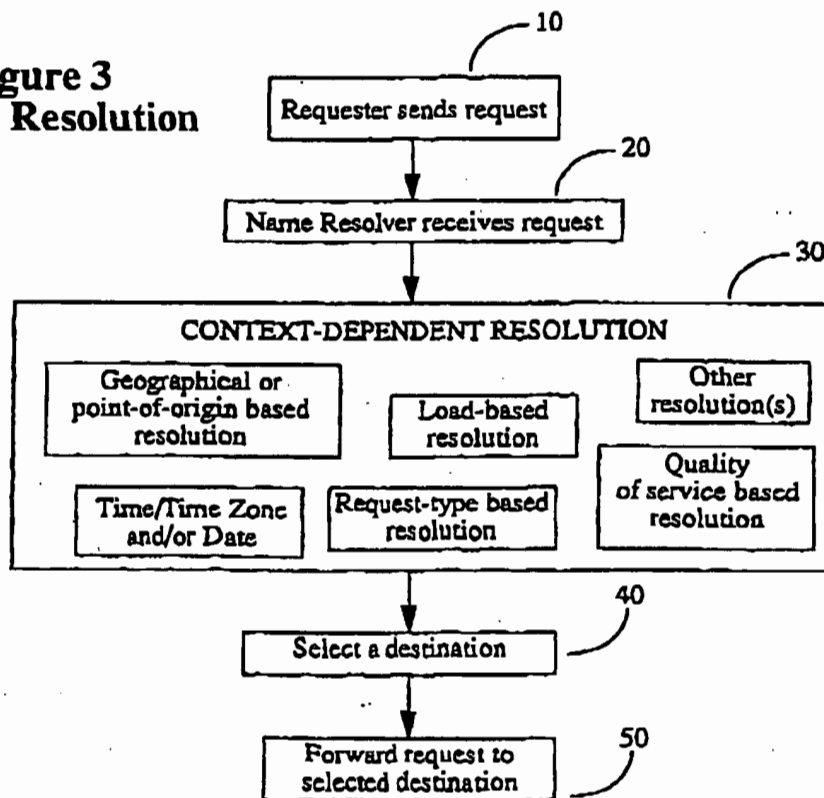
Figure 3
Service Resolution

Figure 4

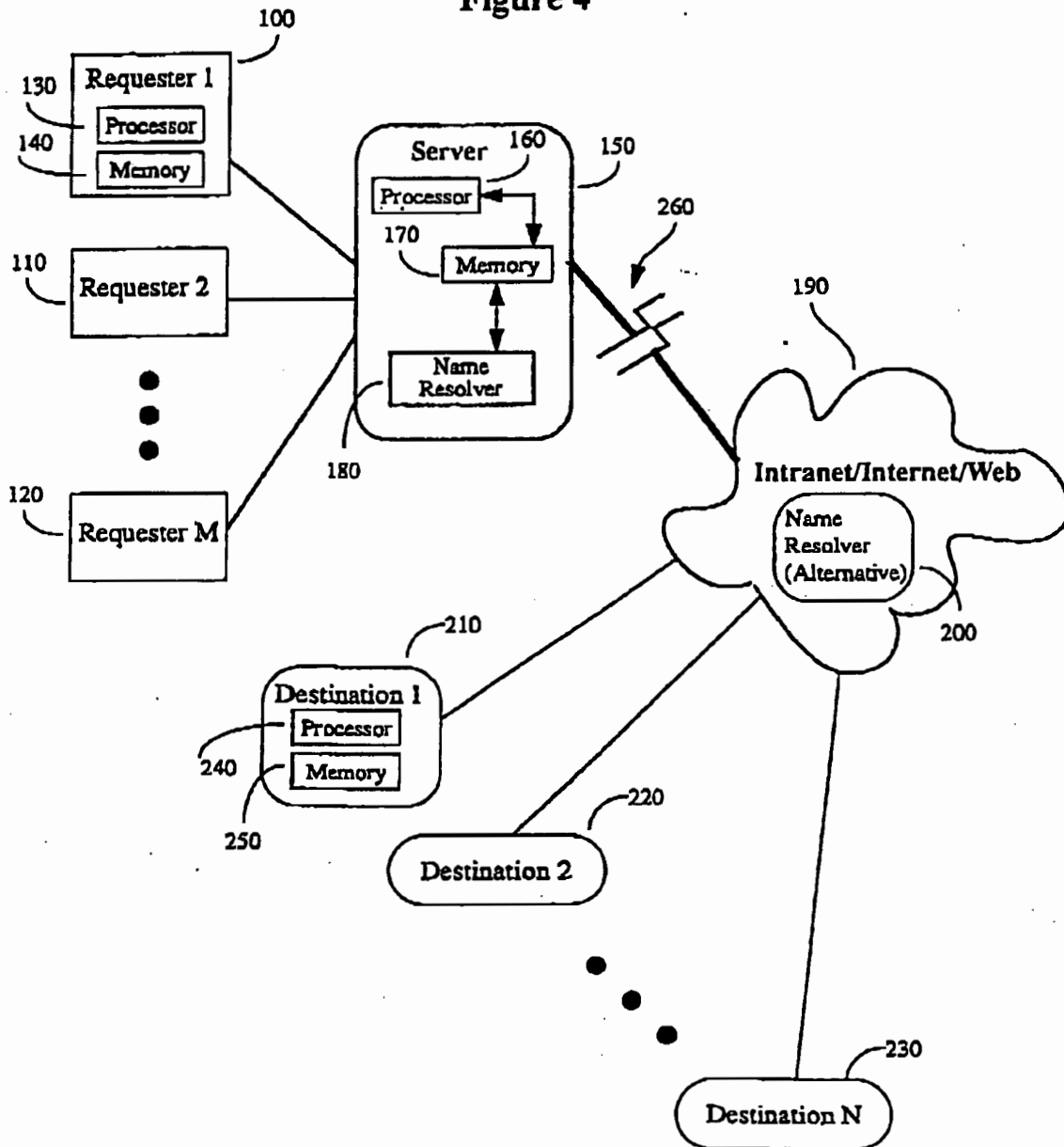


Figure 5

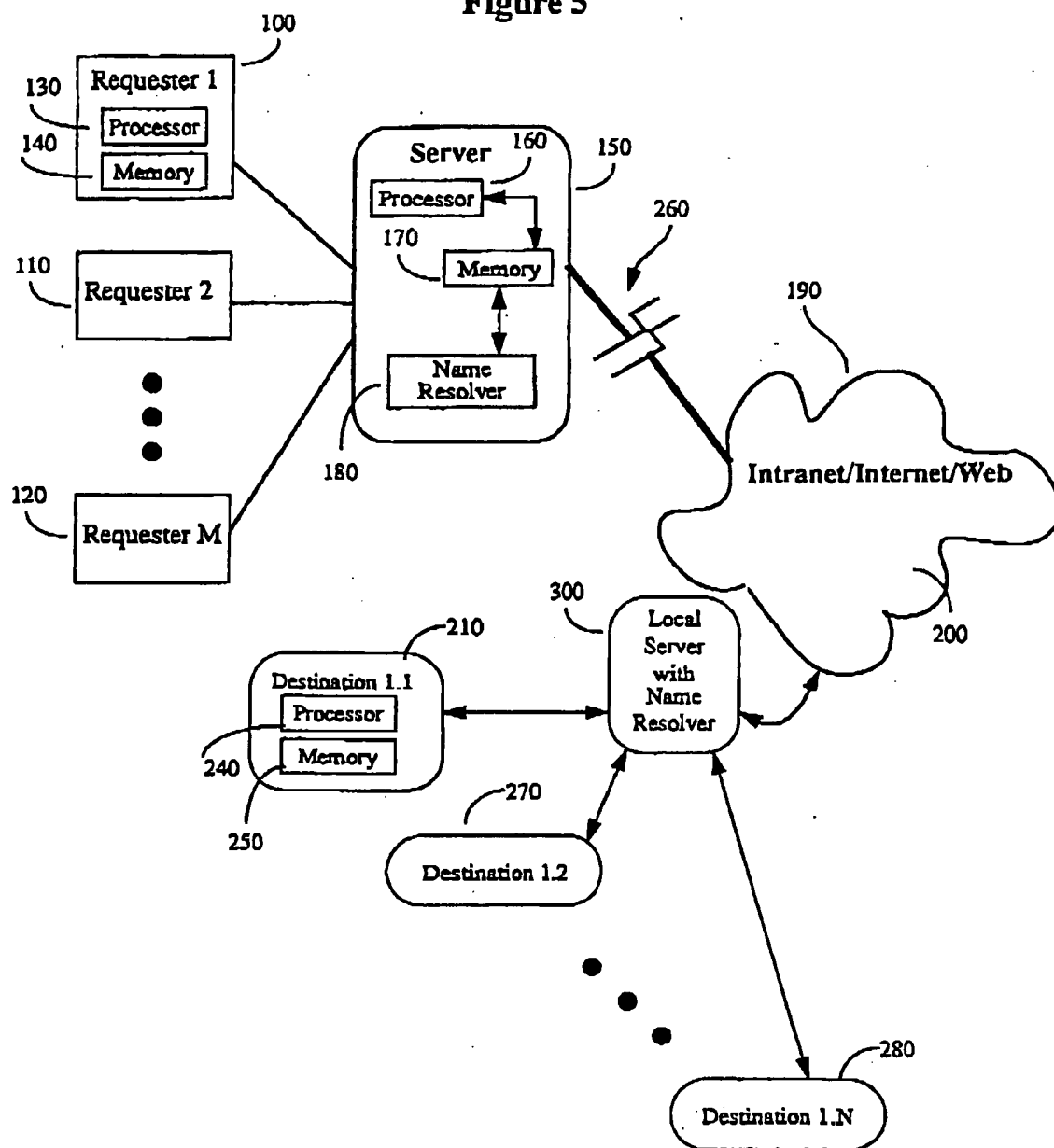


Figure 6

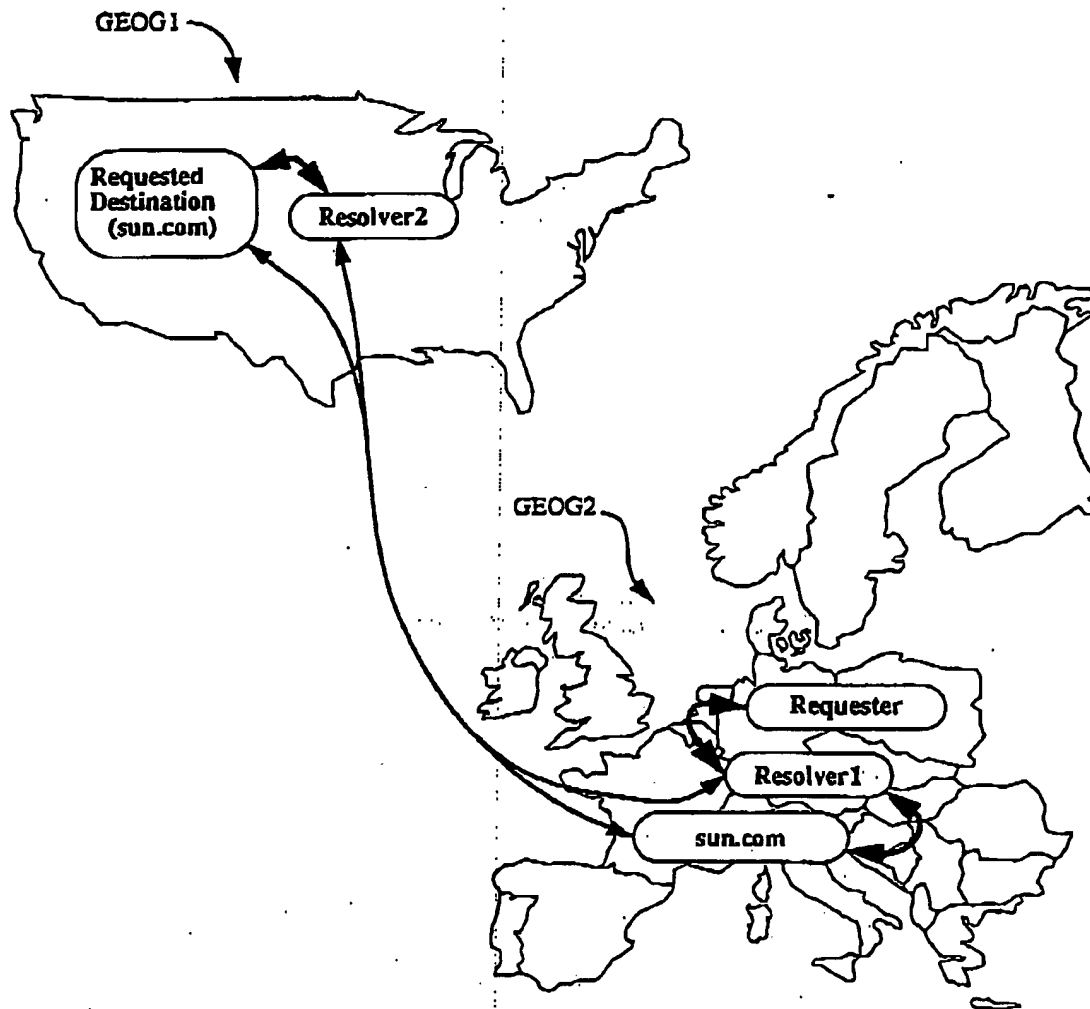


Figure 7

<u>Zone 1</u> SENDER	<u>Zone 2</u> RESOLVER SYSTEM	<u>Zone 3</u> RECEIVER
Service Location Resolver1	Service Location Resolver2	Service Location Resolver3
Destination Lookup1	Destination Lookup2	

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 817 444 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
27.12.2000 Bulletin 2000/52

(51) Int Cl.7: H04L 29/06, H04L 29/12

(43) Date of publication A2:
07.01.1998 Bulletin 1998/02

(21) Application number: 97304697.2

(22) Date of filing: 30.06.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE

(72) Inventor: Ebrahim, Zahir
Mountain View, California 94043 (US)

(30) Priority: 01.07.1996 US 674561

(74) Representative: Turner, James Arthur et al
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

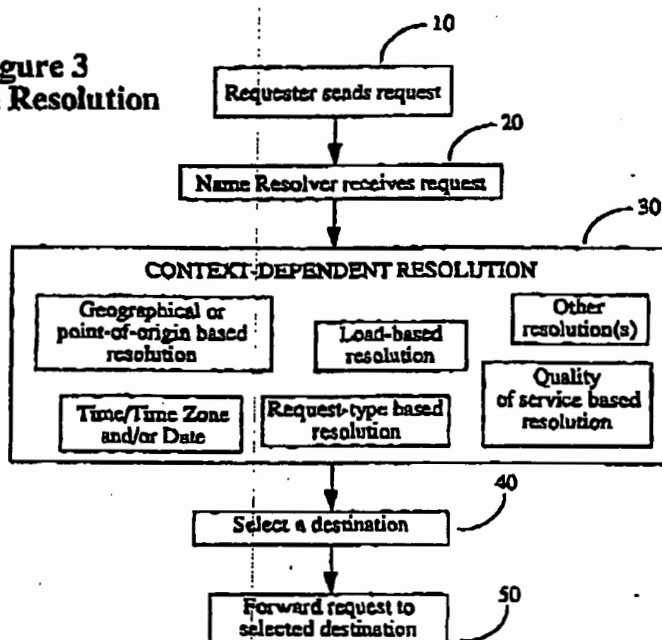
(71) Applicant: SUN MICROSYSTEMS, INC.
Mountain View, California 94043-1100 (US)

(54) System for context-dependent name resolution

(57) A context-dependent, multiply binding name resolution system. A name resolver is provided, connected to either a requester's system or a receiver's system, or both. Requests to a given service or domain name are resolved to the appropriate IP address. The intended recipient of the request is resolved based upon a combination of one or more predetermined criteria, including: information about the sender (e.g. geographical

location, specific requester identity, etc.); information about the intended recipient (e.g. load balance at the receiver, type of service, etc.); information contained within the request itself (e.g. type of service requested); or other information (time of day, date, random selection of recipient, e.g.). The system is implemented in hardware and/or software, and the resolution criteria can be made interdependent or independent.

Figure 3
Service Resolution



EP 0 817 444 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 4697

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	US 5 136 716 A (HARPER JOHN ET AL) 4 August 1992 (1992-08-04) * abstract *	1,6,13, 14,16,17	H04L29/06 H04L29/12
A	* column 2, line 22 - line 53 * * column 3, line 4 - line 40 * * column 3, line 63 - column 5, line 24 * * claims 1,4 *	15,21	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			H04L
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 7 November 2000	Examiner Kesting, V
CATEGORY OF CITED DOCUMENTS		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 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	

EP0 FORM 1500 (02/92) (P/0201)

EP 0 817 444 A3

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 97 30 4697

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-11-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5136716 A	04-08-1992	CA 1312144 A	29-12-1992
		DE 3876617 A	21-01-1993
		DE 3876617 D	21-01-1993
		DE 3876617 T	08-04-1993
		EP 0329779 A	30-08-1989
		JP 1502861 T	28-09-1989
		WO 8902129 A	09-03-1989

EPD FORM 1005

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

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	33	"virtual community" near2 network\$2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:03
S2	19	S1 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:09
S3	5	S2 and ((private or public) with address)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:00
S4	45	((virtual near (community or network)) and (private near address\$3) and (public near address\$3) and (IP near address\$2))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:04
S5	27	S4 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:04
S6	53	("6226751").URPN.	USPAT	OR	OFF	2006/09/13 20:30
S7	1	"20040249911".pn.	US-PGPUB; USPAT	OR	OFF	2006/09/14 09:59
S8	139	("domain name" or DNS) with (VPN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:08
S9	74	S8 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:09
S10	22	S9 and (NAT with (public or private))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 11:02

EAST Search History

S11	1801	709/245.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 11:02
-----	------	---------------	---	----	-----	------------------



UNITED STATES PATENT AND TRADEMARK OFFICE

R

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.
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0	2698

28554 7590 09/22/2006

VIERRA MAGEN MARCUS & DENIRO LLP
575 MARKET STREET SUITE 2500
SAN FRANCISCO, CA 94105

EXAMINER

BLAIR, DOUGLAS B

ART UNIT	PAPER NUMBER
----------	--------------

2142

DATE MAILED: 09/22/2006

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

Office Action Summary

Application No.

10/403,818

Applicant(s)

ALKHATIB ET AL.

Examiner

Douglas B. Blair

Art Unit

2142

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

- 1) ☒ Responsive to communication(s) filed on 31 March 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) 1-109 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed. -
- 6) ☒ Claim(s) 1-109 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ 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).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

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

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
- Paper No(s)/Mail Date 2/9/04, 11/12/04, and 2/6/04

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

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 –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-109 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent

Application Publication Number 2003/0041136 by Cheline et al.

As to claim 1, Cheline teaches a virtual community network system, comprising: a virtual network manager including at least one virtual community definition comprising at least a domain name (**paragraphs 87-89, an infrastructure for dealing with domain names is clearly defined**) and a user set (**paragraph 43, the users registered with the authentication server are a user set**); and at least one route director capable of communicating with users in the user set (**paragraphs 62-64, the modem is considered a route director**).

As to claim 2, Cheline teaches the system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent (**paragraph 51, the user's home client program is an agent**).

As to claim 3, Cheline teaches the system of claim 2 wherein the agent is installed on a processing device (**the home computer**).

Art Unit: 2142

As to claim 4, Cheline teaches the system of claim 2 wherein the agent is installed on a proxy device **(the home computer)**.

As to claim 5, Cheline teaches the system of claim 2 wherein the virtual network manager includes a NAT device detector for agents installed on a processing device behind a NAT device **(Figure 2, the modem is NAT device, the VPN provider detects communication from the modem)**.

As to claim 6, Cheline teaches the system of claim 1 wherein the manager comprises a device coupled to a public network and having a public network address **(paragraph 59)**.

As to claim 7, Cheline teaches the system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device **(paragraph 51)**.

As to claim 8, Cheline teaches the system of claim 7 wherein each said device includes at least one virtual address in the community and at least one physical address **(paragraph 51-54)**.

As to claim 9, Cheline teaches the system of claim 8 wherein the physical address is dynamic **(paragraph 51-54)**.

As to claim 10, Cheline teaches the system of claim 8 wherein the physical address is static **(paragraph 51-54)**.

As to claim 11, Cheline teaches the system of claim 8 wherein the physical address is private **(paragraph 51)**.

Art Unit: 2142

As to claim 12, Cheline teaches the system of claim 8 wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device **(paragraph 51-54)**.

As to claim 13, Cheline teaches the system of claim 12 wherein the physical address is dynamic **(paragraph 51-54)**.

As to claim 14, Cheline teaches the system of claim 12 Wherein the physical address is static **(paragraph 51-54)**.

As to claim 15, Cheline teaches the system of claim 12 wherein said first, device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device **(paragraph 51-54)**.

As to claim 16, Cheline teaches the system of claim 15 wherein said second device includes at least one virtual address in the realm and at least one private physical address **(paragraph 51-54)**.

As to claim 17, Cheline teaches the system of claim 15 wherein the physical address is dynamic **(paragraph 51-54)**.

As to claim 18, Cheline teaches the system of claim 15 wherein the physical address is static **(paragraph 51-54)**.

As to claim 19, Cheline teaches the system of claim 15 wherein said at least first private network and said at least second private network share at least one network address **(paragraph 51-54)**.

As to claim 20, Cheline teaches the system of claim 1 wherein the route director includes a pseudo address assignment for at least one user in the user set **(paragraph 51-54)**.

Art Unit: 2142

As to claim 21, Cheline teaches the system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm **(paragraph 51-54)**.

As to claim 22, Cheline teaches the system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address **(paragraph 51-54)**.

As to claim 23, Cheline teaches the system of claim 22 wherein the route director is coupled to said public network and includes a public network address **(paragraph 51-54)**.

As to claim 24, Cheline teaches the system of claim 22 wherein the route director is coupled to a first private network and said route director includes a private network address **(paragraph 51-54)**.

As to claim 25, Cheline teaches the system of claim 1 wherein communications between users in the user set are encapsulated **(paragraph 71)**.

As to claim 26, Cheline teaches the system of claim 1 wherein communications between users in the user set are encrypted **(paragraph 68)**.

As to claim 27, Cheline teaches the system of claim 26 wherein said encryption uses IPSEC **(paragraph 68)**.

As to claims 28 and 29, Cheline teaches the use of DES and triple DES **(paragraph 42)**.

As to claim 30, Cheline teaches the system of claim 1 wherein the manager includes at least a second virtual domain definition **(paragraph 86)**.

Art Unit: 2142

As to claim 31, Cheline teaches the system of claim 1 further including at least a first public route director (**router 132 in Figure 1**) and a second private route director (**modem 106 in Figure 1**).

As to claim 32, Cheline teaches a system, comprising: a management device including network interface coupled to a public address realm and having a public address (**client device on network in Figure 1**); a virtual community network traffic router (**Figure 1, number 146**); and router data including at least one association of a logical identifier with public routing information for a member (**The VPN is router data and the radius packet is a logical identifier**).

As to claim 33, Cheline teaches the system of claim 32 wherein the network traffic router includes a network interface accessible by a public address in the public address realm (**paragraphs 51-54**).

As to claim 34, Cheline teaches the system of claim 32 wherein the management device includes a UDP port capable of receiving virtual community network traffic (**paragraph 51, ICQ uses UDP**).

As to claim 35, Cheline teaches the system of claim 32 wherein the management device includes a TCP port capable of communicating virtual community network traffic (**paragraphs 51-54**).

As to claim 36, Cheline teaches the system of claim 32 wherein a member accesses a physical network via a processing device and the system further includes at least one agent installed on the processing device (**Figure 1**).

As to claim 37, Cheline teaches the system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router includes a transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent **(paragraphs 51-54)**.

As to claim 38, Cheline teaches the system of claim 32 further including at least one proxy agent on a private physical network communicating with a member and the network traffic router **(paragraphs 51-54)**.

As to claim 39, Cheline teaches the system of claim 38 wherein the member accesses other members using a device coupled to a private physical network **(paragraphs 51-54)**.

As to claim 40, Cheline teaches the system of claim 32 wherein the manager includes a member register module **(paragraph 67)**.

As to claim 41, Cheline teaches the system of claim 40 wherein the manager includes a member join module **(paragraph 67)**.

As to claim 42, Cheline teaches the system of claim 41 wherein the join module provides a virtual address to a registered member **(paragraph 68)**.

As to claim 43, Cheline teaches the system of claim 41 wherein the manager maintains data on an association between at least one virtual address with at least one member **(paragraph 68)**.

As to claim 44, Cheline teaches the system of claim 40 wherein the manager includes a DNS server for the virtual community **(paragraph 64)**.

As to claim 45, Cheline teaches the system of claim 32 further including a virtual community network communication agent for a device, comprising a virtual

Art Unit: 2142

network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via their virtual address (**paragraph 47**).

As to claim 46, Cheline teaches the system of claim 45 wherein the agent includes a domain name routing plugin (**paragraph 47**).

As to claim 47, Cheline teaches the system of claim 45 wherein the agent includes a separate IP stack for each user in the user set accessing the device (**paragraph 47**).

As to claim 48, Cheline teaches the system of claim 45 wherein the adapter is a deterministic network enhancer (**paragraph 47**).

As to claim 49, Cheline teaches the system of claim 45 wherein the adapter includes a DNS plugin (**paragraph 47**).

As to claim 50, Cheline teaches the system of claim 45 wherein the adapter includes an IPSEC plugin (**paragraph 47**).

As to claim 51, Cheline teaches the system of claim 45 wherein the adapter includes a domain name routing plugin (**paragraph 47**).

As to claim 52, Cheline teaches the system of claim 45 wherein the agent includes a community registration module (**paragraph 47**).

As to claim 53, Cheline teaches a virtual community network system, comprising: a virtual community network manager (**paragraphs 87-89**); a route director (**paragraph 47**); at least a first virtual community agent associated community member (**paragraph 86**); and with a first at least a second virtual community agent associated with at least a second community member (**paragraph 86**).

As to claim 54, Cheline teaches the system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address **(paragraph 51-54)**.

As to claim 55, Cheline teaches the system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private physical network address **(paragraph 51-54)**.

As to claim 56, Cheline teaches the system of claim 53 wherein the first or second virtual community network agent is installed on a device used by a member to access a network **(paragraph 51-54)**.

As to claim 57, Cheline teaches the system of claim 56 wherein the device is in a private physical network **(paragraph 51-54)**.

As to claim 58, Cheline teaches the system of claim 56 wherein the device is coupled to a public physical network **(paragraph 51-54)**.

As to claim 59, Cheline teaches the system of claim 53 wherein the first or second virtual community network agent is a proxy agent **(paragraph 51-54)**.

As to claim 60, Cheline teaches the system of claim 53 wherein the first and second members access the virtual community via devices coupled to separate private address physical realms **(paragraph 51-54)**.

As to claim 61, Cheline teaches the system of claim 53 wherein the virtual community network manager includes at least a first community definition and a second community definition **(paragraph 86)**.

Art Unit: 2142

As to claim 62, Cheline teaches the system of claim 53 wherein the community network manager includes a member authenticator (**paragraph 67**).

As to claim 63, Cheline teaches the system of claim 62 wherein the community network manager includes a DNS server providing authoritative responses for DNS queries in the virtual community (**paragraphs 86-89**).

As to claim 64, Cheline teaches a method for providing a secure virtual network, comprising: providing a virtual network manager coupled to a public network (**ref. number 146 in Figure 1**); defining a member set of users entitled to communicate in the virtual network (**paragraph 67**); registering members with the manager (**paragraph 67**); assigning members a virtual address (**paragraph 55**); and routing network traffic between the members in the virtual community (**paragraphs 51-54**).

As to claim 65, Cheline teaches the method of claim 64 further including the step of providing users in said member set with a communication agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 66, Cheline teaches the method of claim 65 wherein said step of providing users with a communication agent includes providing a proxy agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 67, Cheline teaches the method of claim 65 wherein said step of providing users with a communication agent includes providing an agent installed on a device used by the member to couple to a network (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 68, Cheline teaches the method of claim 65 wherein the step of registering comprises authenticating members with the member set (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 69, Cheline teaches the method of claim 64 wherein the step of defining a member set includes the step of assigning a domain name for the community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 70, Cheline teaches the method of claim 64 wherein the step of defining a member set includes defining at least two member sets having at least one different member (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 71, Cheline teaches the method of claim 64 wherein the step of assigning a virtual address includes assigning an IPV4 compliant address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 72, Cheline teaches the method of claim 71 wherein the step of assigning a virtual address includes assigning a non-routable IPV4 compliant address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 73, Cheline teaches the method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address with a second member accessing the public network on a second device having a different public address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 74, Cheline teaches the method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address with a second member

Art Unit: 2142

accessing the public network on a second device having a public address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 75, Cheline teaches the method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address with a second member accessing the public network on a device in a private physical network having a second private physical address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 76, Cheline teaches the method of claim 75 wherein the first private physical address and the second private physical address are identical (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 77, Cheline teaches the method of claim 64 further including the step of responding to DNS requests for members in the virtual network (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 78, Cheline teaches the method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 79, Cheline teaches the method of claim 64 further including applying a group policy to members of the virtual community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 80, Cheline teaches one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to

Art Unit: 2142

perform a method comprising the steps of: managing a virtual community network realm (**Figure 1**); defining a member set of users entitled to communicate in the virtual community (**paragraph 67**); registering users with the virtual community (**paragraph 67**); assigning each user a virtual address (**paragraph 55**); and routing network traffic between the users in the virtual community (**paragraphs 51-54**).

As to claim 81, Cheline teaches the one or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 82, Cheline teaches the one or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 83, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 84, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of assigning a virtual address includes a non-routable IPV4 compliant address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 85, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device

Art Unit: 2142

having a public address with a second member accessing the public address realm on a second device having a different public address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 86, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address with a second member accessing the public address realm on a second device having a public address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 87, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address with a second member accessing the public address realm on a device in a private physical network having a second private physical address (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 88, Cheline teaches the one or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 89, Cheline teaches the one or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

Art Unit: 2142

As to claim 90, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic **(paragraphs 43, 47, 51-55, 62-64 and 86-89).**

As to claim 91, Cheline teaches the one or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic **(paragraphs 43, 47, 51-55, 62-64 and 86-89).**

As to claim 92, Cheline teaches the one or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community **(paragraphs 43, 47, 51-55, 62-64 and 86-89).**

As to claim 93, Cheline teaches a virtual community network system, comprising: a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set **(see mapping in claim 1)**, the network being assessable by users in the user set and users outside the user set **(in Figure 1 the VPN is attached to the Internet)**, the manager exchanging virtual community network information with users in the user set **(paragraphs 51-54).**

As to claim 94, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member register module **(paragraphs 43, 47, 51-55, 62-64 and 86-89).**

As to claim 95, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member join module **(paragraphs 43, 47, 51-55, 62-64 and 86-89).**

Art Unit: 2142

As to claim 96, Cheline teaches the system of claim 95 wherein the join module provides a virtual address to a registered member (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 97, Cheline teaches the system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 98, Cheline teaches the system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 99, Cheline teaches the system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 100, Cheline teaches the system of claim 93 wherein the virtual network manager includes at least a second virtual domain definition (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 101, Cheline teaches the system of claim 93 wherein the virtual network manager includes at least a first virtual community definition and a second virtual community definition (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 102, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member authenticator (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

Art Unit: 2142

As to claim 103, Cheline teaches the system of claim 93 wherein the virtual network manager includes a DNS server providing authoritative responses for DNS queries from users in the virtual community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 104, Cheline teaches the system of claim 93 wherein the system further includes at least one route director capable of communicating with users in the user set (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 105, Cheline teaches the system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 106, Cheline teaches the system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device, wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 107, Cheline teaches the system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

As to claim 108, Cheline teaches the system of claim 93 wherein communications between users in the user set are encrypted (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

Art Unit: 2142

As to claim 109, Cheline teaches the system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

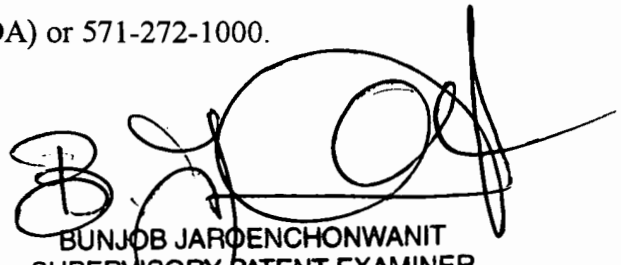
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas B. Blair whose telephone number is 571-272-3893. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

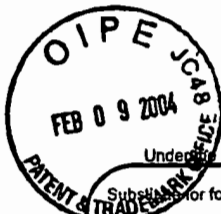
Douglas Blair



BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER

Application/Control Number: 10/403,818
Art Unit: 2142

Page 19



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

Submit this form for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet

1

of

1

Complete if Known

Application Number 10/403,818

Filing Date March 31, 2003

First Named Inventor Alkhatib

Art Unit 2157

Examiner Name

Attorney Docket Number TTCC-01021US0

RECEIVED

FEB 12 2004

Technology Center 2100

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
DB		VENTERS, Demystifying Protocols: A comparison of Protocols Suitable for IP Telephony, Sonus Networks, pp. 1-11, 2000.	
DB		TSUCHIYA, ET AL., Extending the IP Internet Through Address Reuse, ACM SIGCOMM Computer Communication Review, pp. 16-33, JANUARY 1993.	
DB		FRANCIS, ET AL., IPNL: A NAT-Extended Internet Architecture, SIGCOMM'01, 8/27-31, 2001, pp. 69-79.	
DB		YALAGANDULA, ET AL., Transparent Mobility with Minimal Infrastructure, University of Texas at Austin, pp. 1-14, JULY 2001.	
DB		TERAOKA, ET AL., VIP: A Protocol Providing Host Mobility, Communications of the ACM, August 1994/Vol. 37, No. 8, pp. 67-75, 113.	
DB		EDEVANG, ET AL., The IP Network Address Translator (NAT), Network Working Group, RFC 1631, May 1994, pp. 1-10.	
DB		CHATEL, Classical Versus Transparent IP Proxies, Network Working Group, RFC 1919, March 1996, pp. 1-35.	
DB		FINSETH, An Access Control Protocol, Sometimes Called TACACS, Network Working Group, July 1993, pp. 1-18.	
DB		Computer Networks, Third Edition, by Andrew S. Tanenbaum, 1996, pp. 643-670, 685-691.	
DB		PERKINS, Mobile IP, IEEE Communications Magazine, May 1997, pp. 84-99	

Examiner Signature	/Douglas Blair/	Date Considered	09/14/2006
--------------------	-----------------	-----------------	------------

*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 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98: The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

*1 = COPY NOT SUBMITTED BECAUSE IT WAS SUBMITTED IN PRIOR APPLICATION NO. 09/492,565, filed 1/27/2000, which is a continuation of Application No. 09/015,840, filed 1/29/1998.



PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031

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

Complete if Known

(Use as many sheets as necessary)

Sheet	1
-------	---

of 1

Application Number	10/403,818
Filing Date	March 31, 2003
First Named Inventor	Alkhatib
Art Unit	2157
Examiner Name	
Attorney Docket Number	TTCC-01021US0

[illegible][illegible]

Examiner Signature	/Douglas Blair/	Date Considered	09/14/2006
-----------------------	-----------------	--------------------	------------

*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 Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 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.18 if possible. 6 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of
Invention

SECURE VIRTUAL COMMUNITY NETWORK SYSTEM

Application Number: 10/403818



Confirmation Number: 2698

First Named Applicant: HASAN ALKHATIB

Attorney Docket Number: TTCC-01021US0

Art Unit: 2157

Search string: (5361256 or 5623605 or 5717687 or 5751961
or 5777989 or 5781550 or 5790548 or 5805818
or 5805820 or 5856974 or 5867667 or 5884246
or 5889953 or 5913210 or 5937162 or 5937163
or 6003084 or 6055575 or 5793763 or 6119171
or 6061738 or 6047325 or 6032196 or 5815664
or 5764906 or 6006272 or 6557037 or 6591306
or 5734651 or 5701427 or 5563878).pn.

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

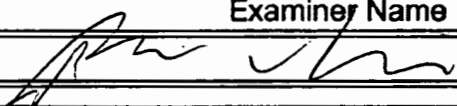
init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
~~DB~~	1	5361256	1994-11-01	Doeringer			
~~DB~~	2	5623605	1997-04-22	Keshav			
~~DB~~	3	5717687	1998-02-10	Minot			
~~DB~~	4	5751961	1998-05-12	Smyk			
~~DB~~	5	5777989	1998-07-07	McGarvey			
~~DB~~	6	5781550	1998-07-14	Templin			
~~DB~~	7	5790548	1998-08-04	Sistainizadeh			
~~DB~~	8	5805818	1998-09-08	Perlman			
~~DB~~	9	5805820	1998-09-08	Bellovin			
~~DB~~	10	5856974	1999-01-05	Gervais			
~~DB~~	11	5867667	1999-02-02	Butman			
~~DB~~	12	5884246	1999-03-16	Boucher			
~~DB~~	13	5889953	1999-03-30	Thebaut			

APP_ID=10403818

page 1 of 2

DBB	14	5913210	1999-06-15	Call
DBB	15	5937162	1999-04-10	Funk
DBB	16	5937163	1999-04-10	Lee
DBB	17	6003084	1999-12-14	Green
DBB	18	6055575	2000-04-25	Paulsen
DBB	19	5793763	1998-08-11	Mayes
DBB	20	6119171	2000-09-12	Alkhatib
DBB	21	6061738	2000-05-09	Osaku
DBB	22	6047325	2000-04-04	Jain
DBB	23	6032196	2000-02-29	Monier
DBB	24	5815664	1998-09-29	Asano
DBB	25	5764906	1998-06-09	Edelstein.
DBB	26	6006272	1999-12-21	Aravamudan
DBB	27	6557037	2003-04-29	Provino
DBB	28	6591306	2003-07-08	Redlich
DBB	29	5734651	1998-03-31	Blakeley
DBB	30	5701427	1997-12-23	Lathrop
DBB	31	5563878	1996-10-08	Blakeley

Signature

Examiner Name	Date
	9/15/06

Notice of References Cited	Application/Control No. 10/403,818	Applicant(s)/Patent Under Reexamination ALKHATIB ET AL.	
	Examiner Douglas B. Blair	Art Unit 2142	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,107,464	09-2006	Shapira et al.	709/200
*	B	US-6,226,751	05-2001	Arrow et al.	726/15
*	C	US-6,970,941	11-2005	Caronni et al.	709/238
*	D	US-7,010,702	03-2006	Bots et al.	726/13
*	E	US-6,701,437	03-2004	Hoke et al.	726/15
*	F	US-6,594,704	07-2003	Birenback et al.	709/238
*	G	US-2004/0148439	07-2004	Harvey et al.	709/249
*	H	US-2003/0041136	02-2003	Cheline et al.	709/223
*	I	US-2003/0041091	02-2003	Cheline et al.	709/200
*	J	US-7,092,390	08-2006	Wan, Albert Chungbor	370/392
*	K	US-6,832,322	12-2004	Boden et al.	726/15
*	L	US-7,107,614	09-2006	Boden et al.	726/15
*	M	US-2002/0133534	09-2002	Forslow, Jan	709/200

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.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)



Notice of References Cited

Part of Paper No. 20060914

Index of Claims



Application/Control No.

10/403,818

Examiner

Douglas B. Blair

Applicant(s)/Patent under
Reexamination

ALKHATIB ET AL.

Art Unit

2142

✓	Rejected
=	Allowed

-	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date											
Final	Original	9/14/06											
	1	✓											
	2	✓											
	3	✓											
	4	✓											
	5	✓											
	6	✓											
	7	✓											
	8	✓											
	9	✓											
	10	✓											
	11	✓											
	12	✓											
	13	✓											
	14	✓											
	15	✓											
	16	✓											
	17	✓											
	18	✓											
	19	✓											
	20	✓											
	21	✓											
	22	✓											
	23	✓											
	24	✓											
	25	✓											
	26	✓											
	27	✓											
	28	✓											
	29	✓											
	30	✓											
	31	✓											
	32	✓											
	33	✓											
	34	✓											
	35	✓											
	36	✓											
	37	✓											
	38	✓											
	39	✓											
	40	✓											
	41	✓											
	42	✓											
	43	✓											
	44	✓											
	45	✓											
	46	✓											
	47	✓											
	48	✓											
	49	✓											
	50	✓											

Claim		Date											
Final	Original												
	51	✓											
	52	✓											
	53	✓											
	54	✓											
	55	✓											
	56	✓											
	57	✓											
	58	✓											
	59	✓											
	60	✓											
	61	✓											
	62	✓											
	63	✓											
	64	✓											
	65	✓											
	66	✓											
	67	✓											
	68	✓											
	69	✓											
	70	✓											
	71	✓											
	72	✓											
	73	✓											
	74	✓											
	75	✓											
	76	✓											
	77	✓											
	78	✓											
	79	✓											
	80	✓											
	81	✓											
	82	✓											
	83	✓											
	84	✓											
	85	✓											
	86	✓											
	87	✓											
	88	✓											
	89	✓											
	90	✓											
	91	✓											
	92	✓											
	93	✓											
	94	✓											
	95	✓											
	96	✓											
	97	✓											
	98	✓											
	99	✓											
	100	✓											

Claim		Date											
Final	Original												
	101	✓											
	102	✓											
	103	✓											
	104	✓											
	105	✓											
	106	✓											
	107	✓											
	108	✓											
	109	✓											
	110												
	111												
	112												
	113												
	114												
	115												
	116												
	117												
	118												
	119												
	120												
	121												
	122												
	123												
	124												
	125												
	126												
	127												
	128												
	129												
	130												
	131												
	132												
	133												
	134												
	135												
	136												
	137												
	138												
	139												
	140												
	141												
	142												
	143												
	144												
	145												
	146												
	147												
	148												
	149												
	150												

Search Notes

Application/Control No.

10/403,818

Examiner

Douglas B. Blair

Applicant(s)/Patent under
Reexamination

ALKHATIB ET AL.

Art Unit

2142

SEARCHED

Class	Subclass	Date	Examiner
709	245	9/14/2006	DBB

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

**SEARCH NOTES
(INCLUDING SEARCH STRATEGY)**

	DATE	EXMR
east text search	9/14/2006	DBB
Inventor name search	9/14/2006	DBB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application	)	<u>PATENT APPLICATION</u>
	)	
Inventors: Alkhatib	)	
	)	Art Unit: 2142
Application No.: 10/403,818	)	
	)	Examiner: Blair, Douglas B.
Filed: March 31, 2003	)	
	)	Customer No. 28554
Title: SECURE VIRTUAL COMMUNITY	)	
NETWORK SYSTEM	)	

RESPONSE A TO OFFICE ACTION UNDER 37 C.F.R. §1.111

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

Sir:

This RESPONSE is in reply to the Office Action mailed September 22, 2006.

AMENDMENTS TO THE SPECIFICATION begin on page 2.

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begin on page 3.

REMARKS begin on page 19.

Applicants hereby petition for a three-month extension of time to extend the time for responding from December 22, 2006 to March 22, 2007. Payment of the appropriate small entity fee is enclosed.

AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph at page 20, lines 3-18 as follows:

Device M_B is in a private domain (e.g. private network)) 540 and connected to a NAT Device ~~515~~ 530 to access the Internet 506 by a private network path 540a. Device M_B may use have a dynamic or static IP address specific to the private domain 540. Generally, such addresses are part of the private received IP classes which are not routable via the Internet. For example, 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255 are network addresses classified for private networks. Firewall/NAT device 515 translates Machine M_B's private IP address to a routable public IP address. NAT device 515 may include other security functions as well. M_B communicates with other non-VCN devices on the Internet via the NAT device 515, and with other members of the VCN via Private Route Director (PRD) 530, which is coupled to the private network path 540a and is a member of the private network 540. Device M_X is also shown as connected to and a member of the private domain 540 but has a static, routable public IP addresses. As such it may communicate with devices coupled to Internet 506 in a different manner, as illustrated in Fig. 5B.

Please amend the paragraph at page 21, lines 16-20 as follows:

As described herein, three forms of communication are used in creating and implementing the VCN. TCP is used in the registration and joining processes; encapsulated UDP ~~UCP~~ packets are used between elements in establishing communication between joined devices and for management traffic, and Encrypted UDP ~~UCP~~ packets are used for agent-to-agent communications.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (currently amended) A virtual community network system, comprising:
a virtual network manager including a definition of at least one virtual community, the definition comprising at least a domain name and a user set, the virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community, the users are identified by one another in the virtual community by their virtual network addresses, and the virtual network addresses are not directly routable; and
at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users.
2. (currently amended) The system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one associated agent.
3. (currently amended) The system of claim 2 wherein, for each user, the associated agent is installed on a processing device.
4. (currently amended) The system of claim 2 wherein, for each user, the associated agent is installed on an associated a-proxy device which is a proxy for the user with respect to the virtual network manager and the at least one route director.
5. (currently amended) The system of claim 2 wherein the virtual network manager detects a presence of ~~includes a~~ NAT device ~~detector~~ when an agent ~~for agents~~ installed in a private network on a processing device behind the a-NAT device contacts the virtual network manager in an attempt to join the virtual community.
6. (currently amended) The system of claim 1 wherein the virtual network manager comprises a device coupled to a public network and having a public network address.

7. (original) The system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device.

8. (currently amended) The system of claim 7 wherein each said processing device is configured with the virtual network address provided to the associated user ~~includes at least one virtual address in the community~~ and at least one physical address.

9. (currently amended) The system of claim 8 wherein the physical addresses are ~~address is~~ dynamic.

10. (currently amended) The system of claim 8 wherein the physical addresses are ~~address is~~ static.

11. (currently amended) The system of claim 8 wherein the physical ~~address is~~ addresses are private network addresses, and the virtual network addresses are unique in the virtual community and do not conflict with the private network addresses.

12. (currently amended) The system of claim 8 wherein ~~at least one of~~ said first processing device ~~or second device~~ is coupled to a first private network and accesses a public network via a first NAT device, the first NAT device transmits packets in which a destination address is a public address of the at least one route director, and the packets include encapsulated packets provided by the first processing device in which a source address is the virtual network address of the first processing device, a destination address is the virtual network address of the second processing device and a shim includes the physical address of the first processing devices as a private network address in the first private network.

13. (currently amended) The system of claim 12 wherein the physical addresses are ~~address is~~ dynamic.

14. (currently amended) The system of claim 12 wherein the physical addresses are address-is-static.

15. (currently amended) The system of claim 12 wherein said ~~first device is coupled to said first private network, and said second~~ processing device is coupled to a second private network and accesses the public network via a second NAT device, the shim includes the physical address of the second processing device as a private network address in the second private network.

16. (currently amended) The system of claim 15 wherein said second device includes ~~at least one virtual address in the realm and~~ at least one private physical address.

17. (original) The system of claim 15 wherein the physical address is dynamic.

18. (original) The system of claim 15 wherein the physical address is static.

19. (currently amended) The system of claim 15 wherein said ~~at least~~ first private network and said ~~at least~~ second private network share at least one network address.

20. (currently amended) The system of claim 1 wherein the route director provides includes a pseudo address assignment for at least one user in the user set when the at least one user communicates with the route director via a NAT device, the route director stores an association of the pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. (original) The system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm.

22. (original) The system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address.

23. (original) The system of claim 22 wherein the route director is coupled to said public network and includes a public network address.

24. (original) The system of claim 22 wherein the route director is coupled to a first private network and said route director includes a private network address.

25. (currently amended) The system of claim 1 wherein communications between users in the user set include packets having a source address which is the virtual network address of the sending user and a destination address which is the virtual network address of the receiving user, the packets are encapsulated and sent to the at least one route director in packets having a destination address which is a public network address of the at least one route director.

26. (currently amended) The system of claim 1 wherein packets communicated ~~communications~~ between users in the user set are encrypted prior to being encapsulated.

27. (original) The system of claim 26 wherein said encryption uses IPSEC.

28. (currently amended) The system of claim 26 wherein said encryption uses DES or triple DES.

29. (currently amended) The system of claim ~~5~~ 26 wherein the virtual network manager detects the presence of the NAT device by receiving a message from the agent when the agent contacts the virtual network manager in the attempt to join the virtual community, and comparing a field in a payload of the message with a source address in a header of the message.

30. (currently amended) The system of claim 1 wherein the virtual network manager includes at least ~~two a second-virtual domain-community definitions~~ definition.

31. _____ (currently amended) The system of claim 1 further including ~~at least a first~~ public route director and a ~~second~~ private route director for routing messages among the users, the public route director is in a public network, and the private route director is in a private network to enable access to users inside the private network from users outside the private network.

32. (currently amended) A system, comprising:
a management device for a virtual community, the management device including a network interface coupled to a public address realm and having a public address; and
a ~~virtual community~~ network traffic router which uses router data to route traffic between members of the virtual community, the ~~;~~ ~~and~~ router data including at least one association of a logical identifier with public routing information for a member.

33. (currently amended) The system of claim 32 wherein the network traffic router includes a network interface accessible to the members by a public address in the public address realm.

34. (currently amended) The system of claim 32 wherein the management device includes a UDP port capable of receiving network traffic of the virtual community ~~network traffic.~~

35. (currently amended) The system of claim ~~34~~ 32 wherein the management device includes a TCP port capable of communicating ~~virtual community~~ network traffic in the virtual community to allow the members to register and join in the virtual community.

36. (currently amended) The system of claim 32 wherein a first member accesses a physical network via a processing device and the system further includes at least one agent installed on the processing device, the at least one agent communicates with the network traffic router to allow the first member to communicate with another member.

37. (original) The system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router includes a

transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent.

38. (currently amended) The system of claim 32 further including at least one proxy agent on a private physical network communicating with at least one of the members ~~a member~~ and the network traffic router, the proxy agent is a proxy for the at least one of members with respect to the network traffic router.

39. (currently amended) The system of claim 38 wherein the at least one of the members ~~member~~ accesses other members using a device coupled to a private physical network.

40. (currently amended) The system of claim 32 wherein the management device ~~manager~~ includes a member register module which allows a potential member to register with the management device.

41. (currently amended) The system of claim 40 wherein the management device ~~manager~~ includes a member join module which allows a particular member to notify the management device via a join request that the particular member is available to participate in the virtual community, and to notify the management device via a leave request that the particular member is no longer available to participate in the virtual community.

42. (currently amended) The system of claim 41 wherein the join module provides a virtual network addresses ~~address to the a registered member~~ members.

43. (currently amended) The system of claim 41 wherein the management device ~~manager~~ maintains data on an association between at least one virtual network address and ~~with~~ at least one member.

44. (currently amended) The system of claim 40 wherein the management device ~~manager~~ includes a DNS server for the virtual community, a first member in the virtual community communicates with another member in the virtual community by querying the DNS

server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router.

45. (currently amended) The system of claim 32 further including a virtual community network communication agent for a device used by a member to communicate in the virtual community, the virtual community network communication agent comprising a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via ~~their~~ associated virtual network addresses ~~address~~.

46. (currently amended) The system of claim 45 wherein the virtual community network communication agent includes a domain name routing plugin.

47. (currently amended) The system of claim 45 wherein the virtual community network communication agent includes a separate IP stack for each member ~~user in the user set~~ accessing the device.

48. (currently amended) The system of claim 45 wherein the virtual network adapter is a deterministic network enhancer.

49. (currently amended) The system of claim 45 wherein the virtual network adapter includes a DNS plugin which processes DNS queries.

50. (currently amended) The system of claim 45 wherein the virtual network adapter includes an IPSEC plugin for encrypting messages.

51. (currently amended) The system of claim 45 wherein the virtual network adapter includes a domain name routing plugin.

52. (currently amended) The system of claim 45 wherein the virtual community network communication agent includes a community registration module for registering the members with the management device.

53. (currently amended) A virtual community network system, comprising:
a ~~virtual community~~ network manager of a virtual community;
a route director;
at least a first virtual community agent associated with a first community member;
and

at least a second virtual community agent associated with at least a second community member, the route director routes communications between the first and second community members via the first and second virtual community agents.

54. (currently amended) The system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address by which the first and second virtual community agents communicate with the network route director.

55. (original) The system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private physical network address.

56. (currently amended) The system of claim 53 wherein the first ~~or second~~ virtual community network agent is installed on a device used by the first community ~~a member~~ to access a network.

57. (currently amended) The system of claim 56 wherein the device is in a private physical network and has an associated private network address for communicating within the private physical network, the device also has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent from outside the private physical network.

58. (currently amended) The system of claim 56 wherein the device is coupled to a public physical network, has an associated public network address for communicating within the

public physical network and has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent.

59. (currently amended) The system of claim 53 wherein the first ~~or second~~ virtual community network agent is a proxy agent for the first community member with respect to the network manager and the route director.

60. (original) The system of claim 53 wherein the first and second members access the virtual community via devices coupled to separate private address physical realms.

61. (original) The system of claim 53 wherein the virtual community network manager includes at least a first community definition and a second community definition.

62. (currently amended) The system of claim 53 wherein the community network manager includes a member authenticator for authenticating potential members when the potential members request to register with the network manager.

63. (currently amended) The system of claim 62 wherein the ~~community~~ network manager includes a DNS server providing ~~authorative~~ authoritative responses for DNS queries in the virtual community, the first virtual community agent provides a DNS query to the DNS server to obtain the virtual network address of the second community member for use in communicating with the second community member.

64. (currently amended) A method for providing a secure virtual network, comprising:

providing a virtual network manager coupled to a public network;

defining a member set of users entitled to communicate in the virtual network;

registering members with the manager;

assigning members ~~a~~ respective virtual addresses which address, are not directly routable;

and

routing network traffic between the members in a ~~the~~ virtual community.

65. (original) The method of claim 64 further including the step of providing users in said member set with a communication agent.

66. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing a proxy agent.

67. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing an agent installed on a device used by the member to couple to a network.

68. (original) The method of claim 65 wherein the step of registering comprises authenticating members with the member set.

69. (currently amended) The method of claim 64 wherein the step of defining a member set includes the step of assigning a domain name for the virtual community.

70. (original) The method of claim 64 wherein the step of defining a member set includes defining at least two member sets having at least one different member.

71. (original) The method of claim 64 wherein the step of assigning a virtual address includes assigning an IPV4 compliant address.

72. (original) The method of claim 71 wherein the step of assigning a virtual address includes assigning a non-routable IPV4 compliant address.

73. (currently amended) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address to with a second member accessing the public network on a second device having a different public address, the traffic includes packets having a source address which is the virtual address of the first member and a destination address which is the virtual

address of the second member, the packets are encapsulated in packets having a source address which is the public address of the first device and a destination address which is the different public address of the second device.

74. (currently amended) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address ~~with~~to a second member accessing the public network on a second device having a public address, the traffic includes packets having a source address which is the virtual address of the first member, a destination address which is the virtual address of the second member, and a shim which includes the private address, the packets are encapsulated in packets having a destination address which is the public address of the second device.

75. (currently amended) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address ~~to with~~to a second member accessing the public network on a device in a private physical network having a second private physical address, the traffic includes encapsulated packets having a source address which is the virtual network address of the first member, a destination address which is the virtual network address of the second member, and a shim which includes the first and second private physical addresses.

76. (original) The method of claim 75 wherein the first private physical address and the second private physical address are identical.

77. (original) The method of claim 64 further including the step of responding to DNS requests for members in the virtual network.

78. (currently amended) The method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network, a first registered member provides a joined status request as a query to the virtual network manager

regarding a status of a second registered member, the status indicating whether or not the second registered member is joined to the virtual community and therefore available to participate in the virtual community.

79. (original) The method of claim 64 further including applying a group policy to members of the virtual community.

80. (currently amended) One or more processor readable storage devices having processor readable code embodied thereon ~~on said processor readable storage devices~~, said processor readable code for programming one or more processors to perform a method comprising the steps of:

managing a virtual community network realm;
defining a member set of users entitled to communicate in the virtual community;
registering users with the virtual community to allow the users to communicate with one another;
assigning each user a virtual address; and
routing network traffic between the users in the virtual community.

81. (original) One or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent.

82. (original) One or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent.

83 (original) One or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community.

84. (currently amended) One or more processor readable storage devices as defined in claim 80 wherein the ~~step of assigning a~~ virtual address includes a non-routable IPV4 compliant address.

85. (currently amended) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device having a public address ~~with~~to a second member accessing the public address realm on a second device having a different public address.

86. (currently amended) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address ~~with~~to a second member accessing the public address realm on a second device having a public address.

87. (currently amended) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address ~~with~~to a second member accessing the public address realm on a device in a private physical network having a second private physical address.

88. (original) One or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device.

89. (original) One or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical.

90. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic.

91. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic.

92. (original) One or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community.

93. (currently amended) A virtual community network system, comprising:
a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set, the network being ~~assessable~~accessible by users in the user set and users outside the user set, the manager exchanging virtual community network information with users in the user set.

94. (original) The system of claim 93 wherein the virtual network manager includes a member register module.

95. (original) The system of claim 93 wherein the virtual network manager includes a member join module.

96. (original) The system of claim 95 wherein the join module provides a virtual address to a registered member.

97. (original) The system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member.

98. (original) The system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community.

99. (original) The system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device.

100. (currently amended) The system of claim 93 wherein the virtual network manager includes at least a second virtual ~~domain~~ community definition.

101. (cancelled)

102. (original) The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. (currently amended) The system of claim 93 wherein the virtual network manager includes a DNS server providing authoritative ~~authoritative~~ responses for DNS queries from users in the virtual community.

104. (currently amended) The system of claim 93 ~~wherein the system further comprising~~ includes at least one route director capable of communicating with users in the user set.

105. (original) The system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent.

106. (currently amended) The system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the virtual community using at least a first processing device, said second user accesses other users in the virtual community using at least a second processing device, wherein at least one of said first device and said ~~or~~ second device is coupled to a first private network and accesses a public network via a NAT device.

107. (original) The system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. (original) The system of claim 93 wherein communications between users in the user set are encrypted.

109. (original) The system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications.

REMARKS

The above Amendments and these Remarks are in reply to the Office Action mailed September 22, 2006

Currently, claims 1-109 are pending. Claims 1-6, 8-16, 19, 20, 25, 26, 28, 29, 30-36, 38-54, 56-59, 62-64, 69, 73-75, 78-80, 84-87, 93, 100, 103, 104 and 106. No new matter is entered. Claim 101 is cancelled.

Claims 1-109 have been rejected under 35 U.S.C. 102 as being anticipated by Cheline et al. (US2003/0041136) (Cheline). Applicants respectfully traverse the rejection.

Cheline is concerned with automatically configuring a virtual private network (VPN). A VPN provides a secure tunnel between a server side system 130 and a client side system 108 (Fig. 1). In this approach, a service provider system 146 provides instructions to configure and control a modem 106 at the client side system 108 and a VPN concentrator 136 at the server side system 130 to provide a VPN tunnel between the modem and the VPN concentrator (par. 31, 33 and 42). The modem can also provide network address translation (NAT) (par. 47). This approach allows a number of client computers in a LAN 104 on the client side system 108 to communicate with the server side system 130 via the VPN tunnel.

However, Applicants' invention differs from Cheline's system in many important aspects. For example, claim 1 sets forth a virtual community network system which includes a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set. Cheline resolves host names in a VPN using multiple DNS servers so that a client knows whether to communicate with an internal DNS Server, which contains private IP addresses, or an external DNS Server, which contains public IP addresses (par. 87 and 88). However, this is not the same as providing a virtual community definition, that is, a definition of a virtual community, which includes a domain name. The fact that Cheline resolves a host name is different than using a domain name as part of a definition of a virtual community.

Further, claim 1 sets forth that a virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community, the users are identified by one another in the virtual community by their virtual network addresses and the virtual network addresses are not directly routable. In Cheline's system, a user's client computer uses either a corporate assigned IP address that can be routed within the server side system, or a private non-routable IP address which is translated using NAT to assume a corporate assigned IP

address (par. 51). The corporate assigned IP address that can be routed is not a virtual network address that is not directly routable. Further, the private non-routable IP address is not a virtual address by which users are identified by one another in a virtual community. Moreover, there is no indication that such an IP address is provided by a virtual network manager when the user joins a virtual community.

In view of the above, claim 1 is clearly patentable over the cited reference.

Further, the dependent claims of claim 1 provide further patentable features. For example, claim 5 sets forth that a virtual network manager detects a presence of a NAT device when an agent installed in a private network on a processing device behind the NAT device contacts the virtual network manager in an attempt to join the virtual community. Even if, arguendo, the modem 106 of Cheline is a NAT device and the VPN provider can receive communications from the NAT device, the VPN provider does not know, and does not detect, if the communication is from behind the NAT device.

The specific technique used to detect the presence of a NAT device as set forth in claim 29 similarly is neither disclosed nor suggested by Cheline.

Further, claim 8 sets forth that processing devices of the users in the virtual community are configured with both a virtual network address and a physical address. In contrast, Cheline indicates that a user's client computer uses either a corporate assigned IP address or a private non-routable IP address (par. 51). There is no indication that the user's client computer is configured with a virtual network address and a physical address, e.g., where the users are identified by one another in the virtual community by their virtual network addresses. Cheline does not provide both types of addresses to the clients 102.

Claim 12 sets forth details of how a first NAT device associated with a first processing device on a first private network transmits packets to a second processing device. The first NAT device transmits packets to a route director, and the packets include encapsulated packets provided by the first processing device in which a source address is the virtual network address of the first processing device, a destination address is the virtual network address of the second processing device and a shim includes the physical address of the first processing devices as a private network address in the first private network. Cheline fails to disclose or suggest this feature.

Claim 15, which depends on claim 12, sets forth that the second processing device is coupled to a second private network and accesses a public network via a second NAT device. In this case, the shim also includes the physical address of the second processing devices as a private network address in the second private network. Cheline is not concerned with processing devices in different private networks communicating in this manner. Instead, Cheline is concerned with clients 102 on a common LAN at client side system 108 communicating with a server side system 130 via a VPN. The clients 102 on the LAN do not communicate with clients on another private network

The remaining dependent claims of claim 1 are similarly patentable over Cheline.

Regarding independent claim 32, the client 102 of Cheline can hardly be considered to be a management device for a virtual community since the client does not perform any managing as claimed. Further, while each client can have an IP address which can be routed through the server side system (par. 51), the clients do not include a network interface coupled to a public address realm. Moreover, the Examiner asserts that the service provider system 146 is a network traffic router as claimed. However, the service provider system 146 is used for providing instructions to configure and control a modem 106 at the client side system 108 and a VPN concentrator 136 at the server side system 130 to provide a VPN tunnel (par. 31, 33 and 42). There is no disclosure or suggestion that the service provider system 146 routes traffic between members of a virtual community as claimed. Moreover, there is no need for the service provider system to route traffic as claimed since the client side system and the server side system communicate directly via the VPN tunnel.

Claim 32 is therefore clearly patentable over Cheline.

Further, the dependent claims of claim 32 provide additional patentable features. For example, regarding claim 35, the client of Cheline is not a management device with a TCP port capable of communicating network traffic in a virtual community to allow members of the virtual community to register and join in the virtual community. The client of Cheline is also not involved with allowing other members of the virtual community to register and join in the virtual community.

Regarding claim 41, Cheline at par. 67 and 68 refers to a client requesting the initiation of a VPN session. However, Cheline does not disclose or suggest that a management device includes a member join module which allows a particular member to notify the management

device via a join request that the particular member is available to participate in the virtual community, and to notify the management device via a leave request that the particular member is no longer available to participate in the virtual community.

Regarding claim 44, Cheline resolves host names in a VPN using multiple DNS servers so that a client knows whether to communicate with an internal DNS Server or an external DNS Server (par. 87 and 88). However, Cheline does not disclose or suggest the features of claim 44 as amended. For example, the client 102(1) of Cheline does not communicate with the DNS server 120 to obtain a virtual network address and private network address of another client such as client 102(2) and to obtain a public network address of the service provider system 146, which is asserted by the Examiner to be a network traffic router as claimed.

The remaining dependent claims of claim 32 are similarly patentable over Cheline.

Regarding independent claim 53, Cheline at par. 86 states that multiple VPNs can be established over a single modem, thus avoiding the need for multiple modems. Cheline indicates that previously, separate modems and telephone lines were need for two clients to communicate via separate VPN tunnels. For example, a husband would communicate with his office via one modem and VPN tunnel, and a wife would communicate with her office via another modem and VPN tunnel (par. 7). Thus, the husband and wife as clients would not be part of the same community. In contrast, claim 53 sets forth routing communications between first and second community members in a community.

Claim 53 and its dependent claims are therefore clearly patentable over Cheline.

Independent claims 64 sets forth, in part, assigning members a respective virtual address, where the virtual addresses are not directly routable, and routing network traffic between the members in a virtual community. Cheline at par. 55 refers to using a DHCP server to allow network administrators to assign IP addresses to client computers. However, these addresses are not virtual addresses which are not directly routable.

Claim 64 and its dependent claims are therefore clearly patentable over Cheline.

Independent claim 80 sets forth, in part, managing a virtual community network realm, defining a member set of users entitled to communicate in the virtual community, and registering users with the virtual community to allow the users to communicate with one another. In contrast, as discussed, Cheline is only concerned with enabling clients to communicate via one or more VPN tunnels with a server, but not with other clients (par. 67).

Claim 80 and its dependent claims are therefore clearly patentable over Cheline.

Claim 93 sets forth, in part, a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set. As discussed above in connection with claim 1, Cheline resolves host names in a VPN using multiple DNS servers so that a client knows whether to communicate with an internal DNS Server or an external DNS Server (par. 87 and 88). However, this is not the same as providing a virtual community definition, that is, a definition of a virtual community, which includes a domain name. The fact that Cheline resolves a host name is different than using a domain name as part of a definition of a virtual community.

Claim 93 and its dependent claims are therefore clearly patentable over Cheline.

Based on the above amendments and these remarks, reconsideration of claims is respectfully requested.

The Examiner's prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: March 22, 2007

By: /Ralph F. Hoppin/
Ralph F. Hoppin
Reg. No. 38,494

VIERRA MAGEN MARCUS & DENIRO LLP
575 Market Street, Suite 2500
San Francisco, California 94105-4206
Telephone: (415) 369-9660
Facsimile: (415) 369-9665

Electronic Patent Application Fee Transmittal					
Application Number:		10403818			
Filing Date:		31-Mar-2003			
Title of Invention:		Secure virtual community network system			
First Named Inventor/Applicant Name:		Hasan S. Alkhatib			
Filer:		Ralph Hoppin			
Attorney Docket Number:		TTCC-01021US0			
Filed as Small Entity					
Utility Filing Fees					
Description		Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					
Extension - 3 months with \$0 paid		2253	1	510	510

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				510

Electronic Acknowledgement Receipt	
EFS ID:	1614156
Application Number:	10403818
International Application Number:	
Confirmation Number:	2698
Title of Invention:	Secure virtual community network system
First Named Inventor/Applicant Name:	Hasan S. Alkhatib
Customer Number:	28554
Filer:	Ralph Hoppin
Filer Authorized By:	
Attorney Docket Number:	TTCC-01021US0
Receipt Date:	22-MAR-2007
Filing Date:	31-MAR-2003
Time Stamp:	11:13:35
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 510
RAM confirmation Number	1533
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	------------------	------------------	------------------

1		1021-response-001.pdf	114767	yes	23
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment - After Non-Final Rejection		1	1	
	Specification		2	2	
	Claims		3	18	
	Applicant Arguments/Remarks Made in an Amendment		19	23	
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8134	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			122901		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 10/403,818		Filing Date 03/31/2003		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY ☒ OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		X \$	=		X \$	=
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=		X \$	=
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	03/22/2007	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
Total (37 CFR 1.16(i))	*	108	Minus	** 109	= 0	X \$25 =	0	OR	X \$ =	
Independent (37 CFR 1.16(h))	*	6	Minus	***6	= 0	X \$100 =	0	OR	X \$ =	
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
Total (37 CFR 1.16(i))	*		Minus	**	=	X \$ =		OR	X \$ =	
Independent (37 CFR 1.16(h))	*		Minus	***	=	X \$ =		OR	X \$ =	
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
Jacquelyn L. Williams

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	33	"virtual community" near2 network\$2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:48
S2	19	S1 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:09
S3	5	S2 and ((private or public) with address)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:00
S4	45	((virtual near (community or network)) and (private near address\$3) and (public near address\$3) and (IP near address\$2))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:04
S5	27	S4 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/13 20:04
S6	53	("6226751").URPN.	USPAT	OR	OFF	2006/09/13 20:30
S7	1	"20040249911".pn.	US-PGPUB; USPAT	OR	OFF	2006/09/14 09:59
S8	139	("domain name" or DNS) with (VPN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:08
S9	74	S8 and @ad<"20030331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 10:09
S10	22	S9 and (NAT with (public or private))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:59

EAST Search History

S11	1801	709/245.ccls:	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/14 11:02
S12	454	"virtual community"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:49
S13	353	router same (public with address\$3) same (private with address\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:50
S14	353	S13 same S13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:50
S15	0	S12 same S13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:50
S16	3	S12 and S13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:50
S17	0	S16 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:51
S18	387	router same (public with address\$3) and router same (private with address\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:50
S19	260	S18 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:52
S20	0	S19 and S12	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:51

EAST Search History

S21	306	rout\$3 with (public near address\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:51
S22	0	S12 same S21	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:52
S23	3	S12 and S21	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:52
S24	0	S23 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:55
S25	1	S12 same public near address\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:53
S26	0	S12 same (rout\$3 with internet)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:53
S27	1	S12 same private near address\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:54
S28	15	(community or group) same S13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:54
S29	7	S28 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 12:59
S30	85	((group or community) with (member\$4 or belong\$3)) and (NAT with (public or private))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:00

EAST Search History

S31	49	S30 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:01
S32	55	((group or community) with (member\$4 or belong\$3)) and ((group\$1 or community) same rout\$3) and (NAT with (public or private))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:25
S33	34	S32 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:27
S34	272055	((group or community) with (member\$4 or belong\$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:25
S35	6111	S34 same server	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:25
S36	124	S35 and ((rout\$3 near2 (messag\$3 or communication\$1)) same (firewall or NAT or private))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:26
S37	68	S36 and (@ad<"20030331" @rlad<"20030331")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:27
S38	35	S37 and "domain name"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/24 13:27
S39	1	"20020152297".pn.	US-PGPUB; USPAT	OR	OFF	2007/05/25 18:47



UNITED STATES PATENT AND TRADEMARK OFFICE

mn
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.
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0	2698

28554 7590 06/05/2007
VIERRA MAGEN MARCUS & DENIRO LLP
575 MARKET STREET SUITE 2500
SAN FRANCISCO, CA 94105

EXAMINER

BLAIR, DOUGLAS B

ART UNIT	PAPER NUMBER
----------	--------------

2142

MAIL DATE	DELIVERY MODE
-----------	---------------

06/05/2007

PAPER

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

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

Office Action Summary

Application No.

10/403,818

Applicant(s)

ALKHATIB ET AL.

Examiner

Douglas B. Blair

Art Unit

2142

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

- 1) ☒ Responsive to communication(s) filed on 22 March 2007.
- 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) 1-100 and 102-109 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-100 and 102-109 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ 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).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

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

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. Claims 1-100 and 102-109 are pending in this application.

Claim Rejections - 35 USC § 102

2. 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 –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 93-100 and 102-109 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication Number 2003/0041136 by Cheline et al.
4. As to claim 93, Cheline teaches a virtual community network system, comprising: a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name **(paragraphs 87-89, an infrastructure for dealing with domain names is clearly defined)** and a user set **(paragraph 43, the users registered with the authentication server are a user set)**, the network being assessable by users in the user set and users outside the user set **(in Figure 1 the VPN is attached to the Internet)**, the manager exchanging virtual community network information with users in the user set **(paragraphs 51-54)**.
5. As to claim 94, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member register module **(paragraphs 43, 47, 51-55, 62-64 and 86-89)**.

Art Unit: 2142

6. As to claim 95, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member join module (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

7. As to claim 96, Cheline teaches the system of claim 95 wherein the join module provides a virtual address to a registered member (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

8. As to claim 97, Cheline teaches the system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

9. As to claim 98, Cheline teaches the system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

10. As to claim 99, Cheline teaches the system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

11. As to claim 100, Cheline teaches the system of claim 93 wherein the virtual network manager includes at least a second virtual domain definition (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

12. As to claim 102, Cheline teaches the system of claim 93 wherein the virtual network manager includes a member authenticator (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

Art Unit: 2142

13. As to claim 103, Cheline teaches the system of claim 93 wherein the virtual network manager includes a DNS server providing authoritative responses for DNS queries from users in the virtual community (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

14. As to claim 104, Cheline teaches the system of claim 93 wherein the system further includes at least one route director capable of communicating with users in the user set (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

15. As to claim 105, Cheline teaches the system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

16. As to claim 106, Cheline teaches the system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device, wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

17. As to claim 107, Cheline teaches the system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

18. As to claim 108, Cheline teaches the system of claim 93 wherein communications between users in the user set are encrypted (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

19. As to claim 109, Cheline teaches the system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications (**paragraphs 43, 47, 51-55, 62-64 and 86-89**).

Claim Rejections - 35 USC § 103

20. 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 negated by the manner in which the invention was made.

21. Claims 1-92 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2003/0041136 by Cheline et al. in view of U.S. Patent Application Publication Number 2004/0006708 to Mukherjee et al.

22. As to claim 1, Cheline teaches a virtual community network system, comprising: a virtual network manager including at least one virtual community definition comprising at least a domain name (**paragraphs 87-89, an infrastructure for dealing with domain names is clearly defined**) and a user set (**paragraph 43, the users registered with the authentication server are a user set**); and at least one route director capable of communicating with users in the user set (**paragraphs 62-64, the modem is considered a route director**); however Cheline does not explicitly teach the users being identified by one another in the virtual community by the virtual network addresses.

Mukherjee teaches a virtual community network system, comprising: a virtual network manager including a definition of at least one virtual community definition (**paragraph**

Art Unit: 2142

47) comprising at least a domain name (**the service provider domain name**) and a user set (**the user group**), the virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community (**paragraph 46**), the users are identified by one another in the virtual community by their virtual network addresses, and the virtual network addresses are not directly routable (**paragraph 56**); and at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users (**paragraph 56**).

It would have been obvious to one of ordinary skill in the Computer Networking art at the time of the invention to combine the teachings of Cheline regarding the implementation of a virtual community with the teachings of Mukherjee regarding users being identified by one another in the virtual community by the virtual network addresses being identified in a virtual community because such identifications provide a more user friendly way to contact fellow group members (**paragraph 47**).

23. As to claim 2, Mukherjee teaches the system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one associated agent (**paragraph 47, the VISA program**).

24. As to claim 3, Mukherjee teaches the system of claim 2 wherein, for each user, the associated agent is installed on a processing device (**paragraph 47**).

25. As to claim 4, Mukherjee teaches the system of claim 2 wherein the agent is installed on an associated proxy device which is proxy for the user with respect to the virtual network manager and the at least one route director (**paragraph 47**).

Art Unit: 2142

26. As to claim 5, Cheline teaches the system of claim 2 wherein the virtual network manager includes a NAT device detector for agents installed on a processing device behind a NAT device (**Figure 2, the modem is NAT device, the VPN provider detects communication from the modem**).

27. As to claim 6, Mukherjee teaches the system of claim 1 wherein the manager comprises a device coupled to a public network and having a public network address (**paragraph 45**).

28. As to claim 7, Mukherjee teaches the system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device (**paragraph 45**).

29. As to claim 8, Mukherjee teaches the system of claim 7 wherein each said device includes at least one virtual address in the community and at least one physical address (**paragraph 45**).

30. As to claim 9, Mukherjee teaches the system of claim 8 wherein the physical address is dynamic (**paragraph 45**).

31. As to claim 10, Mukherjee teaches the system of claim 8 wherein the physical address is static (**paragraph 45**).

32. As to claim 11, Mukherjee teaches the system of claim 8 wherein the physical address is private (**paragraph 45**).

33. As to claim 12, Cheline teaches the system of claim 8 wherein at least one of said first device or second device is coupled to a first private network and accesses a public network via a NAT device **(paragraph 51-54)**.

34. As to claim 13, Cheline teaches the system of claim 12 wherein the physical address is dynamic **(paragraph 51-54)**.

35. As to claim 14, Cheline teaches the system of claim 12 Wherein the physical address is static **(paragraph 51-54)**.

36. As to claim 15, Cheline teaches the system of claim 12 wherein said first, device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device **(paragraph 51-54)**.

37. As to claim 16, Cheline teaches the system of claim 15 wherein said second device includes at least one virtual address in the realm and at least one private physical address **(paragraph 51-54)**.

38. As to claim 17, Cheline teaches the system of claim 15 wherein the physical address is dynamic **(paragraph 51-54)**.

39. As to claim 18, Cheline teaches the system of claim 15 wherein the physical address is static **(paragraph 51-54)**.

40. As to claim 19, Cheline teaches the system of claim 15 wherein said at least first private network and said at least second private network share at least one network address **(paragraph 51-54)**.

41. As to claim 20, Mukherjee teaches the system of claim 1 wherein the route director includes a pseudo address assignment for at least one user in the user set **(paragraph 47)**.

Art Unit: 2142

42. As to claim 21, Mukherjee teaches the system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm **(paragraph 47)**.

43. As to claim 22, Mukherjee teaches the system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address **(paragraph 47)**.

44. As to claim 23, Mukherjee teaches the system of claim 22 wherein the route director is coupled to said public network and includes a public network address **(paragraph 47)**.

45. As to claim 24, Mukherjee teaches the system of claim 22 wherein the route director is coupled to a first private network and said route director includes a private network address **(paragraph 47)**.

46. As to claim 25, Mukherjee teaches the system of claim 1 wherein communications between users in the user set are encapsulated **(paragraph 45)**.

47. As to claim 30, Mukherjee teaches the system of claim 1 wherein the manager includes at least a second virtual domain definition **(paragraph 40-41)**.

48. As to claim 31, Mukherjee teaches the system of claim 1 further including at least a first public route director and a second private route director **(paragraph 40-41)**.

49. As to claims 32-92, they feature limitations found in claims 1-31 and are rejected for the same reasons as claims 1-31.

Response to Arguments

50. Applicant's arguments with respect to claims 1-92 have been considered but are moot in view of the new ground(s) of rejection.

51. Applicant's arguments filed 3/22/2007 with respect to claim 93 and its dependents have been fully considered but they are not persuasive. The Applicant argues that Cheline does not show a virtual community definition that includes a domain name. Instead the Applicant states that Cheline resolves host names in a VPN using multiple DNS server so that the client knows whether to communicate with an internal DNS Server or an external DNS server. However, the Examiner points out that the DNS Server's are considered part of the virtual community definition. Since the DNS Server's include many domain names, the virtual community definition includes domain names. Claim 93 does nothing to specify the relationship between a domain name and the virtual community definition so this interpretation is reasonable given the broad nature of claim 93.

Conclusion

52. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

53. 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,

Art Unit: 2142

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

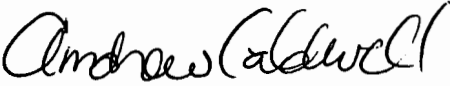
54. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas B. Blair whose telephone number is (571) 272-3893.

The examiner can normally be reached on 9:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Douglas Blair
DBB


ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Notice of References Cited	Application/Control No. 10/403,818	Applicant(s)/Patent Under Reexamination ALKHATIB ET AL.	
	Examiner Douglas B. Blair	Art Unit 2142	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0006708	01-2004	Mukherjee et al.	713/201
*	B	US-2004/0111612	06-2004	Choi et al.	713/163
	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.

Index of Claims



Application/Control No.

10/403,818

Examiner

Douglas B. Blair

Applicant(s)/Patent under
Reexamination

ALKHATIB ET AL.

Art Unit

2142

✓	Rejected
=	Allowed

—	(Through numeral) Cancelled
+	Restricted

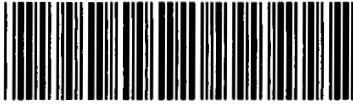
N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date						
Final	Original	9/14/06	5/28/07					
	1	✓	✓					
	2	✓	✓					
	3	✓	✓					
	4	✓	✓					
	5	✓	✓					
	6	✓	✓					
	7	✓	✓					
	8	✓	✓					
	9	✓	✓					
	10	✓	✓					
	11	✓	✓					
	12	✓	✓					
	13	✓	✓					
	14	✓	✓					
	15	✓	✓					
	16	✓	✓					
	17	✓	✓					
	18	✓	✓					
	19	✓	✓					
	20	✓	✓					
	21	✓	✓					
	22	✓	✓					
	23	✓	✓					
	24	✓	✓					
	25	✓	✓					
	26	✓	✓					
	27	✓	✓					
	28	✓	✓					
	29	✓	✓					
	30	✓	✓					
	31	✓	✓					
	32	✓	✓					
	33	✓	✓					
	34	✓	✓					
	35	✓	✓					
	36	✓	✓					
	37	✓	✓					
	38	✓	✓					
	39	✓	✓					
	40	✓	✓					
	41	✓	✓					
	42	✓	✓					
	43	✓	✓					
	44	✓	✓					
	45	✓	✓					
	46	✓	✓					
	47	✓	✓					
	48	✓	✓					
	49	✓	✓					
	50	✓	✓					

Claim		Date						
Final	Original							
	51	✓	✓					
	52	✓	✓					
	53	✓	✓					
	54	✓	✓					
	55	✓	✓					
	56	✓	✓					
	57	✓	✓					
	58	✓	✓					
	59	✓	✓					
	60	✓	✓					
	61	✓	✓					
	62	✓	✓					
	63	✓	✓					
	64	✓	✓					
	65	✓	✓					
	66	✓	✓					
	67	✓	✓					
	68	✓	✓					
	69	✓	✓					
	70	✓	✓					
	71	✓	✓					
	72	✓	✓					
	73	✓	✓					
	74	✓	✓					
	75	✓	✓					
	76	✓	✓					
	77	✓	✓					
	78	✓	✓					
	79	✓	✓					
	80	✓	✓					
	81	✓	✓					
	82	✓	✓					
	83	✓	✓					
	84	✓	✓					
	85	✓	✓					
	86	✓	✓					
	87	✓	✓					
	88	✓	✓					
	89	✓	✓					
	90	✓	✓					
	91	✓	✓					
	92	✓	✓					
	93	✓	✓					
	94	✓	✓					
	95	✓	✓					
	96	✓	✓					
	97	✓	✓					
	98	✓	✓					
	99	✓	✓					
	100	✓	✓					

Claim		Date						
Final	Original							
	101	✓						
	102	✓	✓					
	103	✓	✓					
	104	✓	✓					
	105	✓	✓					
	106	✓	✓					
	107	✓	✓					
	108	✓	✓					
	109	✓	✓					
	110							
	111							
	112							
	113							
	114							
	115							
	116							
	117							
	118							
	119							
	120							
	121							
	122							
	123							
	124							
	125							
	126							
	127							
	128							
	129							
	130							
	131							
	132							
	133							
	134							
	135							
	136							
	137							
	138							
	139							
	140							
	141							
	142							
	143							
	144							
	145							
	146							
	147							
	148							
	149							
	150							

Search Notes

Application/Control No.

10/403,818

Examiner

Douglas B. Blair

Applicant(s)/Patent under
Reexamination

ALKHATIB ET AL.

Art Unit

2142

SEARCHED

Class	Subclass	Date	Examiner
709	245	9/14/2006	DBB
update		5/24/2007	DBB

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

**SEARCH NOTES
(INCLUDING SEARCH STRATEGY)**

	DATE	EXMR
east text search	9/14/2006	DBB
Inventor name search	9/14/2006	DBB
update	5/24/2007	DBB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application	)	<u>PATENT APPLICATION</u>
	)	
Inventors: Alkhatib	)	
	)	Art Unit: 2142
Application No.: 10/403,818	)	
	)	Examiner: Blair, Douglas B.
Filed: March 31, 2003	)	
	)	Customer No. 28554
Title: SECURE VIRTUAL COMMUNITY	)	
NETWORK SYSTEM	)	
_____	)	

RESPONSE B TO OFFICE ACTION UNDER 37 C.F.R. §1.116

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

Sir:

This is a response to the final Office Action mailed June 5, 2007.

A listing of the claims begins on page 2.

Remarks begin on page 17.

Applicants hereby petition for a two-month extension of time to extend the time for responding from September 5, 2007 to November 5, 2007. The appropriate small entity extension fee is enclosed.

LISTING OF THE CLAIMS

A listing of the pending claims is provided below.

1. (previously presented) A virtual community network system, comprising:
a virtual network manager including a definition of at least one virtual community, the definition comprising at least a domain name and a user set, the virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community, the users are identified by one another in the virtual community by their virtual network addresses, and the virtual network addresses are not directly routable; and
at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users.
2. (previously presented) The system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one associated agent.
3. (previously presented) The system of claim 2 wherein, for each user, the associated agent is installed on a processing device.
4. (previously presented) The system of claim 2 wherein, for each user, the associated agent is installed on an associated proxy device which is a proxy for the user with respect to the virtual network manager and the at least one route director.
5. (previously presented) The system of claim 2 wherein the virtual network manager detects a presence of a NAT device when an agent installed in a private network on a processing device behind the NAT device contacts the virtual network manager in an attempt to join the virtual community.
6. (previously presented) The system of claim 1 wherein the virtual network manager comprises a device coupled to a public network and having a public network address.

7. (original) The system of claim 1 wherein the user set includes at least a first user and a second user, said first user accesses other users in the community using at least a first processing device, said second user accesses other users in the community using at least a second processing device.

8. (previously presented) The system of claim 7 wherein each said processing device is configured with the virtual network address provided to the associated user and at least one physical address.

9. (previously presented) The system of claim 8 wherein the physical addresses are dynamic.

10. (previously presented) The system of claim 8 wherein the physical addresses are static.

11. (previously presented) The system of claim 8 wherein the physical addresses are private network addresses, and the virtual network addresses are unique in the virtual community and do not conflict with the private network addresses.

12. (previously presented) The system of claim 8 wherein said first processing device is coupled to a first private network and accesses a public network via a first NAT device, the first NAT device transmits packets in which a destination address is a public address of the at least one route director, and the packets include encapsulated packets provided by the first processing device in which a source address is the virtual network address of the first processing device, a destination address is the virtual network address of the second processing device and a shim includes the physical address of the first processing device as a private network address in the first private network.

13. (previously presented) The system of claim 12 wherein the physical addresses are dynamic.

14. (previously presented) The system of claim 12 wherein the physical addresses are static.

15. (previously presented) The system of claim 12 wherein said second processing device is coupled to a second private network and accesses the public network via a second NAT device, the shim includes the physical address of the second processing device as a private network address in the second private network.

16. (previously presented) The system of claim 15 wherein said second device includes at least one private physical address.

17. (original) The system of claim 15 wherein the physical address is dynamic.

18. (original) The system of claim 15 wherein the physical address is static.

19. (previously presented) The system of claim 15 wherein said first private network and said second private network share at least one network address.

20. (previously presented) The system of claim 1 wherein the route director provides a pseudo address assignment for at least one user in the user set when the at least one user communicates with the route director via a NAT device, the route director stores an association of the pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. (original) The system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm.

22. (original) The system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address.

23. (original) The system of claim 22 wherein the route director is coupled to said public network and includes a public network address.

24. (original) The system of claim 22 wherein the route director is coupled to a first private network and said route director includes a private network address.

25. (previously presented) The system of claim 1 wherein communications between users in the user set include packets having a source address which is the virtual network address of the sending user and a destination address which is the virtual network address of the receiving user, the packets are encapsulated and sent to the at least one route director in packets having a destination address which is a public network address of the at least one route director.

26. (previously presented) The system of claim 1 wherein packets communicated between users in the user set are encrypted prior to being encapsulated.

27. (original) The system of claim 26 wherein said encryption uses IPSEC.

28. (previously presented) The system of claim 26 wherein said encryption uses DES or triple DES.

29. (previously presented) The system of claim 5 wherein the virtual network manager detects the presence of the NAT device by receiving a message from the agent when the agent contacts the virtual network manager in the attempt to join the virtual community, and comparing a field in a payload of the message with a source address in a header of the message.

30. (previously presented) The system of claim 1 wherein the virtual network manager includes at least two virtual community definitions .

31. (previously presented) The system of claim 1 further including a public route director and a private route director for routing messages among the users, the public route

director is in a public network, and the private route director is in a private network to enable access to users inside the private network from users outside the private network.

32. (previously presented) A system, comprising:
a management device for a virtual community, the management device including a network interface coupled to a public address realm and having a public address; and
a network traffic router which uses router data to route traffic between members of the virtual community, the router data including at least one association of a logical identifier with public routing information for a member.

33. (previously presented) The system of claim 32 wherein the network traffic router includes a network interface accessible to the members by a public address in the public address realm.

34. (previously presented) The system of claim 32 wherein the management device includes a UDP port capable of receiving network traffic of the virtual community .

35. (previously presented) The system of claim 34 wherein the management device includes a TCP port capable of communicating network traffic in the virtual community to allow the members to register and join in the virtual community.

36. (previously presented) The system of claim 32 wherein a first member accesses a physical network via a processing device and the system further includes at least one agent installed on the processing device, the at least one agent communicates with the network traffic router to allow the first member to communicate with another member.

37. (original) The system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router includes a transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent.

38. (previously presented) The system of claim 32 further including at least one proxy agent on a private physical network communicating with at least one of the members and the network traffic router, the proxy agent is a proxy for the at least one of members with respect to the network traffic router.

39. (previously presented) The system of claim 38 wherein the at least one of the members accesses other members using a device coupled to a private physical network.

40. (previously presented) The system of claim 32 wherein the management device includes a member register module which allows a potential member to register with the management device.

41. (previously presented) The system of claim 40 wherein the management device includes a member join module which allows a particular member to notify the management device via a join request that the particular member is available to participate in the virtual community, and to notify the management device via a leave request that the particular member is no longer available to participate in the virtual community.

42. (previously presented) The system of claim 41 wherein the join module provides virtual network addresses to the members.

43. (previously presented) The system of claim 41 wherein the management device maintains data on an association between at least one virtual network address and at least one member.

44. (previously presented) The system of claim 40 wherein the management device includes a DNS server for the virtual community, a first member in the virtual community communicates with another member in the virtual community by querying the DNS server to determine a virtual network address and a private network address for the another member, and to determine a public address of the network traffic router.

45. (previously presented) The system of claim 32 further including a virtual community network communication agent for a device used by a member to communicate in the virtual community, the virtual community network communication agent comprising a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via associated virtual network addresses .

46. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a domain name routing plugin.

47. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a separate IP stack for each member accessing the device.

48. (previously presented) The system of claim 45 wherein the virtual network adapter is a deterministic network enhancer.

49. (previously presented) The system of claim 45 wherein the virtual network adapter includes a DNS plugin which processes DNS queries.

50. (previously presented) The system of claim 45 wherein the virtual network adapter includes an IPSEC plugin for encrypting messages.

51. (previously presented) The system of claim 45 wherein the virtual network adapter includes a domain name routing plugin.

52. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a community registration module for registering the members with the management device.

53. (previously presented) A virtual community network system, comprising:
a network manager of a virtual community;

a route director;
at least a first virtual community agent associated with a first community member;
and
at least a second virtual community agent associated with at least a second community member, the route director routes communications between the first and second community members via the first and second virtual community agents.

54. (previously presented) The system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address by which the first and second virtual community agents communicate with the network route director.

55. (original) The system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private physical network address.

56. (previously presented) The system of claim 53 wherein the first virtual community network agent is installed on a device used by the first community member to access a network.

57. (previously presented) The system of claim 56 wherein the device is in a private physical network and has an associated private network address for communicating within the private physical network, the device also has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent from outside the private physical network.

58. (previously presented) The system of claim 56 wherein the device is coupled to a public physical network, has an associated public network address for communicating within the public physical network and has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent.

59. (previously presented) The system of claim 53 wherein the first virtual community network agent is a proxy agent for the first community member with respect to the network manager and the route director.

60. (original) The system of claim 53 wherein the first and second members access the virtual community via devices coupled to separate private address physical realms.

61. (original) The system of claim 53 wherein the virtual community network manager includes at least a first community definition and a second community definition.

62. (previously presented) The system of claim 53 wherein the community network manager includes a member authenticator for authenticating potential members when the potential members request to register with the network manager.

63. (previously presented) The system of claim 62 wherein the network manager includes a DNS server providing authoritative responses for DNS queries in the virtual community, the first virtual community agent provides a DNS query to the DNS server to obtain the virtual network address of the second community member for use in communicating with the second community member .

64. (previously presented) A method for providing a secure virtual network, comprising:

- providing a virtual network manager coupled to a public network;
- defining a member set of users entitled to communicate in the virtual network;
- registering members with the manager;
- assigning members respective virtual addresses which are not directly routable; and
- routing network traffic between the members in a virtual community.

65. (original) The method of claim 64 further including the step of providing users in said member set with a communication agent.

66. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing a proxy agent.

67. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing an agent installed on a device used by the member to couple to a network.

68. (original) The method of claim 65 wherein the step of registering comprises authenticating members with the member set.

69. (previously presented) The method of claim 64 wherein the step of defining a member set includes the step of assigning a domain name for the virtual community.

70. (original) The method of claim 64 wherein the step of defining a member set includes defining at least two member sets having at least one different member.

71. (original) The method of claim 64 wherein the step of assigning a virtual address includes assigning an IPV4 compliant address.

72. (original) The method of claim 71 wherein the step of assigning a virtual address includes assigning a non-routable IPV4 compliant address.

73. (previously presented) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address to a second member accessing the public network on a second device having a different public address, the traffic includes packets having a source address which is the virtual address of the first member and a destination address which is the virtual address of the second member, the packets are encapsulated in packets having a source address which is the public address of the first device and a destination address which is the different public address of the second device.

74. (previously presented) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address to a second member accessing the public network on a second device having a public address, the traffic includes packets having a source address which is the virtual address of the first member, a destination address which is the virtual address of the second member, and a shim which includes the private address, the packets are encapsulated in packets having a destination address which is the public address of the second device.

75. (previously presented) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address to a second member accessing the public network on a device in a private physical network having a second private physical address, the traffic includes encapsulated packets having a source address which is the virtual network address of the first member, a destination address which is the virtual network address of the second member, and a shim which includes the first and second private physical addresses.

76. (original) The method of claim 75 wherein the first private physical address and the second private physical address are identical.

77. (original) The method of claim 64 further including the step of responding to DNS requests for members in the virtual network.

78. (previously presented) The method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network, a first registered member provides a joined status request as a query to the virtual network manager regarding a status of a second registered member, the status indicating whether or not the second registered member is joined to the virtual community and therefore available to participate in the virtual community.

79. (original) The method of claim 64 further including applying a group policy to members of the virtual community.

80. (previously presented) One or more processor readable storage devices having processor readable code embodied thereon, said processor readable code for programming one or more processors to perform a method comprising the steps of:

managing a virtual community network realm;
defining a member set of users entitled to communicate in the virtual community;
registering users with the virtual community to allow the users to communicate with one another;
assigning each user a virtual address; and
routing network traffic between the users in the virtual community.

81. (original) One or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent.

82. (original) One or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent.

83 (original) One or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community.

84. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the virtual address includes a non-routable IPV4 compliant address.

85. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first

member accessing the public address realm on a first device having a public address to a second member accessing the public address realm on a second device having a different public address.

86. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address to a second member accessing the public address realm on a second device having a public address.

87. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address to a second member accessing the public address realm on a device in a private physical network having a second private physical address.

88. (original) One or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device.

89. (original) One or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical.

90. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic.

91. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic.

92. (original) One or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community.

93. (previously presented) A virtual community network system, comprising:
a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set, the network being accessible by users in the user set and users outside the user set, the manager exchanging virtual community network information with users in the user set.

94. (original) The system of claim 93 wherein the virtual network manager includes a member register module.

95. (original) The system of claim 93 wherein the virtual network manager includes a member join module.

96. (original) The system of claim 95 wherein the join module provides a virtual address to a registered member.

97. (original) The system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member.

98. (original) The system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community.

99. (original) The system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device.

100. (previously presented) The system of claim 93 wherein the virtual network manager includes at least a second virtual community definition.

101. (cancelled)

102. (original) The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. (previously presented) The system of claim 93 wherein the virtual network manager includes a DNS server providing authoritative responses for DNS queries from users in the virtual community.

104. (previously presented) The system of claim 93 further comprising at least one route director capable of communicating with users in the user set.

105. (original) The system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent.

106. (previously presented) The system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the virtual community using at least a first processing device, said second user accesses other users in the virtual community using at least a second processing device, wherein at least one of said first device and said second device is coupled to a first private network and accesses a public network via a NAT device.

107. (original) The system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. (original) The system of claim 93 wherein communications between users in the user set are encrypted.

109. (original) The system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications.

REMARKS

This is a response to the final Office Action mailed June 5, 2007.

No claims are amended in this response.

Claims 93-100 and 102-109 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. pub. 2003/0041136 to Cheline et al.

Claims 1-92 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Cheline et al. in view of U.S. pub. 2004/0006708 to Mukherjee et al.

Applicants respectfully traverse on the grounds that the claims have not been properly examined. In particular, it is noted that the Office Action does not address the amended claims in Applicants' amendment filed on March 22, 2007, at least in regard to claims 5, 8, 11, 12, 15, 20, 25, 30 and any claims in claims 32-92 which feature similar limitations. The Office Action instead addresses the corresponding claims as filed. Further, the Office Action does not address claims 26-29 at all.

For example, regarding claim 5, paragraph 26 of the Office Action states: "As to claim 5, Cheline teaches the system of claim 2 wherein the virtual network manager includes a NAT device detector for agents installed on a processing device behind a NAT device..." However, claim 5 as pending states: "The system of claim 1 wherein communications between users in the user set include packets having a source address which is the virtual network address of the sending user and a destination address which is the virtual network address of the receiving user, the packets are encapsulated and sent to the at least one route director in packets having a destination address which is a public network address of the at least one route director." Clearly, the Office Action does not address the pending claims.

As stated in MPEP 2142 (Legal Concept of *Prima Facie* Obviousness), "The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." See also MPEP 706.02(j) (Contents of a 35 U.S.C. 103 Rejection).

In view of this oversight, Applicants do not believe it is appropriate or necessary for them to comment on the substance of the current rejections.

The Office is requested to examine the application based on the amended claims filed on March 22, 2007.

Conclusion

Each of the pending claims is believed to be in condition for immediate allowance. The Examiner is therefore requested to pass this application on to an early issue. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

The Examiner's prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: Nov. 5, 2007

By: /Ralph F. Hoppin/
Ralph F. Hoppin
Reg. No. 38,494

VIERRA MAGEN MARCUS & DENIRO LLP
575 Market Street, Suite 2500
San Francisco, California 94105-4206
Telephone: (415) 369-9660, x214
Facsimile: (415) 369-9665

Electronic Patent Application Fee Transmittal				
Application Number:		10403818		
Filing Date:		31-Mar-2003		
Title of Invention:		Secure virtual community network system		
First Named Inventor/Applicant Name:		Hasan S. Alkhatib		
Filer:		Ralph Hoppin		
Attorney Docket Number:		TTCC-01021US0		
Filed as Small Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	2252	1	230	230

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				230

Electronic Acknowledgement Receipt

EFS ID:	2427030
Application Number:	10403818
International Application Number:	
Confirmation Number:	2698
Title of Invention:	Secure virtual community network system
First Named Inventor/Applicant Name:	Hasan S. Alkhatib
Customer Number:	28554
Filer:	Ralph Hoppin
Filer Authorized By:	
Attorney Docket Number:	TTCC-01021US0
Receipt Date:	05-NOV-2007
Filing Date:	31-MAR-2003
Time Stamp:	18:09:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 230
RAM confirmation Number	2766
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1		1021-response-002.pdf	108899	yes	18						
			ade186ed6b23e2962cfa0ddcb5aa3d9dcb922138								
	Multipart Description/PDF files in .zip description										
	Document Description		Start	End							
	Amendment After Final		1	1							
	Claims		2	16							
	Applicant Arguments/Remarks Made in an Amendment		17	18							
Warnings:											
Information:											
2	Fee Worksheet (PTO-06)	fee-info.pdf	8133	no	2						
			d6763226158c84e3b705523e06d52716aa974670								
Warnings:											
Information:											
Total Files Size (in bytes):			117032								
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.											

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 10/403,818		Filing Date 03/31/2003		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY ☒ OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		X \$	=		X \$	=
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=		X \$	=
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	11/05/2007	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
Total (37 CFR 1.16(i))	* 108	Minus	** 109	= 0	X \$25 =	0	OR	X \$ =		
Independent (37 CFR 1.16(h))	* 8	Minus	***6	= 2	X \$105 =	210	OR	X \$ =		
☐ Application Size Fee (37 CFR 1.16(s))							OR			
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR			
					TOTAL ADD'L FEE	210	OR	TOTAL ADD'L FEE		
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	Total (37 CFR 1.16(i))	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
Independent (37 CFR 1.16(h))	*	Minus	**	=	X \$ =		OR	X \$ =		
☐ Application Size Fee (37 CFR 1.16(s))							OR			
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR			
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
lamont mclaulhlin

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/403,818	03/31/2003	Hasan S. Alkhatib	TTCC-01021US0	2698

28554 7590 11/19/2007
VIERRA MAGEN MARCUS & DENIRO LLP
575 MARKET STREET SUITE 2500
SAN FRANCISCO, CA 94105

EXAMINER

BLAIR, DOUGLAS B

ART UNIT	PAPER NUMBER
----------	--------------

2142

MAIL DATE	DELIVERY MODE
-----------	---------------

11/19/2007

PAPER

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

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

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

10/403,818

Applicant(s)

ALKHATIB ET AL.

Examiner

Douglas B. Blair

Art Unit

2142

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

THE REPLY FILED 05 November 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- 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.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) 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).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, 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: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
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: 1-100 and 102-109.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.
13. ☐ Other: _____.



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Continuation of 11. does NOT place the application in condition for allowance because: The applicant's response cannot place the application in condition for allowance because it does not address the patentability of any of the independent claims.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application) PATENT APPLICATION
Inventors: Alkhatib)
Application No.: 10/403,818) Art Unit: 2142
Filed: March 31, 2003) Examiner: Blair, Douglas B.
Title: SECURE VIRTUAL COMMUNITY) Customer No. 28554
NETWORK SYSTEM)
_____)

RESPONSE B TO OFFICE ACTION UNDER 37 C.F.R. §1.116

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

Sir:

This is a response to the final Office Action mailed June 5, 2007.

A listing of the claims begins on page 2.

Remarks begin on page 17.

Applicants hereby petition for a two-month extension of time to extend the time for responding from September 5, 2007 to November 5, 2007. The appropriate small entity extension fee is enclosed.

- 1 -

Attorney Docket No.: TTCC-01021US0
ttcc/1021/1021.response-002

Please Enter - DBB

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	10403818	Filing Date	2003-03-31	Docket Number (if applicable)	TTCC-01021US0	Art Unit	2142
First Named Inventor	Alkhatib			Examiner Name	Blair, Douglas B.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____.
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 501826

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Ralph F. Hoppin/	Date (YYYY-MM-DD)	2007-12-04
Name	Ralph F. Hoppin	Registration Number	38494

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application	)	<u>PATENT APPLICATION</u>
	)	
Inventors: Alkhatib	)	
	)	Art Unit: 2142
Application No.: 10/403,818	)	
	)	Examiner: Blair, Douglas B.
Filed: March 31, 2003	)	
	)	Customer No. 28554
Title: SECURE VIRTUAL COMMUNITY	)	
NETWORK SYSTEM	)	
_____	)	

RESPONSE C TO OFFICE ACTION WITH RCE UNDER 37 C.F.R. §1.114

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

Sir:

This is a response to the final Office Action mailed June 5, 2007, and supplements the response filed on November 5, 2007.

A listing of the claims begins on page 2.

Remarks begin on page 18.

Applicants hereby petition for a three-month extension of time to extend the time for responding from September 5, 2007 to December 5, 2007. Applicants previously paid the fee for a two-month extension of time. Accordingly, an amount which is the difference between the two- and three-month small entity extension fees is now being paid.

LISTING OF THE CLAIMS

A listing of the pending claims is provided below.

1. (currently amended) A virtual community network system, comprising:
a virtual network manager including a definition of at least one virtual community, the definition comprising at least a domain name and a user set, the virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community, the users are identified by one another in the virtual community by their virtual network addresses, and the virtual network addresses are not directly routable; and
at least one route director capable of communicating with users in the user set, the at least one route director routes traffic between the users, wherein communications between users include encapsulated packets having a source address which is the virtual network address of a first, sending user and a destination address which is the virtual network address of a second, receiving user, and the encapsulated packets are sent to the at least one route director in encapsulating packets having a destination address which is a public network address of the at least one route director.
2. (previously presented) The system of claim 1 wherein each user communicates with the virtual network manager and other users in the user set via at least one associated agent.
3. (previously presented) The system of claim 2 wherein, for each user, the associated agent is installed on a processing device.
4. (previously presented) The system of claim 2 wherein, for each user, the associated agent is installed on an associated proxy device which is a proxy for the user with respect to the virtual network manager and the at least one route director.
5. (previously presented) The system of claim 2 wherein the virtual network manager detects a presence of a NAT device when an agent installed in a private network on a

processing device behind the NAT device contacts the virtual network manager in an attempt to join the virtual community.

6. (previously presented) The system of claim 1 wherein the virtual network manager comprises a device coupled to a public network and having a public network address.

7. (currently amended) The system of claim 1 wherein ~~the user set includes at least a first user and a second user,~~ said first, sending user accesses other users in the community using at least a first processing device, and said second, receiving user accesses other users in the community using at least a second processing device.

8. (previously presented) The system of claim 7 wherein each said processing device is configured with the virtual network address provided to the associated user and at least one physical address.

9. (previously presented) The system of claim 8 wherein the physical addresses are dynamic.

10. (previously presented) The system of claim 8 wherein the physical addresses are static.

11. (previously presented) The system of claim 8 wherein the physical addresses are private network addresses, and the virtual network addresses are unique in the virtual community and do not conflict with the private network addresses.

12. (currently amended) The system of claim 8 wherein said first processing device is coupled to a first private network and accesses a public network via a first NAT device, the first NAT device transmits the encapsulating packets, and the encapsulating packets in which a destination address is a public address of the at least one route director, and the packets include encapsulated packets provided by the first processing device in which a source address is the virtual network address of the first processing device, a destination address is the virtual network

~~address of the second processing device and include~~ a shim which includes the physical address of the first processing device as a private network address in the first private network.

13. (previously presented) The system of claim 12 wherein the physical addresses are dynamic.

14. (previously presented) The system of claim 12 wherein the physical addresses are static.

15. (previously presented) The system of claim 12 wherein said second processing device is coupled to a second private network and accesses the public network via a second NAT device, the shim includes the physical address of the second processing device as a private network address in the second private network.

16. (previously presented) The system of claim 15 wherein said second device includes at least one private physical address.

17. (original) The system of claim 15 wherein the physical address is dynamic.

18. (original) The system of claim 15 wherein the physical address is static.

19. (previously presented) The system of claim 15 wherein said first private network and said second private network share at least one network address.

20. (currently amended) The system of claim 1 wherein the route director provides a user-specific pseudo address assignment for at least one user in the user set when the at least one user communicates with the route director via a NAT device, the route director stores an association of the user-specific pseudo address with a public network address of the NAT device and a port number of the NAT device.

21. (original) The system of claim 1 wherein the route director includes a translator for virtual address information for a virtual user in a private network realm.

22. (original) The system of claim 1 wherein the virtual community manager is coupled to a public network and includes a public network address.

23. (original) The system of claim 22 wherein the route director is coupled to said public network and includes a public network address.

24. (currently amended) The system of claim 22 wherein the route director is coupled to a first private network and ~~said route director~~ includes a private network address.

25. (cancelled)

26. (previously presented) The system of claim 1 wherein packets communicated between users in the user set are encrypted prior to being encapsulated.

27. (original) The system of claim 26 wherein said encryption uses IPSEC.

28. (previously presented) The system of claim 26 wherein said encryption uses DES or triple DES.

29. (previously presented) The system of claim 5 wherein the virtual network manager detects the presence of the NAT device by receiving a message from the agent when the agent contacts the virtual network manager in the attempt to join the virtual community, and comparing a field in a payload of the message with a source address in a header of the message.

30. (previously presented) The system of claim 1 wherein the virtual network manager includes at least two virtual community definitions.

31. (previously presented) The system of claim 1 further including a public route director and a private route director for routing messages among the users, the public route director is in a public network, and the private route director is in a private network to enable access to users inside the private network from users outside the private network.

32. (previously presented) A system, comprising:
a management device for a virtual community, the management device including a network interface coupled to a public address realm and having a public address; and
a network traffic router which uses router data to route traffic between members of the virtual community, the router data including at least one association of a logical identifier with public routing information for a member.

33. (previously presented) The system of claim 32 wherein the network traffic router includes a network interface accessible to the members by a public address in the public address realm.

34. (previously presented) The system of claim 32 wherein the management device includes a UDP port capable of receiving network traffic of the virtual community.

35. (previously presented) The system of claim 34 wherein the management device includes a TCP port capable of communicating network traffic in the virtual community to allow the members to register and join in the virtual community.

36. (previously presented) The system of claim 32 wherein a first member accesses a physical network via a processing device and the system further includes at least one agent installed on the processing device, the at least one agent communicates with the network traffic router to allow the first member to communicate with another member.

37. (original) The system of claim 36 wherein the processing device is coupled to a private physical network behind a NAT device, and the network traffic router includes a

transposer for routing information in a packet destined for the agent to direct the packet to the NAT device for the agent.

38. (previously presented) The system of claim 32 further including at least one proxy agent on a private physical network communicating with at least one of the members and the network traffic router, the proxy agent is a proxy for the at least one of members with respect to the network traffic router.

39. (previously presented) The system of claim 38 wherein the at least one of the members accesses other members using a device coupled to a private physical network.

40. (previously presented) The system of claim 32 wherein the management device includes a member register module which allows a potential member to register with the management device.

41. (previously presented) The system of claim 40 wherein the management device includes a member join module which allows a particular member to notify the management device via a join request that the particular member is available to participate in the virtual community, and to notify the management device via a leave request that the particular member is no longer available to participate in the virtual community.

42. (previously presented) The system of claim 41 wherein the join module provides virtual network addresses to the members.

43. (previously presented) The system of claim 41 wherein the management device maintains data on an association between at least one virtual network address and at least one member.

44. (currently amended) The system of claim 32, 40 wherein each member receives a respective virtual network address when registering with the management device to join the virtual community, the management device includes a DNS server for the virtual community, a

first member in the virtual community communicates with another member in the virtual community by querying the DNS server to determine ~~a virtual network address and a private network~~ and the respective virtual network address for the another member, and to determine a public address of the network traffic router, and the first member communicates with the another member using an encapsulated packet having a source address which is the respective virtual network address of the first member and a destination address which is the respective virtual network address of the another member, by sending the encapsulated packet to the network traffic router in an encapsulating packet having a destination address which is the public address of the network traffic router, the private network address for the another member is included in the encapsulating packet and is used by the network traffic router to route the encapsulated packet to the another member.

45. (previously presented) The system of claim 32 further including a virtual community network communication agent for a device used by a member to communicate in the virtual community, the virtual community network communication agent comprising a virtual network adapter interfacing with the device and applications on the device to route traffic to members of the virtual community via associated virtual network addresses.

46. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a domain name routing plugin.

47. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a separate IP stack for each member accessing the device.

48. (previously presented) The system of claim 45 wherein the virtual network adapter is a deterministic network enhancer.

49. (previously presented) The system of claim 45 wherein the virtual network adapter includes a DNS plugin which processes DNS queries.

50. (previously presented) The system of claim 45 wherein the virtual network adapter includes an IPSEC plugin for encrypting messages.

51. (previously presented) The system of claim 45 wherein the virtual network adapter includes a domain name routing plugin.

52. (previously presented) The system of claim 45 wherein the virtual community network communication agent includes a community registration module for registering the members with the management device.

53. (previously presented) A virtual community network system, comprising:
a network manager of a virtual community;
a route director;
at least a first virtual community agent associated with a first community member;
and
at least a second virtual community agent associated with at least a second community member, the route director routes communications between the first and second community members via the first and second virtual community agents.

54. (previously presented) The system of claim 53 wherein the route director is a network route director, and includes a public network interface and public address by which the first and second virtual community agents communicate with the network route director.

55. (original) The system of claim 53 wherein the route director is a private route director, and includes a private physical network address interface and a private physical network address.

56. (previously presented) The system of claim 53 wherein the first virtual community network agent is installed on a device used by the first community member to access a network.

57. (currently amended) The system of claim 56 wherein the device is in a private physical network, ~~and~~ has an associated private network address for communicating within the private physical network, and the device also has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent from outside the private physical network, the first virtual network address is not directly routable.

58. (previously presented) The system of claim 56 wherein the device is coupled to a public physical network, has an associated public network address for communicating within the public physical network and has a first virtual network address, assigned by the network manager, by which the device can be identified by the second virtual community agent.

59. (previously presented) The system of claim 53 wherein the first virtual community network agent is a proxy agent for the first community member with respect to the network manager and the route director.

60. (original) The system of claim 53 wherein the first and second members access the virtual community via devices coupled to separate private address physical realms.

61. (original) The system of claim 53 wherein the virtual community network manager includes at least a first community definition and a second community definition.

62. (previously presented) The system of claim 53 wherein the community network manager includes a member authenticator for authenticating potential members when the potential members request to register with the network manager.

63. (previously presented) The system of claim 62 wherein the network manager includes a DNS server providing authoritative responses for DNS queries in the virtual community, the first virtual community agent provides a DNS query to the DNS server to obtain the virtual network address of the second community member for use in communicating with the second community member.

64. (currently amended) A method for providing a secure virtual network, comprising:

providing a virtual network manager coupled to a public network;

defining a member set of users entitled to communicate in the virtual network using associated processing devices which each have at least one physical address which is a private network address;

registering members with the manager;

assigning members respective virtual addresses which are not directly routable, the virtual addresses are unique among the members and do not conflict with the private network addresses;

configuring each of said processing devices with the virtual address assigned to the associated member; and

routing network traffic between the members in a virtual community.

65. (original) The method of claim 64 further including the step of providing users in said member set with a communication agent.

66. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing a proxy agent.

67. (original) The method of claim 65 wherein said step of providing users with a communication agent includes providing an agent installed on a device used by the member to couple to a network.

68. (original) The method of claim 65 wherein the step of registering comprises authenticating members with the member set.

69. (previously presented) The method of claim 64 wherein the step of defining a member set includes the step of assigning a domain name for the virtual community.

70. (original) The method of claim 64 wherein the step of defining a member set includes defining at least two member sets having at least one different member.

71. (original) The method of claim 64 wherein the step of assigning a virtual address includes assigning an IPV4 compliant address.

72. (original) The method of claim 71 wherein the step of assigning a virtual address includes assigning a non-routable IPV4 compliant address.

73. (previously presented) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device having a public address to a second member accessing the public network on a second device having a different public address, the traffic includes packets having a source address which is the virtual address of the first member and a destination address which is the virtual address of the second member, the packets are encapsulated in packets having a source address which is the public address of the first device and a destination address which is the different public address of the second device.

74. (previously presented) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a first device in a private physical network having a private address to a second member accessing the public network on a second device having a public address, the traffic includes packets having a source address which is the virtual address of the first member, a destination address which is the virtual address of the second member, and a shim which includes the private address, the packets are encapsulated in packets having a destination address which is the public address of the second device.

75. (currently amended) The method of claim 64 wherein the step of routing network traffic includes routing traffic from a first member accessing the public network on a device in a private physical network having a first private physical address to a second member accessing the public network on a device in a private physical network having a second private physical

address, the traffic includes encapsulated packets having a source address which is the virtual network address of the first member, and a destination address which is the virtual network address of the second member, and the traffic also includes a shim which includes the first and second private physical addresses.

76. (original) The method of claim 75 wherein the first private physical address and the second private physical address are identical.

77. (original) The method of claim 64 further including the step of responding to DNS requests for members in the virtual network.

78. (previously presented) The method of claim 64 further including the step of responding to joined status requests for registered members in the virtual network, a first registered member provides a joined status request as a query to the virtual network manager regarding a status of a second registered member, the status indicating whether or not the second registered member is joined to the virtual community and therefore available to participate in the virtual community.

79. (original) The method of claim 64 further including applying a group policy to members of the virtual community.

80. (currently amended) One or more processor readable storage devices having processor readable code embodied thereon, said processor readable code for programming one or more processors to perform a method comprising the steps of:

managing a virtual community network realm;

defining a member set of users entitled to communicate in the virtual community using associated processing devices which each have at least one physical address which is a private network address;

registering users with the virtual community to allow the users to communicate with one another via the associated processing devices;

assigning each user a virtual address which is not directly routable, the virtual addresses are unique among the users and do not conflict with the private network addresses;

configuring each of said processing devices with the virtual address assigned to the associated user; and

routing network traffic between the users in the virtual community.

81. (original) One or more processor readable storage devices as defined in claim 80 further including code for programming one or more processors to perform a step of providing users in said member set with a communication agent.

82. (original) One or more processor readable storage devices as defined in claim 81 wherein said step of providing users with a communication agent includes providing a proxy agent.

83 (original) One or more processor readable storage devices as defined in claim 80 wherein the step of defining a member set includes the step of assigning a domain name for the community.

84. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the virtual address includes a non-routable IPV4 compliant address.

85. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device having a public address to a second member accessing the public address realm on a second device having a different public address.

86. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a first device in a private physical network having a private address to a second member accessing the public address realm on a second device having a public address.

87. (previously presented) One or more processor readable storage devices as defined in claim 80 wherein the step of routing network traffic includes routing traffic from a first member accessing the public address realm on a device in a private physical network having a first private physical address to a second member accessing the public address realm on a device in a private physical network having a second private physical address.

88. (original) One or more processor readable storage devices as defined in claim 87 wherein the step of routing network traffic includes routing traffic to the first or second member via a NAT device.

89. (original) One or more processor readable storage devices as defined in claim 87 wherein the first private physical address and the second private physical address are identical.

90. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encapsulated traffic.

91. (original) One or more processor readable storage devices as defined in claim 80 wherein the step of routing includes routing encrypted traffic.

92. (original) One or more processor readable storage devices as defined in claim 80 further including applying a group policy to members of the virtual community.

93. (previously presented) A virtual community network system, comprising:
a virtual network manager having a network interface coupled to a network, the manager including at least one virtual community definition comprising at least a domain name and a user set, the network being accessible by users in the user set and users outside the user set, the manager exchanging virtual community network information with users in the user set.

94. (original) The system of claim 93 wherein the virtual network manager includes a member register module.

95. (original) The system of claim 93 wherein the virtual network manager includes a member join module.

96. (original) The system of claim 95 wherein the join module provides a virtual address to a registered member.

97. (original) The system of claim 93 wherein the virtual network manager maintains data on an association between at least one virtual address with at least one member.

98. (original) The system of claim 93 wherein the virtual network manager includes a DNS server for the virtual community.

99. (original) The system of claim 93 wherein the virtual network manager includes a NAT device detector for users connecting with the virtual network manager using a processing device behind a NAT device.

100. (previously presented) The system of claim 93 wherein the virtual network manager includes at least a second virtual community definition.

101. (cancelled)

102. (original) The system of claim 93 wherein the virtual network manager includes a member authenticator.

103. (currently amended) The system of claim 93 wherein the virtual network manager includes a DNS server providing authoritative responses for DNS queries ~~form~~ from users in the virtual community.

104. (previously presented) The system of claim 93 further comprising at least one route director capable of communicating with users in the user set.

105. (original) The system of claim 93 wherein each user communicates with the virtual network manager and other users in the user set via at least one agent.

106. (previously presented) The system of claim 93 wherein the user set includes at least a first user and a second user, said first user accesses other users in the virtual community using at least a first processing device, said second user accesses other users in the virtual community using at least a second processing device, wherein at least one of said first device and said second device is coupled to a first private network and accesses a public network via a NAT device.

107. (original) The system of claim 106 wherein said first device is coupled to said first private network, and said second device is coupled to a second private network and accesses the public network via a second NAT device.

108. (original) The system of claim 93 wherein communications between users in the user set are encrypted.

109. (original) The system of claim 108 wherein the virtual network manager provides a shared secret to users in the user set to establish encrypted communications.

REMARKS

This is a response to the final Office Action mailed June 5, 2007, and supplements the response filed on November 5, 2007.

Claims 1, 7, 12, 20, 24, 44, 57, 64, 75 are 80 are amended. Claim 25 is cancelled. No new matter is presented. Example support for the claims is as follows: claim 1 (former claim 12), claim 7 (amended for consistency with claim 1), claim 12 (amended for consistency with claim 1), claim 20 (step 2135, Fig. 21), claim 24 (amended for conciseness), claim 44 (p.24, line 3 to p.2, line 3; Figs. 6a and 6b), claim 57 (claim 1), claim 64 (claim 11), claim 75 (p.25, line 25 to p.26, line 3) and claim 80 (claim 1).

In Applicants' response of November 5, 2007, it was pointed out that: 1) the Office Action did not address all of the amended claims in Applicants' amendment filed on March 22, 2007, at least in regard to claims 5, 8, 11, 12, 15, 20, 25, 30 and any claims in claims 32-92 which feature similar limitations, 2) the Office Action instead addressed the corresponding claims as filed, and 3) the Office Action did not address claims 26-29 at all. The Examiner is requested to carefully consider the language of each pending claim.

Claims 93-100 and 102-109 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. pub. 2003/0041136 to Cheline et al.

Claims 1-92 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Cheline et al. in view of U.S. pub. 2004/0006708 to Mukherjee et al.

Cheline is concerned with automatically configuring a virtual private network (VPN). A VPN provides a secure tunnel between a server side system 130 and a client side system 108 (Fig. 1). In this approach, a service provider system 146 provides instructions to configure and control a modem 106 at the client side system 108 and a VPN concentrator 136 at the server side system 130 to provide a VPN tunnel between the modem and the VPN concentrator (par. 31, 33 and 42). The modem can also provide network address translation (NAT) (par. 47). This approach allows a number of client computers in a LAN 104 on the client side system 108 to communicate with the server side system 130 via the VPN tunnel.

Mukherjee provides a peer-to-peer virtual private network in which a virtual private host (VPH) is provided for each user device, and each VPH communicates with each user device via a respective tunnel to provide secure communications between user devices. Mukherjee is cited as teaching the use of virtual network addresses to identify users in a virtual community.

However, Applicants' invention differs from the cited references. For example, claim 1 sets forth a virtual community network system which includes a virtual network manager including at least one virtual community definition comprising at least a domain name and a user set. Cheline resolves host names in a VPN using multiple DNS servers so that a client knows whether to communicate with an internal DNS Server, which contains private IP addresses, or an external DNS Server, which contains public IP addresses (par. 87 and 88). However, this is not the same as providing a virtual community definition, that is, a definition of a virtual community, which includes a domain name. The fact that Cheline resolves a host name is different than using a domain name as part of a definition of a virtual community.

Further, claim 1 sets forth that a virtual network manager provides virtual network addresses to users in the user set when the users join the virtual community, the users are identified by one another in the virtual community by their virtual network addresses and the virtual network addresses are not directly routable. Mukherjee provides subnet addresses for a group and host addresses for end user devices (par. 46).

However, neither Cheline nor Mukherjee, taken alone or in combination, suggests or discloses that communications between users include encapsulated packets having a source address which is the virtual network address of a first, sending user and a destination address which is the virtual network address of a second, receiving user. Moreover, the encapsulated packets are sent to at least one route director in encapsulating packets having a destination address which is a public network address of the at least one route director. For example, the host addresses for end user devices in Mukherjee are not used in this way.

In view of the above, claim 1 and its dependent claims are clearly patentable over the cited references.

Further, the dependent claims of claim 1 provide further patentable features. For example, claim 5 sets forth that a virtual network manager detects a presence of a NAT device when an agent installed in a private network on a processing device behind the NAT device contacts the virtual network manager in an attempt to join the virtual community. Even if, arguendo, the modem 106 of Cheline is a NAT device and the VPN provider can receive communications from the NAT device, the VPN provider does not know, and does not detect, if the communication is from behind the NAT device. Moreover, Applicants note that the

comments in the Office Action indicate that the currently pending claim was not examined. The Examiner is requested to carefully consider the language of the claim as pending.

Further, claim 12 sets forth that the first processing device is coupled to a first private network and accesses a public network via a first NAT device, the first NAT device transmits the encapsulating packets, and the encapsulating packets include a shim which includes the physical address of the first processing device as a private network address in the first private network. Neither Cheline nor Mukherjee discloses or suggests the transmission of such packets.

Claim 15, which depends on claim 12, sets forth that the second processing device is coupled to a second private network and accesses a public network via a second NAT device. In this case, the shim also includes the physical address of the second processing devices as a private network address in the second private network. Cheline is not concerned with processing devices in different private networks communicating in this manner. Instead, Cheline is concerned with clients 102 on a common LAN at client side system 108 communicating with a server side system 130 via a VPN. The clients 102 on the LAN do not communicate with clients on another private network. Moreover, Applicants note that the comments in the Office Action indicate that the currently pending claim was not examined. The Examiner is requested to carefully consider the language of the claim as pending.

Claim 20 sets forth that the route director provides a user-specific pseudo address assignment for at least one user in the user set when the at least one user communicates with the route director via a NAT device, and the route director stores an association of the user-specific pseudo address with a public network address of the NAT device and a port number of the NAT device. Regarding Mukherjee assigning a network access identifier (NAI) to a user group (par. 47), this is not a user-specific pseudo address as claimed. Further, there is no disclosure or suggestion of storing an association of the user-specific pseudo address with a public network address of a NAT device and a port number of the NAT device. Moreover, Applicants note that the comments in the Office Action indicate that the currently pending claim was not examined. The Examiner is requested to carefully consider the language of the claim as pending.

The remaining claims are similarly patentable based on the above comments.

Conclusion

In view of the above, each of the pending claims is believed to be in condition for immediate allowance. The Examiner is therefore requested to pass this application on to an early

issue. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

The Examiner's prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: Dec. 4, 2007

By: /Ralph F. Hoppin/
Ralph F. Hoppin
Reg. No. 38,494

VIERRA MAGEN MARCUS & DENIRO LLP
575 Market Street, Suite 2500
San Francisco, California 94105-4206
Telephone: (415) 369-9660, x214
Facsimile: (415) 369-9665

Electronic Patent Application Fee Transmittal					
Application Number:		10403818			
Filing Date:		31-Mar-2003			
Title of Invention:		Secure virtual community network system			
First Named Inventor/Applicant Name:		Hasan S. Alkhatib			
Filer:		Ralph Hoppin			
Attorney Docket Number:		TTCC-01021US0			
Filed as Small Entity					
Utility Filing Fees					
Description		Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					
Extension - 3 months with \$230 paid		2253	1	295	295

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	405	405
Total in USD (\$)				700

Electronic Acknowledgement Receipt	
EFS ID:	2545743
Application Number:	10403818
International Application Number:	
Confirmation Number:	2698
Title of Invention:	Secure virtual community network system
First Named Inventor/Applicant Name:	Hasan S. Alkhatib
Customer Number:	28554
Filer:	Ralph Hoppin
Filer Authorized By:	
Attorney Docket Number:	TTCC-01021US0
Receipt Date:	04-DEC-2007
Filing Date:	31-MAR-2003
Time Stamp:	18:49:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 700
RAM confirmation Number	2507
Deposit Account	
Authorized User	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)

1	Request for Continued Examination (RCE)	TTCC-1021-RCE.pdf	719224 1f10704f4e38cd1d651f04462dda56a4c7e554a7	no	3
Warnings:					
Information:					
2		1021-response-003.pdf	104859 0e9c0f40d5123eb8d21fc826dfb0ff109defb88a	yes	21
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	17	
	Applicant Arguments/Remarks Made in an Amendment		18	21	
Warnings:					
Information:					
3	Fee Worksheet (PTO-06)	fee-info.pdf	8302 a1e4257ce7e0678105c9ffeb774471890dbb735b	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			832385		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Filing Date
03/31/2003

APPLICATION AS FILED – PART I

OTHER THAN

(Column 1)

(Column 2)

SMALL ENTITY ☒

OR

SMALL ENTITY

FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)		OR	RATE (\$)		FEE (\$)	
☐	BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A					N/A			
☐	SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A					N/A			
☐	EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A					N/A			
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 =	*	X \$ =					X \$ =			
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	X \$ =					X \$ =			
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).										
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))												
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL					TOTAL			

APPLICATION AS AMENDED – PART II

(Column 1)

(Column 2)

(Column 3)

SMALL ENTITY

OR

OTHER THAN

SMALL ENTITY

AMENDMENT	12/04/2007	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	* 108	Minus	** 109	= 0
	Independent (37 CFR 1.16(h))	* 8	Minus	***8	= 0
	☐ Application Size Fee (37 CFR 1.16(s))				
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))				

RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
X \$25 =	0	OR	X \$ =	
X \$105 =	0	OR	X \$ =	
		OR		
TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

(Column 1)

(Column 2)

(Column 3)

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=		X \$ =			X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		X \$ =			X \$ =	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE		TOTAL ADD'L FEE	OR			

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
Kim Downing

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

Application Number		10403818
Filing Date		2003-03-31
First Named Inventor	Alkhatib	
Art Unit	2142	
Examiner Name	Blair, Douglas B.	
Attorney Docket Number	TTCC-1021US0	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6983319		2006-01-03	Lu	
	2	7032242		2006-04-18	Grabelsky	
	3	7139828		2006-11-21	Alkhatib	
	4	6353614		2002-03-05	Borella	
	5	6353886		2002-03-05	Howard	
	6	6981020		2005-12-27	Miloslavsky	
	7	6982953		2006-01-03	Swales	
	8	6438597		2002-08-20	Mosberger	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit		2142
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number		TTCC-1021US0

	9	6438612		2002-08-20	Ylonen	
	10	6381638		2002-04-30	Mahler	
	11	6457061		2002-09-24	Bal	
	12	6993012		2006-01-31	Liu	
	13	6490289		2002-12-03	Zhang	
	14	6496867		2002-12-17	Beser	
	15	6507873		2003-01-14	Suzuki	
	16	6523068		2003-02-18	Beser	
	17	6556584		2003-04-29	Horsley	
	18	6993595		2006-01-31	Luptowski	
	19	6557306		2003-05-06	Sekiya	

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

Application Number		10403818
Filing Date		2003-03-31
First Named Inventor	Alkhatib	
Art Unit		2142
Examiner Name	Blair, Douglas B.	
Attorney Docket Number		TTCC-1021US0

	20	6996628		2006-02-07	Keane	
	21	6430622		2002-08-06	Aiken, Jr.	
	22	6996631		2006-02-07	Aiken	
	23	7003481		2006-02-21	Banka	
	24	6631416		2003-10-07	Bendinelli	
	25	6772210		2004-08-03	Edholm	
	26	6657991		2003-12-02	Akgun	
	27	6778528		2004-08-17	Blair	
	28	6697377		2004-02-24	Ju	
	29	6430623		2002-08-06	Alkhatib	
	30	6452925		2002-09-17	Sistanizadeh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit		2142
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number		TTCC-1021US0

	31	6781982		2004-08-24	Borella	
	32	6480508		2002-11-12	Mwikalo	
	33	6948003		2005-09-20	Newman	
	34	6557037		2003-04-29	Provino	
	35	6591306		2003-07-08	Redlich	
	36	6618757		2003-09-09	Babbitt	
	37	6973485		2005-12-16	Ebata	
	38	6629137		2003-09-30	Wynn	
	39	6651101		2003-11-18	Gai	
	40	6662223		2003-12-09	Zhang	
	41	6742045		2004-05-25	Albert	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818	
	Filing Date		2003-03-31	
	First Named Inventor	Alkhatib		
	Art Unit	2142		
	Examiner Name	Blair, Douglas B.		
	Attorney Docket Number	TTCC-1021US0		

	42	6747979		2004-06-08	Banks	
	43	6754706		2004-06-22	Swildens	
	44	6779035		2004-08-17	Gbadegesin	
	45	6973485		2005-12-06	Ebata	

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

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

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

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

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

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

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit	2142	
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number	TTCC-1021US0	

	1		☐
--	---	--	--------------------------

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

Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	10403818
	Filing Date	2003-03-31
	First Named Inventor	Alkhatib
	Art Unit	2142
	Examiner Name	Blair, Douglas B.
	Attorney Docket Number	TTCC-1021US0

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Ralph F. Hoppin/	Date (YYYY-MM-DD)	2007-12-05
Name/Print	Ralph F. Hoppin	Registration Number	38494

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

Privacy Act Statement

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

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

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

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

Application Number		10403818
Filing Date		2003-03-31
First Named Inventor	Alkhatib	
Art Unit	2142	
Examiner Name	Blair, Douglas B.	
Attorney Docket Number	TTCC-1021US0	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5864666		1999-01-26	Shrader	
	2	6058431		2000-05-02	Srisuresh	
	3	6128664		2000-10-13	Yanagidate	
	4	6173399		2001-01-09	Gilbrech	
	5	5159592		1992-10-27	Perkins	
	6	5361256		1994-11-01	Doeringer	
	7	5563878		1996-10-08	Blakeley	
	8	5623605		1997-04-22	Keshav	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818	
	Filing Date		2003-03-31	
	First Named Inventor	Alkhatib		
	Art Unit		2142	
	Examiner Name	Blair, Douglas B.		
	Attorney Docket Number		TTCC-1021US0	

	9	5701427		1997-12-23	Lathrop	
	10	5717686		1998-02-10	Schiavoni	
	11	5717687		1998-02-10	Minot	
	12	5734651		1998-03-31	Blakeley	
	13	5751961		1998-05-12	Smyk	
	14	5764906		1998-06-09	Edelstein	
	15	5777989		1998-07-07	McGarvey	
	16	5781550		1998-07-14	Templin	
	17	5790548		1998-08-04	Sistanizadeh	
	18	5793763		1998-08-11	Mayes	
	19	5805818		1998-09-08	Perlman	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit		2142
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number		TTCC-1021US0

	20	5805820		1998-09-08	Bellovin	
	21	5815664		1998-09-29	Asano	
	22	5826014		1998-10-20	Coley	
	23	5856974		1999-01-05	Gervais	
	24	5867667		1999-02-02	Butman	
	25	5884038		1999-03-16	Kapoor	
	26	5884246		1999-03-16	Boucher	
	27	5889953		1999-03-30	Thebaut	
	28	5897662		1999-04-27	Corrigan	
	29	5898830		1999-04-27	Wesinger, Jr.	
	30	5913210		1999-06-15	Call	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818	
	Filing Date		2003-03-31	
	First Named Inventor	Alkhatib		
	Art Unit		2142	
	Examiner Name	Blair, Douglas B.		
	Attorney Docket Number		TTCC-1021US0	

	31	5937162		1999-08-10	Funk	
	32	5937163		1999-08-10	Lee	
	33	6003084		1999-12-14	Green	
	34	6006272		1999-12-21	Aravamudan	
	35	6032196		2000-02-29	Monier	
	36	6047325		2000-04-04	Jain	
	37	6055236		2000-04-25	Nessett	
	38	6055575		2000-04-25	Paulsen	
	39	6061349		2000-05-09	Coile	
	40	6061738		2000-05-09	Osaku	
	41	6101543		2000-08-08	Alden	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818	
	Filing Date		2003-03-31	
	First Named Inventor	Alkhatib		
	Art Unit	2142		
	Examiner Name	Blair, Douglas B.		
	Attorney Docket Number	TTCC-1021US0		

	42	6119171		2000-09-12	Alkhatib	
	43	6122276		2000-09-19	Boe	
	44	6137791		2000-10-24	Frid	
	45	6154839		2000-11-28	Arrow	
	46	6219715		2001-04-17	Ohno	
	47	6243749		2001-06-05	Sitaraman	
	48	6249801		2001-06-19	Zisapel	
	49	6266707		2001-07-24	6266707	
	50	6304906		2001-10-16	Bhatti	

If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit	2142	
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number	TTCC-1021US0	

	1					
--	---	--	--	--	--	--

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

FOREIGN PATENT DOCUMENTS	Remove
---------------------------------	---------------------------------------

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS	Remove
--	---------------------------------------

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	KESSLER, Gary C., "Mobile IP: Harbinger of Untethered Computing," http://www.garykessler.net/library/mobileip.htm , 1/20/2004	☐
	2	REKHTER, "Cisco Systems' Tag Switching Architecture overview," Network Working Group, February 1997.	☐
	3	KENT, "Security Architecture for the Internet Protocol," Network Working Group, November 1998.	☐
	4	Computer Dictionary; Microsoft Press; 3rd Edition; 1997; p. 264.	☐
	5	Excerpts from the Help section of Microsoft Outlook pertaining to rules and forwarding email. Microsoft Corporation.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10403818
	Filing Date		2003-03-31
	First Named Inventor	Alkhatib	
	Art Unit	2142	
	Examiner Name	Blair, Douglas B.	
	Attorney Docket Number	TTCC-1021US0	

	6	K. EGEVANG and P. FRANCIS, RFC 1631, The IP Network Address Translator (NAT), May 1994.	☐
--	---	---	--------------------------

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

Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	10403818
	Filing Date	2003-03-31
	First Named Inventor	Alkhatib
	Art Unit	2142
	Examiner Name	Blair, Douglas B.
	Attorney Docket Number	TTCC-1021US0

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Ralph F. Hoppin/	Date (YYYY-MM-DD)	2007-12-05
Name/Print	Ralph F. Hoppin	Registration Number	38494

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

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt	
EFS ID:	2550830
Application Number:	10403818
International Application Number:	
Confirmation Number:	2698
Title of Invention:	Secure virtual community network system
First Named Inventor/Applicant Name:	Hasan S. Alkhatib
Customer Number:	28554
Filer:	Ralph Hoppin
Filer Authorized By:	
Attorney Docket Number:	TTCC-01021US0
Receipt Date:	05-DEC-2007
Filing Date:	31-MAR-2003
Time Stamp:	16:09:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	1021-ids-004-part1.pdf	1050297	no	8
			6530d44cde912ad775f0c9cae0df5889dd309c68		
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Filed	1021-ids-004-part2.pdf	1130215	no	9
			e2fd714c2&d341baeb32091087b7a45ae2fd714c2&d341baeb32091087b7a45ae084555c2		
Warnings:					
Information:					
3	NPL Documents	Microsoft-dictionary2.pdf	2544882	no	3
			d950db4c42db8d2ec848bb6221b2139d8a539c77		
Warnings:					
Information:					
4	NPL Documents	Kessler2.pdf	119823	no	9
			1d5595abb575fb70cd744378c154224ad10317d5		
Warnings:					
Information:					
5	NPL Documents	Rekhter2.pdf	76085	no	13
			cc5f57ebf4de72be4374cd5ab65ded90bf6deb24		
Warnings:					
Information:					
6	NPL Documents	Kent2.pdf	376445	no	66
			6aa57ce7a23b036ad5225eb24771302debd86b89		
Warnings:					
Information:					
7	NPL Documents	Microsoft-manage-the-inbox 2.pdf	226838	no	3
			9006c22b1f11fe7745d6a44d8708d7d75512537		
Warnings:					
Information:					
8	NPL Documents	Egevang2.pdf	96471	no	9
			a152fc8385dd8aeb372388d1a25dee9f3c4b8de		
Warnings:					
Information:					
Total Files Size (in bytes):			5621056		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

INUF007

PTO/SB/96 (04-07)

Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

STATEMENT UNDER 37 CFR 3.73(b)Applicant/Patent Owner: Inpro Network Facility, LLCApplication No./Patent No.: 10/403,818 Filed/Issue Date: March 31, 2003Entitled: Secure virtual community network systemInpro Network Facility, LLC, a LLC
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest
(The extent (by percentage) of its ownership interest is _____ %)

in the patent application/patent identified above by virtue of either:

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

OR

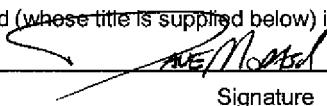
- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Hasan S. Alkhatib To: IP Dynamics, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 014340, Frame 0968, or for which a copy thereof is attached.
2. From: IP Dynamics, Inc. To: Inpro Network Facility, LLC
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.
3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

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

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



SignatureDavid A. Morasch

Printed or Typed Name

Attorney of Record, Reg. No. 42905

Title

Jan. 22, 2008

Date509-755-7262

Telephone Number

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

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.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:



Practitioners associated with the Customer Number:

75671

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:



The address associated with Customer Number:

75671

OR



Firm or Individual Name

Address

City

State

Zip

Country

Telephone

Email

Assignee Name and Address:

Inpro Network Facility, LLC
2711 Centerville Road, Suite 400
Wilmington, DE 19808

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	<i>Pat Mathews</i>	Date	<i>22 January 2008</i>
Name	Pat Mathews	Telephone	
Title	Authorized Person for Inpro Network Facility, LLC		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Assignment of Patent Rights

IP Dynamics, Inc., acting through its Chapter 7 bankruptcy trustee, Mohamed Poonja ("Assignor"), hereby assigns to Inpro Network Facility, LLC, a Delaware limited liability company, with an address at 2711 Centerville Road, Suite 400, Wilmington, DE 19808 ("Assignee"), all present and future right, title, and interest in and to all: (a) patent applications and patents of Assignor, including, without limitation, those listed below, together with all reissues, reexaminations, extensions, continuations, continuations in part, continuing prosecution applications, requests for continuing examinations, divisions, registrations of any such patent applications and patents of Assignor (the "Patents"); (b) inventions, invention disclosures, and discoveries described in any of the Patents; and (c) causes of action for past, current, and future infringement of the Patents (the "Purchased Assets").

Patent/Application No.	Patent/Application Name	Filing Country	First Named Inventor	Filing Date
6119171	DOMAIN NAME ROUTING	US	ALKHATIB, HASAN S.	1/29/1998
EP99903457.2	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SE NT TO A DESTINATION ON A NETWORK	EP	ALKHATIB, HASAN S.	3/08/2000
KR1020007008280	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SE NT TO A DESTINATION ON A NETWORK	KR	ALKHATIB, HASAN S.	7/28/2000
CN99802561.5	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SE NT TO A DESTINATION ON A NETWORK	CN	ALKHATIB, HASAN S.	7/31/2000
JP12-0529825	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SE NT TO A DESTINATION ON A NETWORK	JP	ALKHATIB, HASAN S.	7/31/2000
AU19990023470	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SE NT TO A DESTINATION ON A NETWORK	AU	ALKHATIB, HASAN S.	1/27/1999
6430623	DOMAIN NAME ROUTING	US	ALKHATIB, HASAN S.	1/27/2000
6772227	COMMUNICATING BETWEEN ADDRESS SPACES	US	ALKHATIB, HASAN S.	5/26/2002
6421732	IPNET GATE	US	ALKHATIB, HASAN S.	10/06/1998
6532217	SYSTEM FOR AUTOMATICALLY DETERMINING A NETWORK ADDRESS	US	ALKHATIB, HASAN S.	06/28/1999
7133404	COMMUNICATION USING TWO ADDRESSES FOR AN ENTITY	US	ALKHATIB, HASAN S.	08/10/2001

M

Patent/Application No.	Patent/Application Name	Filing Country	First Named Inventor	Filing Date
7139828	ACCESSING AN ENTITY INSIDE A PRIVATE NETWORK	US	ALKHATIB, HASAN S.	3/30/2002
10/161,573	CREATING A PUBLIC IDENTITY FOR AN ENTITY ON A NETWORK	US	ALKHATIB, HASAN S.	6/3/2002
10/233,288	COMMUNICATING WITH AN ENTITY INSIDE A PRIVATE NETWORK USING AN EXISTING CONNECTION TO INITIATE COMMUNICATION	US	ALKHATIB, HASAN S.	8/30/2002
10/403,518	GROUP AGENT	US	ALKHATIB, HASAN S.	3/31/2003
10/403,818	SECURE VIRTUAL COMMUNITY NETWORK SYSTEM	US	ALKHATIB, HASAN S.	3/31/2003
10/403,829	SECURE VIRTUAL ADDRESS REALM	US	ALKHATIB, HASAN S.	3/31/2003
PCT/US1999/01806	SYSTEM AND METHOD FOR USING DOMAIN NAMES TO ROUTE DATA SENT TO A DESTINATION ON A NETWORK	WO	ALKHATIB, HASAN S.	1/27/1999
60/098,205	IPNET GATEWAY	US	ALKHATIB, HASAN S.	8/27/1998
60/091,000	SYSTEM FOR AUTO-CONFIGURING AN IP DEVICE	US	ALKHATIB, HASAN S.	6/29/1998
60/224,864	COMMUNICATION USING TWO ADDRESSES FOR AN ENTITY	US	ALKHATIB, HASAN S.	8/11/2000
PCT/US2003/27161	ACCESSING AN ENTITY INSIDE A PRIVATE NETWORK	WO	ALKHATIB, HASAN S.	8/27/2003
PCT/US2003/27160	COMMUNICATING WITH AN ENTITY INSIDE A PRIVATE NETWORK USING AN EXISTING CONNECTION TO INITIATE COMMUNICATION	WO	ALKHATIB, HASAN S.	8/23/2000
09/637,803		US	ALKHATIB, HASAN S.	

Assignor hereby authorizes the Commissioner of Patents and Trademarks of the United States and other empowered officials of the United States Patent and Trademark Office and/or the appropriate empowered officials of other relevant jurisdictions outside the United States to record the transfer of the Patents and related assets to Assignee, in accordance with this Assignment, and to issue to Assignee all letters patent which may issue with respect to the Purchased Assets.

At the reasonable request of Assignee, Assignor will execute and deliver such other instruments as may be necessary or desirable for effecting completely the consummation of the transactions contemplated hereby.

The terms and conditions of this Assignment of Patent Rights will inure to the benefit of Assignee,

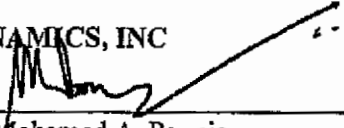
M

its successors, assigns, and other legal representatives and will be binding upon Assignor, its successors, assigns, and other legal representatives.

IN WITNESS WHEREOF, Assignor has caused these presents to be duly executed in a manner appropriate thereto as of January 7, 2008.

Assignor:

IP DYNAMICS, INC

By: 

Name: Mohamed A. Poonja

Title: Chapter 7 Bankruptcy Trustee

ACKNOWLEDGMENT

State of California)

County of Santa Clara) ss:

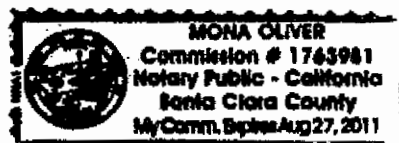
On this 7th day of January XXX 2008, before me, the undersigned, personally appeared Mohammed A. Poonja personally known to me and acknowledged to me that he/she/they executed the same in his capacity as the Chapter 7 Trustee of IP Dynamics, Inc., and that by his signature on the instrument executed this instrument on behalf of IP Dynamics, Inc.

WITNESS my hand and official seal.

Signature: Mona Oliver

Notary Public

(Seal)



Electronic Acknowledgement Receipt	
EFS ID:	2789466
Application Number:	10403818
International Application Number:	
Confirmation Number:	2698
Title of Invention:	Secure virtual community network system
First Named Inventor/Applicant Name:	Hasan S. Alkhatib
Customer Number:	28554
Filer:	William Breen/Linnaea Freeman
Filer Authorized By:	William Breen
Attorney Docket Number:	TTCC-01021US0
Receipt Date:	30-JAN-2008
Filing Date:	31-MAR-2003
Time Stamp:	15:33:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	INNFO017.pdf	193617	no	5
			ea511d7c17b4dc7164d138f3af55a1a3644581ff1		
Warnings:					
Information:					

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. 10/403,818
Confirmation No. 2698
Filing Date Mar 31, 2003
Inventorship Hasan S. Alkhatib
Assignee..... Inpro Network Facility, LLC
Group Art Unit 2142
Examiner Douglas B. Blair
Attorney's Docket No. INN0017
Title: Secure virtual community network system

NOTIFICATION OF LOSS OF ENTITLEMENT TO SMALL ENTITY STATUS

To: Honorable Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

From: Michael K. Colby (Tel. 509-755-7262; Fax 509-755-7252)
Sadler, Breen, Morasch & Colby, p.s.
422 W. Riverside Avenue, Suite 424
Spokane, WA 99201

Customer No. 75671

Due to an assignment of ownership in the above patent application, the entity status of the Assignee in this patent application should be changed to Large Entity Status.

Respectfully Submitted,

Date: 1 February 2008

By: /Michael K. Colby/
Michael K. Colby
Reg. No. 45816
Attorney for Applicant
Sadler, Breen, Morasch & Colby, PS
422 W. Riverside Avenue, Suite 424
Spokane, Washington 99201
Telephone: (509) 755-7254
Facsimile: (509) 755-7252