



(22) Date de dépôt/Filing Date: 2000/10/12

(41) Mise à la disp. pub./Open to Public Insp.: 2002/02/18

(30) Priorités/Priorities: 2000/08/18 (2,316,428) CA;
2000/09/12 (09/660,245) US

(51) Cl.Int.⁷/Int.Cl.⁷ H04L 9/32

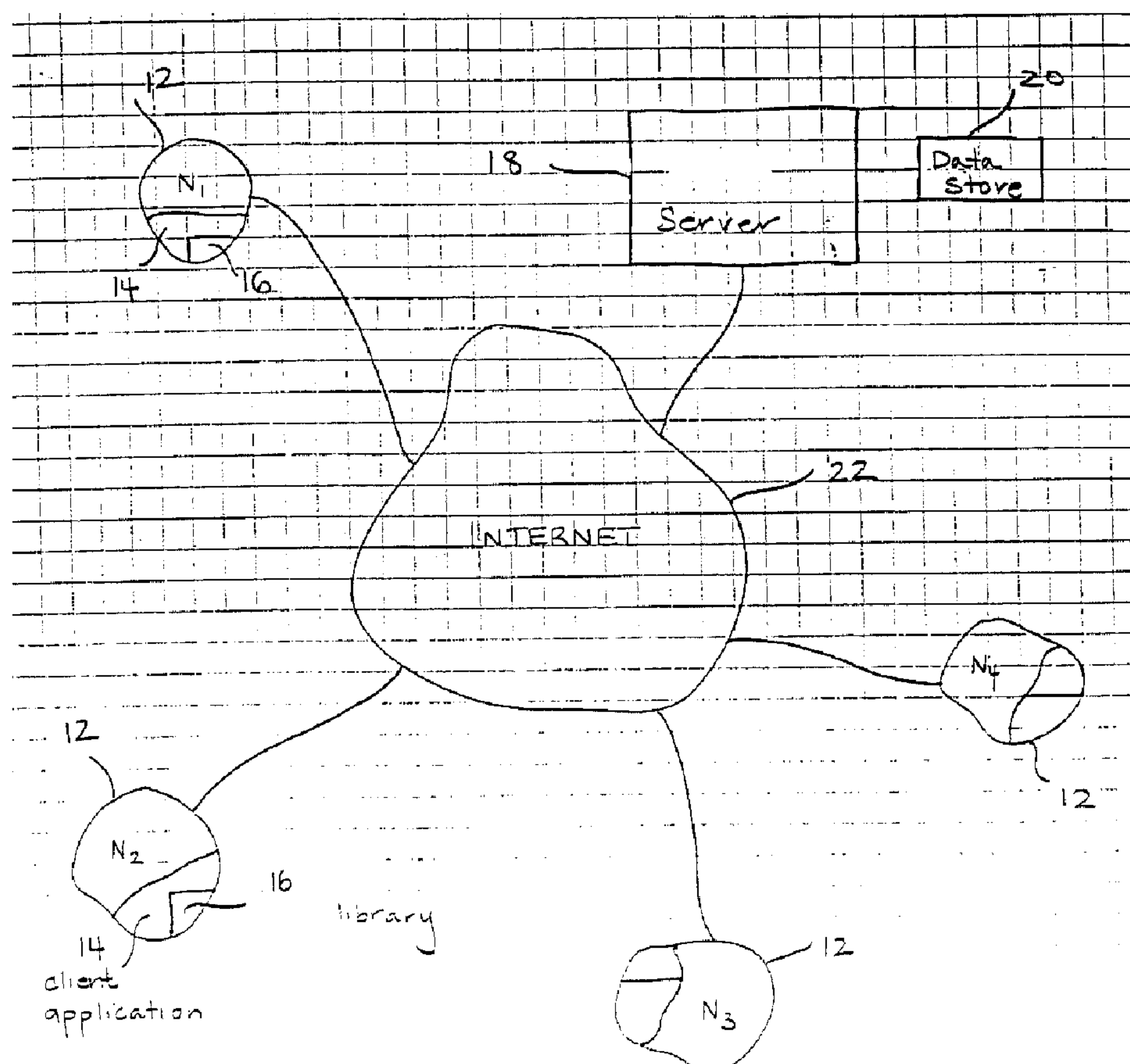
(71) Demandeur/Applicant:
ETUNNELS INC., US

(72) Inventeurs/Inventors:
POIER, M. SKYE, CA;
MEHARG, GERSHAM, CA

(74) Agent: ORANGE & CHARI

(54) Titre : METHODE ET APPAREIL DE TRANSMISSION DE DONNEES ENTRE UN CERTAIN NOMBRE DE
CORRESPONDANTS

(54) Title: METHOD AND APPARATUS FOR DATA COMMUNICATION BETWEEN A PLURALITY OF PARTIES



(57) Abrégé/Abstract:

A system and method to enable the secure transfer of information between nodal points in a workgroup over a public network by facilitating the creation of a virtual private network (VPN). The system comprises at least three nodal points and where at least



(57) Abrégé(suite)/Abstract(continued):

one of these nodal points is a server. The system is configured so as to centrally manage the system and allow for the update, modification, and implementation of information for each node in the workgroup from an server. The system further comprises a database linked to the server and a client application having an library located at each node. The client application communicates with the library through an API, and where the library transmits data to and receives data from the server.

Abstract:

A system and method to enable the secure transfer of information between nodal points in a workgroup over a public network by facilitating the creation of a virtual private network (VPN).

- 5 The system comprises at least three nodal points and where at least one of these nodal points is a server. The system is configured so as to centrally manage the system and allow for the update, modification, and implementation of information for each node in the workgroup from an server. The system further comprises a database linked to the server and a client application having an library located at each node. The client application communicates with the library through an
- 10 API, and where the library transmits data to and receives data from the server.

METHOD AND APPARATUS FOR DATA COMMUNICATION BETWEEN A PLURALITY OF PARTIES

FIELD OF THE INVENTION:

5

The invention relates to a system and method of providing secure communications over an open network, and more specifically to the application of a virtual private network which runs on a diverse set of operating systems and hardware platforms and facilitates ease of use.

10 BACKGROUND:

Workgroup computing involves, by definition, the exchange of data between the nodes of the workgroup, a node being a computer connected to a network which can be identified with an individual, a set of resources (files, services, devices, etc), or a gateway. Often, the tasks of a
15 workgroup are of a sensitive nature containing, for instance, confidential information on finances, business development plans, or private email. The Internet (and its native IP protocol) has become ubiquitous as a means of connecting nodes in a workgroup computing environment as it is cheaper and more effective than traditional private networks, especially when the nodes are geographically disparate. However, with the adoption of a public networking infrastructure comes the risk that an
20 unauthorised 3rd party with access to the physical data route between two nodes may intercept and reconstruct data transferred between them. To prevent interception, a mechanism is required to modify the transmission of data such that only the intended receiver may access it and the receiver can be guaranteed of the data origin.

25 A virtual private network is a system for securing communications between computers over an open network such as the Internet. By securing communications between the nodes, it is as if the computers were linked together on a private local area network (LAN). An Internet-based virtual private network (VPN) is virtual because although the Internet is freely accessible to the public, the Internet appears to the organization to be a dedicated private network. In order to accomplish
30 this, the data traffic for the organization may be encrypted at the sender's end and then decrypted at the receiver's end so that other users of the public network can intercept the data traffic, but

cannot read it due to the encryption.

5 A VPN can replace an existing private data network, supplement a private data network by helping relieve the load on the private data network, handle new software applications without disturbing the existing private data network or permit new locations to be easily added to the network. A typical VPN connects one or more private networks together through the Internet in which the network on each side of the Internet has a gateway and a leased line connecting the network to the Internet. In these typical VPNs, the same protocol for each private network is
10 used which makes it easier to communicate data between the two networks. To create the VPN, a secure communications path between the two gateways is formed so that the two private networks may communicate with each other.

15 In the case of Internet communications, the most commonly used software routines for the transport which involves addressing, routing, and data formatting is the Transmission Control Protocol (TCP/IP). The TCP/IP suite consists of four layers: an application layer, a transport layer, a network layer, and a physical layer. Each of these layers interacts only with the layer immediately above and below, and serves a specific set of functions. Security measures may be implemented at any of the layers. However, VPN's are generally built at the network level which
20 is responsible for the routing of data packets and the addressing mechanism.

In order to establish secure communication between any two nodes on a virtual private network, each node must obtain by some means information ("configuration") including but not limited to:

- 25 • The identity and state of the remote nodes within the VPN(s) of which the node is a member
- The location of the remote nodes on the logical network (IP address)
- The relationships between nodes (VPN membership)
- The keys to be used for encrypting and decrypting data transferred between nodes (one per node pair)
- 30 • Verification of the identity of the remote nodes

It is this securing of communication between nodes in a workgroup that the present invention is designed to facilitate.

5 Traditional VPN solutions are comprised of a number of tunnel termination devices which provide a central "hub" for VPN communication. Software is then deployed to nodes that wish to participate in a VPN, and the software is configured manually with the address of the tunnel termination device(s). The software is then executed in order to participate in the VPN. However, there are several disadvantages with respect to this technology. Each of the nodes may only be a
10 member of one VPN at a time in the majority of implementations. This limits the ultimate efficiency of the user at each node. In addition, the network does not have the ability to automatically configure nodes for VPN participation.

The Microsoft® Active Directory is a directory service designed to extend Microsoft®'s Windows
15 NT "domain" architecture. It allows organizations to share and manage information about network resources and users. In addition, Active Directory acts as the central authority for network security, permitting the Windows operating system to verify a user's identity and control access to Microsoft® network resources. It also acts as an integration point for bringing systems together and consolidating management tasks. As part of the authentication process for "logging into" a
20 domain, Active Directory allows a system administrator to specify security relationships to be automatically established by the authenticating node to other nodes within the NT domain. Using this technology has several drawbacks in that each of the nodes on the network must be running Win2000 Server or Professional Edition. Further, each of the nodes participating in the VPN must have accounts and be logged into the same NT domain which precludes automatic
25 provisioning of cross-organizational or "extranet" VPNs. The system also poses greater security risks as it requires more TCP ports to be open through firewalls for automatic VPN provisioning.

The use of VPN's is well known in the computer world each using different mechanisms to provide a means of secure data transmission. United States Patent No. 6,061,796 entitled "Multi-
30 Access" Virtual Private Network describes system and method for allowing private

communication over an open network. This system however, specifies what mechanism protocol level the Agent (VPN provisioning application) uses to intercept incoming and outgoing data from a node and is not designed to work with IP networks. In addition, it would be difficult to scale this particular system for large-scale use. In United States Patents No. 5,884,035 and 5 6026430 data transmission is only through the domain hierarchy and not on a data to client application basis. In the VPN system described in United States Patent No. 6,055,575 it notes that the "host computer establishes a secure communications path, referred to as a tunnel, through the public network with the remote client". This has firewall implications in that a remote node can rarely accept incoming connections.

10

The Internet today has become the world's largest public data network. The world wide web facilitates searching for information on virtually any topic, business expansion opportunities outside a local area, the emergence of virtual stores, and new methods of doing business. However, with the increased popularity of the Internet for both personal and business use, there 15 is a commensurate increase in public demand wishing access to Internet resources. As the internet expands, the number of sites connected to the Internet also expand. This increases the value of each site's connection to the Internet as it provides that organisation with an expanding population of potential customers. What the general public is unaware of however, are the scaling problems that relate to this expansion.

20

Currently, the internet uses an internet protocol version four (IPv4) as a means to provide internet address space. An IPv4 address is defined by a 32-bit address, thus there are 2^{32} IPv4 addresses available. While this may seem like a large number of addresses, with the expansion of the internet and the growing interest of businesses to make their services/products available 25 'on-line', a large portion of the world's population are now interested in having IP addresses. Therefore, the number of IPv4 addresses available will eventually be exhausted. In addition, a second problem stemming from Internet scaling issues is the ability to route traffic between the number of networks that form the Internet.

30 Transfer of information between networks connected to the Internet occurs via Internet routing tables. Several "backbone" routers maintain the complete routing information for the Internet.

As the demand for the Internet has increased, the number of required routing tables has experienced exponential growth. However, simply installing additional router memory and increasing the size of routing tables will not solve the problem. There are additional factors such as: the requirement for increased CPU horsepower in order to compute routing tables/topology changes, the increasingly dynamic nature of world wide web connections and, in turn, there effect on router forwarding caches, and the volume of information that must be managed by both people and machines. A limitless sized routing table is infeasible as it eventually leads to “backbone routers” dropping particular routes leaving portions of the Internet unreachable. There is a long-term solution in progress, the deployment of IP version 6 (Ipv6) however, this will not solve immediate internet growth related issues.

In general, each system wishing to have an Internet connection must be assigned a unique 32 bit Internet address. The address typically is divided into 2 parts, referred to as two-level addressing. The first portion of the Internet address identifies the network on which the host resides (network number), the second portion identifies the particular host on a given network (host number). All hosts on a given network share a common first portion given that this first portion identifies the network number. However, the second portion identifying the host itself, must be unique. In turn, two hosts operating on different networks will have different network numbers however, they may have identical host numbers. Further, there are three common address classes, A, B, and C. These classes are differentiated by the location of the boundary between the network number and the host number. These are three most popular classes, however additional classes do exist.

A typical method to overcome the lack of available of IP addresses is the use of non-routable IP addresses. A non-routable address is one that may not be routed over the internet. In this circumstance, to facilitate communication over the Internet, a local area network (LAN) uses a single set of IP addresses for internal traffic (non-routable addresses) and a second set of IP addresses for external traffic. A network address translation (NAT) box is located where the LAN meets the Internet in order to make all the necessary IP address translations. A NAT box typically has a pool of globally routable IP addresses and provides a type of firewall by hiding internal IP addresses. This, in turn, enables a company to use more internal IP addresses and,

because they are only used internally, there is no possibility of conflict with IP addresses of other companies. The NAT box typically intercepts packets, examines the source IP, and modifies the packet so as to substitute a globally registered IP address into the source IP address portion of the message when leaving the LAN. On returning information back to the sender, the NAT box,
5 when the data packet arrives, strips the globally registered IP address and resorts the private LAN IP address. However, a message sent using this system must initiate from within the LAN as an external sender will have no idea as to what globally routable IP address will be assigned to the message on its arrival at the NAT box. Further, when using a NAT box, end to end security is not possible. A NAT box modifies the data packet en route by the addition of a globally
10 routable IP address. When the packet arrives at the destination port and the message is decrypted, the authentication mechanism detects the data packet has been modified, and will in turn reject the message.

A port address translation (PAT) box acts in a similar manner to a network address translation
15 (NAT) box except, it uses only one globally routable IP address for all client computers on a LAN. In this circumstance, the client computer will make a socket connection with a port. A port number is then assigned at both ends meaning that the socket connection has a host number and a PAT port number. The port numbers are randomly allocated on the client or host end. The host numbers enable the PAT to send the information to the correct host on a LAN. The port
20 address is a known port number associated with the PAT box and is representative of the one single globally routable address. The IP address when sending a data packet, has two portions and is written as **(host port number, PAT port number)**. This system requires any firewall located in front of a LAN be configured to allow PAT box modified data packets to pass through. Generally, this is done by assigning a particular port number for use by PAT modified data
25 packets. This means that the selected port number is left open and may cause a break in security measures. Typically, in both NAT and PAT environments where security is required, encryption is performed after the NAT/PAT transformation on the outside edge. Accordingly, end to end security is not available and may limit the uses of the VPN.

30 In order to avoid complications arising from the presence of a NAT/PAT box, the prior art may employ a tunnelling scheme. The purpose of tunnelling applications is to run a protocol which

encapsulates IP data packets into a format suitable for transport over a TCP based connection. This requires encapsulating a TCP within a second TCP connection. This stacking of TCP's causes problems with "timeout" as the upper and lower TCP's have different timers. As a result, the upper TCP has a faster timer than the lower TCP, resulting in the lower TCP having a period
5 with a slow and unreliable connection. The end result is an internal meltdown with the upper TCP wherein there is layer queuing up retransmissions faster than the lower layer is able to process them.

10 It is an object of the present invention to obviate and mitigate at least some the aforementioned disadvantages of the prior art.

SUMMARY OF THE INVENTION:

Accordingly one aspect of the present invention provides a system for facilitating the secure
15 communication between nodes in a workgroup by the creation of a "n"-tiered virtual private network. Each node has the ability to transmit and receive data over a public network such as the Internet. The system comprises at least 3 nodes and where at least one of these nodes is an server, a data store linked to the server (where the data store maybe in the form of memory, disk, a database etc), and a client application including: an library located on each node and a
20 mechanism to transmit data within the workgroup. The data store further includes information pertaining to the configuration of virtual private networks (VPN), VPN relationships (eg. client computers membership to VPN's), settings and options (eg. encryption level, IP compression), authentication information, and objects and attributes (eg. status - online/offline, full user name, user IP). The system further includes a means to intercept both incoming and outgoing data from
25 a node so as to create a secure bridge between an open network and a node by encrypting and decrypting data. In addition, the system has a means for verification of node credentials against authentication servers. The bridge enables data to be securely shared to a private group. Each of the nodes has the ability to act as both a client and a server, such that a node either pulls updates from the server or the server pushes updates to the node (in this case the node acts like a server).

30

In a preferred embodiment, on start up of a node within the workgroup, the client application instructs the library to form a connection with the server. The library transmits authentication credentials to the server, the server authenticates the validity of the credentials, and a connection is established. Following the creation of a secure connection between the server and a node, the library synchronizes with the server and retrieves a packet of information from the data store that is transmitted to the library. This information packet includes a list of VPN's of which this particular node is a member and their respective attributes, a listing of other nodes which are members of the same VPN as the client computer, the current status of each node in each respective VPN, and other related details. Once a node, say node 1, is logged onto the server and, in turn, a desired VPN, the library of node 1 sits in the loop between the library of the client computer and the server. The central management of the system enables the server to be informed of any changes to a VPN eg. a node logging off, and is informed of these changes in a timely manner, where the time frame is elected by the node. The server then relays this information to the library of each client computer within a VPN and the library, in turn, sends a message to the client computer reporting the change to the VPN.

This system is global by the nature of the server such that it facilitates the central management of any VPN. The server facilitates the ability to make changes to a VPN without having to effect changes manually in each node of a virtual private network. A change made to the data store linked to the server is transmitted in a timely manner to all client computers effected by the change. For example, to change the password of a VPN for each node in a network, requires making that change to the data store and, in turn, that change is transmitted to each node on the virtual private network. While changing a password is a relatively simple task, the ability to effect more detailed changes to a VPN requires updating only a single point in a VPN and then transmitting that data to the remaining nodes in the workgroup via the secure connection. In use, the network has the ability to automatically and securely provision security associations between nodes.

In its simplest configuration the system employs security measures at the transport layer of the TCP/IP, however, any layer or combination of layers of a transport protocol may be used by the interception means in order to transfer data. Generally, the client application sees the destination

IP address in the header of the data packet, if that address is a node within the VPN, a key is applied using traditional methods, to encrypt the data which is then sent to the appropriate node. The process works the same way for decrypting to provide END-to-END security. When a node initially logs onto to a VPN and receives the information packet from the server, that information may contain keys for node pair within a VPN to encrypt and decrypt messages sent within that VPN network. The method of encryption and decryption employed is beyond the scope of this invention.

The control of the VPN created using the server may be in house in the sense that, at a particular company subscribing to this service, the IP manager would administer and maintain the VPN and have rights to modify information on the server and data store as it pertains to their VPN. Relationships between nodes in a VPN are pair based. Any and all IP traffic between two nodes on a VPN is encrypted and decrypted regardless of the type of information being sent. The server itself does not participate in the data transfer.

This invention further provides a system to enable secure communication between nodes over the Internet and have the benefit of end to end security. This system enables a node, which may operate behind a NAT or PAT box and/or a firewall, to establish secure communication over the Internet with another node having a globally routable IP address. The system comprises at least a pair of nodes located on the same virtual private network, a packet interception mechanism, a secure line for communication, and a client application located at each node. The client application located at each node includes a mechanism to transmit data within the virtual private network, and a library of configuration information including VPN relationships, authentication information, and settings and options (eg. encryption level, IP compression). In addition, the library will include information with respect to the presence of PAT or NAT boxes in front of particular nodes in a VPN. The system further comprises a mechanism for verification of node credentials against authentication servers, which enables data to be securely shared amongst members of a private group. The packet interception mechanism is generic and known to one skilled in the art.

Once nodes are logged onto a VPN, they may exchange information. A mechanism assesses connectivity between two nodes, say node A and node B, and if connectivity can not be determined, information sent from node A is not received by node B. The system then assesses the security associations of each node. If a node is located behind a PAT box, the security associations must also specify a specific port number for the post PAT box connection. Data packets are intercepted and then those containing the destination addresses of a specific node, say node B are selected. Packet headers containing this destination address are re-written so as to have the appearance of an SSL TCP header. The new TCP header is inserted after the existing IP header. The remaining portion of the data packet becomes an encapsulated secure payload (ESP). Within the new modified packet is a "masquerade bit", which indicates to the node receiving the data packet that the packet header has been re-written and will require decoding. The data packet is sent to the receiving party specified by the IP address portion of the packet header. On sending, the data packet appears to be a secure socket link (SSL) protocol session. In the case of a firewall the packet appears as an SSL protocol session and passes through port 443 unread. Generally a firewall allows outbound connections to port 443 in order to allow secure web browsing by client computers. The data stream over port 443 is encrypted such that the firewall can not inspect the contents of the traffic. This system, by re-writing the packet header to appear as TCP data in SSL format, allows data packets to be passed through firewalls via port 443, and facilitates the smooth and simple transfer of data between nodes.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1: is a schematic diagram of an overview of a computer system;

Figure 2: is a functional block diagram detailing the method for establishing secure communication between nodes, in the computer system of figure 1;

Figure 3: is a schematic of the computer system incorporating a plurality of types of nodes;

Figure 4: is a schematic diagram of the computer system detailing use of a gateway node in

co-operation with the plurality of other nodes;

Figure 5: is a functional block diagram detailing the communication hierarchy of the interaction of the API with the computer system of the present invention;

Figure 6: is a schematic diagram of an overview of a computer system incorporating LAN's, a gateway, and a firewall;

Figure 7: is a functional block diagram detailing the method for sending data over a VPN having secure communication in the computer system of figure 6;

Figure 8: is a functional block diagram detailing the method for receiving data over a VPN having secure communication in the computer system of figure 6; and

Figure 9: is a schematic of the data packets transferred between a plurality of types of nodes on a VPN.

To facilitate the understanding of the preferred embodiments described below, the following terminology will be used, it being understood that this is for illustrative purposes only and is not limiting:

Client Application - the software that acts as a slave to a server and is present on each node within a work group;

VPN - a virtual private network that is constructed over a public network to connect nodes within a work group such that:

- a) data transferred between those nodes is secure and cannot be intercepted, modified, or replaced on route; and
- b) it contains mechanisms to ensure that only authorized users may access the network..

Node - a computer connected to a network which maybe identified with an individual, a set of resources, or gateway;

Work Group - a group of two or more individual nodes working collaboratively on a group of tasks;

Library - this is the software portion of the client application, it provides a library of functions and includes configuration data received from the server during the synchronisation phase to be described hereafter;

API - application program interface, generally for communicating between software application and in this instance, an API defines the interface between software components within an application;

Gateway - a special node that provides secure communication to a specific network of nodes located behind the gateway; and

Network Address Translation – (NAT) an Internet Standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

DETAILED DESCRIPTION OF THE EMBODIMENT

A computer system for establishing a secure connection for the transfer of data between nodes in a work group over a public network is illustrated in figures 1 through 5 and is generally designated by reference numeral 10. The system 10 may be configured in a number of different ways including those utilizing individual users as shown in Figure 1, those utilizing individuals and intranet as shown in Figure 3, and those utilizing a gateway as shown in Figure 4. Initially it is necessary to establish communication between members of virtual private network (VPN) and this procedure will be described in respect of each configuration.

As shown in Figure 1, a computer system 10 comprises a plurality of nodes 12, server 18, and a data store 20 whose contents may be updated or changed periodically by external intervention. Each of the nodes 12 has a client application 14 and a library 16. The system 10 is arranged to enable the establishment of a secure path for communication between nodes 12 over a public network such as the internet 22. The server 18 collects and distributes data collected by the library 16 at each node 12, so as to maintain state information for each node 12. The server 18 tracks changes made to the data store 20 and subsequently updates each of the libraries 16. The library 16 communicates with the client application 14, and vice versa, through an application program interface (API), where the library 16 is responsible for transmitting to and receiving from information client application 14, and related library 16, and the server 18. The server 18

also serves to generate specific node cues based on those events, such as the availability of upgrades for client application. The data store 20 is linked to the server 18, and is essentially managed so as to enable the automatic provisioning of security relationships with nodes 12 in a network. A network having secure communication between these nodes 12 is typically known as
5 and from herein referred to "a virtual private network" (VPN). The centrally managed data store 20 allows for arbitrary additions, modifications, and alterations to that data store 20 and, in turn, deploys that information through the server 18, to nodes 12 located within a virtual private network.

10 The method of establishing secure communication between nodes in a work group is detailed in Figure 2. On startup of a node within a work group, the client application 14 instructs the library 16, through the API to form a connection with the server 18. Once the instructions have been received, as indicated at 102, the API forms a socket connection (generally using secure socket links such as SSL/3DES socket security). Once a connection, 104, is formed between the
15 server and a node, the authentication phase, 106, begins. The client application transmits credentials through the library 16 to the server. The server then authenticates the validity of these credentials and returns data stating the success 108 or failure 109 of the logon to the server. If the credentials are found to be invalid the process fails and ends. Once logged onto the VPN, Figure 5 illustrates the functioning of a communication system of a typical operating system in
20 unison with the client application of the present invention and a network enabled application. An API is designed for transparent communication between nodes/client computers as well as various internet services. The API is basically a configuration manager that generally operates through a remote procedure call protocol in order to communicate demands between an application program and a protocol stack. An API may also facilitate communication with other
25 programs. Prior to the transport of data packets between the protocol stack and the hardware driver, a packet interceptor intercepts a data packet in order to authenticate both the sender and receiver and to ensure a secure channel between the server 18 and the nodes 12 (as in Figure 3). The packet interceptor communicates with the library 16 through a plurality of security associations in order to ensure the validity of the credentials.

30

Once the node is logged onto the server 18 the synchronization phase 110 begins. The server 18 delivers a packet of information to the library 16 via the secure socket connection so as to establish a virtual private network. The data packet includes, but is not limited to, a list of virtual private networks to which that node is a member, their related attributes, the state of other client computers located within a virtual private network of which the client computer is a member, and their related details such as IP address. Once this transfer of information 112 has occurred, the server 18 and node 12 are successfully linked as indicated at 114, and the transfer of data over a secure line of communication is enabled. Once logged onto the server 18, data is transferred between a pair of nodes 12 by invoking procedures on remotely hosted objects on a node 12 and determining the type and target of the change or data to be distributed.

Thereafter, any change to the data store 20 that affects a work group of which the node is a member will be forwarded from the server 18 to that node. The server is able to determine the relevant nodes 12 from the contents of the data product received during the information transfer phase 112. There are two types of changes that affect the datastore 20. A node generated change eg/ going offline, invokes a method of an object located on the server 18 to change the attribute of "itself". The server 18 examines the type of change, in this case - going offline, and determines all online nodes in the VPN's that the node is a member of which require notification. The server 18 retrieves a list of those nodes from the datastore 20, and notifies each interested node. The notification is either synchronous or asynchronous.

A management interface change eg/ altering VPN membership through a web-based configuration tool, invokes a procedure on the server 18 notifying the server 18 of the change to the datastore 20. The server 18 examines the type of change and distributes the notification as described above. Accordingly, a VPN is established to allow communication between each of the nodes. A similar procedure may be utilized in the configuration of Figure 3.

Figure 3 illustrates a plurality of nodes 12A through 12E, where at nodes 12C through 12E there are a plurality of client computers. The computer system 10 detailed in Figure 3 is a multi tiered client/server system in which every node 12 acts as both a client and server. A node either pulls update from the server, and in such a case in synchronous and acts as a client, or the server

pushes updates to a node by invoking a method on an object which resides on the node, hence is a synchronous and acts as a server. The server 18 operates over an existing network connection to the public network connection 22 that each node 12 possesses. The computer system 10 allows arbitrary grouping of nodes 12 on the Internet 22 into VPNs across, for instance, network,
5 organisational and geographical boundaries.

The computer system 10 enables an extranet connection for example between two offices of a company 12D and 12E, each of which has its own intranet, to be included a work group. In this situation a corporation typically will have at least one localized server 17B, 19B, which will act
10 as server for that intranet. Each client computer within that corporation will be connected to that localized server. The localized server 17B, 19B exists within a hierarchy within the computer system such that if a node/client computer within the corporation queries the localized server, and that server does not contain the information queried for, that server climbs the hierarchy chain to a higher up server and queries for the information. This process continues until the
15 information is returned to the localized server where it can be distributed to the appropriate client computers within that network. Alternatively, a node within the corporate network is capable of communicating with, for example a traveling user 12B located outside the office.

When each node 12A through 12E logs onto the server 18, such that each node in the network
20 exists in a parallel relationship with another node. Each pair of nodes is typically setup with a set of keys and a unique identity such that they may transmit secure messages that have been encrypted and decrypted using this set of pair based keys. Preferably, the system 10 employs an existing peer-to-peer key exchange mechanism eg Internet Key Exchange (IKE), to negotiate session keys with each peer for data exchange. However, in the event that IKE is inaccessible, a
25 pair of nodes 12 may negotiate and transmit keys via server 18. In the alternative, the server 18 may generate and distribute to keys and node pairs 12. It will be appreciated that when transmitting data between two nodes logged on to a virtual private network, that data is not transmitted through the server 18. The server 18 is used for the initial provisioning of the virtual private network and to transfer information through the API to the library 16 of each node with
30 configuration information for the provisioning of that virtual private network. Again a VPN is established between a set of nodes interconnected by the internet 22.

Figure 4 again shows computer system 10, and in this embodiment, involves the use of a gateway 24 that includes a library portion containing attributes of the servers connected to the gateway 24. Although the gateway 24 controls access to several nodes, each indicated as a server 25, the gateway 24 is considered a node by other users and has a key pair associating it with each of the other nodes in the system 10. During the logon process detailed in Figure 2, the server 18 will detect the presence of the gateway 24 and, during the synchronization phase, the data store 20 will provide information to the library portion 16 of the gateway 24 as to the range of IP addresses that are assigned to nodes behind the gateway. In an alternative embodiment, the server will also detect the presence of a firewall 23 (shown in Figure 4), NAT box, or PAT box (not shown) as above. The gateway 24 has a set of rules called security associations that are designed to control access to the VPN such that the gateway protects a plurality of nodes. Conventionally, when a node in front of the gateway, such as 12A wishes to communicate with a node behind the gateway such as 12G, the node 12A selects the key pair associated with the gateway 24 to provide encryption and decryption of the data. The decryption then occurs at the gateway as opposed to at the node to which the message is directed. The same is true of a NAT or PAT box. Where decryption traditionally occurs at the box. When a user who is typically a member of the plurality of nodes located behind the gateway, such as a company network 12G, is working from home 12A, the IP address of the home computer 12A is not in the range of IP addresses specified by the gateway 24. When an IP address falls outside the range of addresses known to the gateway 24 access may be denied to the company network. In such a situation, a virtual IP (VIP) address is typically assigned to the home user 12A. When a VIP is assigned to the node of the home user 12A, data sent from node 12A to the company network 12G, located behind the gateway 24, the gateway will route this data through a virtual interface. In the case where a node is a intranet, as in Figure 3 node 12C, and that node 12C wants to send data to 19B, the server 18 will have a plurality of rules known as an access control list (ACL), stating which client computers located within 12C may access data on the servers. Security measures in each of the above cases conventionally are employed at the gateway 24.

In order to employ end to end security in the presence of firewalls, gateways, NAT/PAT boxes, or when connections are slow and unreliable, the procedure set forth in Figure 6 is utilized.

On startup of a node 12 within a work group (as shown in Figures 3, 4), that node logs on to a virtual private network so as to create a secure communication link and, in the preferred embodiment, is as described in Figure 2. Once logged on the VPN, a mechanism is employed to assess connectivity between nodes and determines its availability. This check is performed by each node and is directed at its peer. On assessing connectivity, 204, the peer is located behind a NAT or PAT box, that information is conveyed to the library 16 of that specific node 12. Provided a node is not located behind a gateway, NAT/PAT box, or firewall, when connectivity is established, a data packet, originating from independent applications, is sent securely from one node 12 to another typically employing conventional methods of end-to-end security. Such packets typically comprise an IP header 72, a TCP header 74, and data 76 as shown in Figure 8a. The IP header communicates the data's endpoint, the TCP header specifies the transport protocol, and the data portion is the bit stream which comprises the message being sent. The actual processing of the information contained within the data packets, as well as the decryption, is known in the art and falls outside the scope of this invention.

Once it is determined that connectivity can not be established, often due to a slow connection, the presence of a firewall etc., the method detailed in Figure 6 is enabled to facilitate data transfer. The failure to establish connectivity indicates to the system 10 to assess the security associations (SA) for each node, 206. Data packets, originating from independent applications, are intercepted, 207 and those packets having the globally routable IP address of the peer, the intended receiver, are selected. The lack of connectivity informs the system 10 that these data packets that have been intercepted require modification in order to enable their sending. Thus, the data packets are examined and packet headers are modified (as shown in Figure 8) so as to appear as SSL TCP headers, 208. This masques the data packets such that, to a firewall, they appear to be a SSL TCP session. The modified header preserves the original packet header information within the modified header. Modified packet headers include a masquerade bit which is inserted into the data packet, 210. This masquerade bit acts as a "flag" or "indicator" that the packet header has been modified. To a firewall (like the one shown in Figure 4), the data packet appears to be an SSL protocol session and passes through the firewall unread. Therefore, upon receipt at the firewall, the modified header is identified as an SSL and is directed to

dedicated port 443 in the wall. It passes through that port without further examination to the intended receiver, a node or a NAT/PAT box.

5 The modification of the packet header to appear as a SSL TCP session overcomes problems associated with employing a tunneling scheme, namely TCP stacking, as the packet is transformed as opposed to stacked.

10 Assuming the peer, the intended recipient is logged on to the VPN, the node receives a data packet 252 as shown in Figure 7. When a data packet arrives, the interception mechanism (253) analyses the packet header 254 for the presence of a masquerade bit. This bit is generally located in the TCP options field. If a masquerade bit is not detected, the data packet received by a node 262 and is processed. In the case where the node is located behind a NAT/PAT box, the box receives the data packet. The data packet is processed and decrypted at the box and then sent to the intended node in the clear. In such a case, end to end security is not possible. However, 15 when a masquerade bit is detected 256, it indicates that special processing is required. When the peer is located behind a NAT/PAT box, it is the box that receives the data packet, analyzes the header, and detects the presence of a masquerade bit. In the case where there is no NAT/PAT box, the node performs the analysis and detects the masquerade bit. Once the masquerade bit is found, the modified TCP header is removed 258 to reveal to original header. This original 20 header is examined and the packet is routed to the intended receiving node. In the case where the node is located behind a NAT/PAT box; once the packet is received by the node, the original source IP and port are overwritten with source IP and port from the transformed header to preserve the transformation made by the PAT or NAT device in transit. Further, in the case where the peer is located behind a PAT box, the SA's must also specify the specific peer port 25 number required for the post PAT box connection.

If, in the above circumstance, the node is not logged on to a VPN, the packet is sent and once the peer or intended receiving node logs on to a VPN the packet is received by the peer following the procedure outlined in Figure 7.

30

Figure 8 shows the transformation of a regular data packet 70 illustrated in Figure 8a to a modified data packet 90 illustrated in Figure 8b that was described in Figure 7. The originating data packet 70 has an IP header 72, a TCP header 74, and a data portion 76. In order to facilitate end-to-end security in the presence of a firewall, NAT/PAT box or gateway, the data packet is modified/re-written, as described in Figures 6 step 208. The modified header comprises an IP header 91, a new TCP portion 92, and a data payload 96. The header 91 of the modified packet 90 comprises the original IP header 72 and a TCP portion 92. The TCP portion further includes a new TCP header 93 and a masquerade bit 94. The data payload 96 of the modified pack 90 encapsulates the original TCP header 74 and data 76. On receiving a modified pack, as detailed in Figure 7, the new TCP portion 92 is removed and the packet is processed to reveal the original TCP header 74 and data 76.

On securing a communications path over a public network between two nodes in a computer work group, a typical encryption technique used to transfer data between these nodes includes: generating a data packet to be transmitted over the secured communications path where the data packet includes routing information; encrypting that data packet using an encryption technique known to one skilled in the art; encapsulating the encrypted data packet into a secondary data packet compatible with public network protocols; transmitting the encapsulated data packet over the public network; the data packet arriving at the receiving node; and that receiving node unpacking the encrypted data packet using a set of authentication keys, stripping the second data packet from the original data packet, and decrypting that data packet received from the originating node.

In the preferred embodiment, the system of the present invention is a TCP based n-tier client-server system in which each node is capable of acting as both a client and a server over a single connection. The Distributed Object Architecture (DOA) generally used is a 3rd party implementation of the CORBA 2.3 specification using, for the most part, SSL encrypted BIIOP. In CORBA, interfaces to remote objects are described in a platform-neutral interface definition language. This choice of protocols satisfies the requirement that the protocol operate through most firewalls, since encrypted data cannot be inspected in transit. In addition, the system will use port 443 (fallback to port 7030 if unavailable), such that the session will appear to be a HTTPS session

to firewalls. The use of BIIOP allows both peers to act as a client and server over a single connection which the client initiates to a server, which eliminates more potential firewall problems as incoming socket connections are rarely allowed. The use of the CORBA 2.3 specification, and in particular the new portable object architecture (POA) layer, ensures independence from a particular CORBA implementation such that future implementations may be changed without serious impact on the codebase.

The SSL encryption at the BIIOP layer typically utilises server-side certificates in order to establish upstream trust relationships between peers. A primary data object of the computer system described above is the platform independent servers and related databases, from herein referring to as ENSDataModel class, which contains the following objects and their related methods and attributes:

- nodes (user, server, gateway)
- relationships (VPN membership)

15

Each node of the computer system may instantiate the ENSDataModel class, which abstracts the use of CORBA to communicate with remote instances of the ENSDataModel class.

The ENSDataModel object provides methods for iterating over and retrieving nodes. In addition, the ENSDataModel generally provides two mechanisms for receiving notification of changes to the ENSDataModel. First, methods for “subscribing” to a particular node are provided such that if the target object changes within the filter rules specified, a registered call-back is invoked. In the second method, an ENSDataModel-wide change call-back may be registered, again with filter rules to narrow the notifications to those of interest. This mechanism not only serves the client application but is the mechanism by which the ENSDataModel propagates notification of changes to objects through the hierarchy of nodes.

Another object class in the computer system is denoted is ENSAuth. This object allows the client application to submit its authentication credentials and receive a token that is supplied to the ENSDataModel in order to gain access to the data store. Authentication credentials may also allow a node to act as the authenticator for a particular node or network. In this case, the request will be routed to this node for approval by modifying the appropriate attribute for the object that this node

30

wished to be responsible for authenticating. Authentication may take one of several forms. In its most basic form, credentials are a double consisting of <ID, password>. Some credentials, such as those used for servers or gateways, may be IP restricted. In this case, the credentials are a triple consisting of <ID, password, IP address>. In addition to the above scenarios, the use of certificates
 5 may be employed. If the attributes of a particular VPN specify the use of certificates, then the user's "self" object will indicate that a public/private key pair require generation and the ENSDataModel will deny any requests for data. The public key may then be submitted to the PKI database of the upstream ENS server (through the appropriate ENSDataModel method). The node is then forced to re-authenticate using a signed signature, and checked against the stored public
 10 key. The verification of node credentials may be against internal or external authentication servers.

In the preferred embodiment secure IP communication using end-to-end security between any two nodes 12 over the Internet 22 is established with only minimal assumptions about any particular node's connectivity privileges. This is accomplished by applying IPsec
 15 transformations to incoming and outgoing IP packets at the transport layer and then transforming these processed packets so they appear to be an SSL protocol session until received by the destination node.

The minimum configuration required for a node (base configuration) is defined as follows:

- 20 • An IP address and a connection to the Internet (may be non-unique); and
- Ability to send and receive TCP data on port 443 in SSL format (on some servers may also require the ability to send and receive TCP data in SSL format on a port specified by the server).

The optimal configuration for a node (recommended configuration) is defined as follows:

- 25 • Those abilities defined in the base configuration; and
- A globally routable IP address or 1:1 static NAT.

At least one node in each pair must support at least the recommended configuration, and the other node must support at least the minimum configuration. The system requires that only one of a pair of nodes may be located behind a firewall. The recommended encryption level for data in transit is
 30 3DES. The system, in the preferred embodiment, has accesses to both:

- configuration data (IP addresses, etc) provided by server, client application, and library aforementioned; and
- a packet interception and injection mechanism partially provided by Trilogy AdmitOne

5

A network is created, using the aforementioned technology, consisting of two users who are accessing the service on nodes 'A' and 'B'. Node 'A' operates under at least the "recommended configuration" and node 'B' operates under at least the "base configuration". A mechanism, namely IPSec in the preferred embodiment, is required to determine the connectivity between nodes 'A' and 'B'. If B is behind a NAT or PAT box, then the information may be conveyed via the server during node A's notification of node B's connectivity details (which must include both pre- and post-translated address and port). However if both node 'A' and node 'B' have globally routable IP addresses, and the reason for IPSec connectivity failure is an intermediary firewall, an "IPSec Ping" will need to be employed to detect the failure. This check will be performed by each node, directed at its peer after receiving connectivity state information about the peer and determining that connectivity cannot be determined from that information alone, and before setting up the IPSec SA for the peer. If the IPSec Ping fails, a system for establishing secure communications where connectivity cannot be established is enabled.

Once the lack of connectivity is established, the system is active, and data packets are selected based on SA's set up with the destination addresses of the packets, the destination address being the globally routable IP address of the peer. If the peer is behind PAT box, the SA must also specify a specific peer port number for the post-PAT TCP connection. This value will be stored during the examination of incoming data. Packet headers are rewritten, after ESP processing, to appear as TCP port 443 (HTTPS) packets. However, since the IP header is stripped at the receiving end, any port number can be specified here such that it will allow the packet to traverse firewalls. A client-side option may be specified to set the source port address for system, the default port address is 443, however, that will affect the construction of the packet. The system may incorporate an automatic scanning procedure in order to determine potential candidate ports. On rewriting the packet header, a new TCP header is inserted after the existing IP header. The remainder of the ESP packet becomes "payload". A special "Masquerade Bit" is inserted into the options field of the TCP header. This is the preferred location for the masquerade bit given

that TCP headers with or without options are constant in length while the IP headers will change in length based on the options and the field ought to be observed by routers. When packets arrive at the NAT or PAT box, the system reviews the TCP options field and searches for the presence of a masquerade bit. When the source IP address is the post-PAT address of a peer
5 behind PAT, the source port is examined and a set of SA's are constructed (if one does not already exist) for outgoing data for this particular session. Once a masquerade bit is detected, it indicates to the system to strip off the fake TCP header and begin ESP processing. In the case where the remote node is behind NAT/PAT, the inner source address and port are replaced with the values from the outer TCP header. In this instance the system employs ALGs similar to
10 those found in NAT. In the case of stateful firewalls, data traffic is made to appear as cyclical TCP sessions by varying the control bit field through defined repeating sequences.

The computer system 10 may be run on a diverse set of operating systems and hardware platforms such as open BSD, UNIX, Windows NT, Windows 95/98, Linux, and Solaris.

15

CLAIMS:

1. A method for establishing a system for the secure communications between nodes in a workgroup over a public network by facilitating the creation of a virtual private network, the method comprising the steps of:
 - said method comprising the steps of:
 - a) a client application instructing a library of one of said nodes to form a connection with a server;
 - 10 b) said server authenticating the validity of a credential of one of said nodes and returning data allowing said node to logon to said server;
 - c) synchronization of one of said nodes with said server such that said library of receives a list of VPN's to which said node is a member, their related attributes, status of additional nodes located within the VPN's of which said node is a member, and the related attributes of said
 - 15 additional nodes; and
 - wherein the data store of said server is centrally managed so as to enable the automatic provisioning of security relationships with nodes in a VPN.
- 20 2. The method for establishing the computer system of claim 1, wherein said server enables the automatic and secure exchange of configuration information between said nodes within said workgroup and restricts configuration exchanges based on trust relationship established by said node credentials.
- 25 3. The method for establishing the computer system of claim 1, wherein said library of each of said nodes remains in a loop with said server so as to relay any changes within a VPN to each node within that VPN automatically.
4. The method for establishing the computer system of claim 2, wherein said server
 - 30 automatically sends changes within a VPN to each of said nodes in that VPN.

5. The method for establishing the computer system of claim 2, wherein said client application of one of said nodes automatically pull changes within a VPN from said server so as to update said library of said node.

5 6. A computer system for establishing secure communication between nodes in a workgroup over a public network by facilitating the creation of a virtual private network, the system comprises:

at least three of said nodes in said workgroup connected by said network;

10

one of said nodes is a server, said server for monitoring the automatic distribution of data collected by each of said nodes, said server having a data store linked thereto; and

15

a client application software located at each of said nodes, said client application software including a library having functions related to the operation of said server, said client application capable of communicating with said library through an API;

wherein the data store of said server is centrally managed so as to enable the automatic provisioning of security relationships with nodes in a VPN.

20

7. The computer system of claim 6, wherein said server monitors arbitrary additions, modifications, and alterations to said data store and deploying that information through said server to said nodes within a VPN.

25

8. A method for establishing a system for the secure transfer of data between at least a pair in a workgroup over a public network, where said nodes are members of a virtual private network, the method comprising the steps of:

30

- a) said at least a pair of nodes logging onto a VPN;
- b) a mechanism assessing the connectivity between said at least a pair of nodes and determining the security associations of the same;
- c) modifying packet headers of data packet intended for transfer between nodes to have the appearance of a SSL TCP header; and

wherein said modification of said packet headers facilitates the data flow between nodes to appear as TCP traffic in SSL format.

9. The method for establishing the system of claim 8, wherein said modification of a packet header includes the insertion of a masquerade bit, and wherein said masquerade bit indicates to the receiving node that said data packet has been modified.
10. The method for establishing the system of claim 8, wherein said modified packet header comprises a new TCP header and an original IP header; where said new TCP header is inserted before said original IP header; and wherein the remaining portion of the data packet is an encapsulated secure payload.
11. The method for establishing the system of claim 10, wherein said new TCP header includes a masquerade bit, and wherein said masquerade bit indicates to the receiving node that said data packet has been modified.
12. The method for establishing the system of claim 9, wherein a packet interception mechanism analyses said packet headers for the presence of said masquerade bit.
13. The method for establishing the system of claim 12, wherein, when said masquerade bit is present, said new TCP header is removed and said original IP header routes said data packet to the intended receiver.
14. A computer system for establishing the secure transfer of data between nodes in a workgroup over a public network, where said nodes are members of a VPN, the system comprises:
- at least a pair of said nodes in said workgroup connected by said network;
 - a packet interception mechanism;
 - a mechanism to assess node connective;
 - a mechanism to determine security associations of said nodes;

wherein when a data packet is transferred from one of said pair of nodes to the second of said pair of nodes, if connectivity fails, said packet is intercepted and the packet header portion of said data packet is modified to facilitate the data transfer between said nodes.

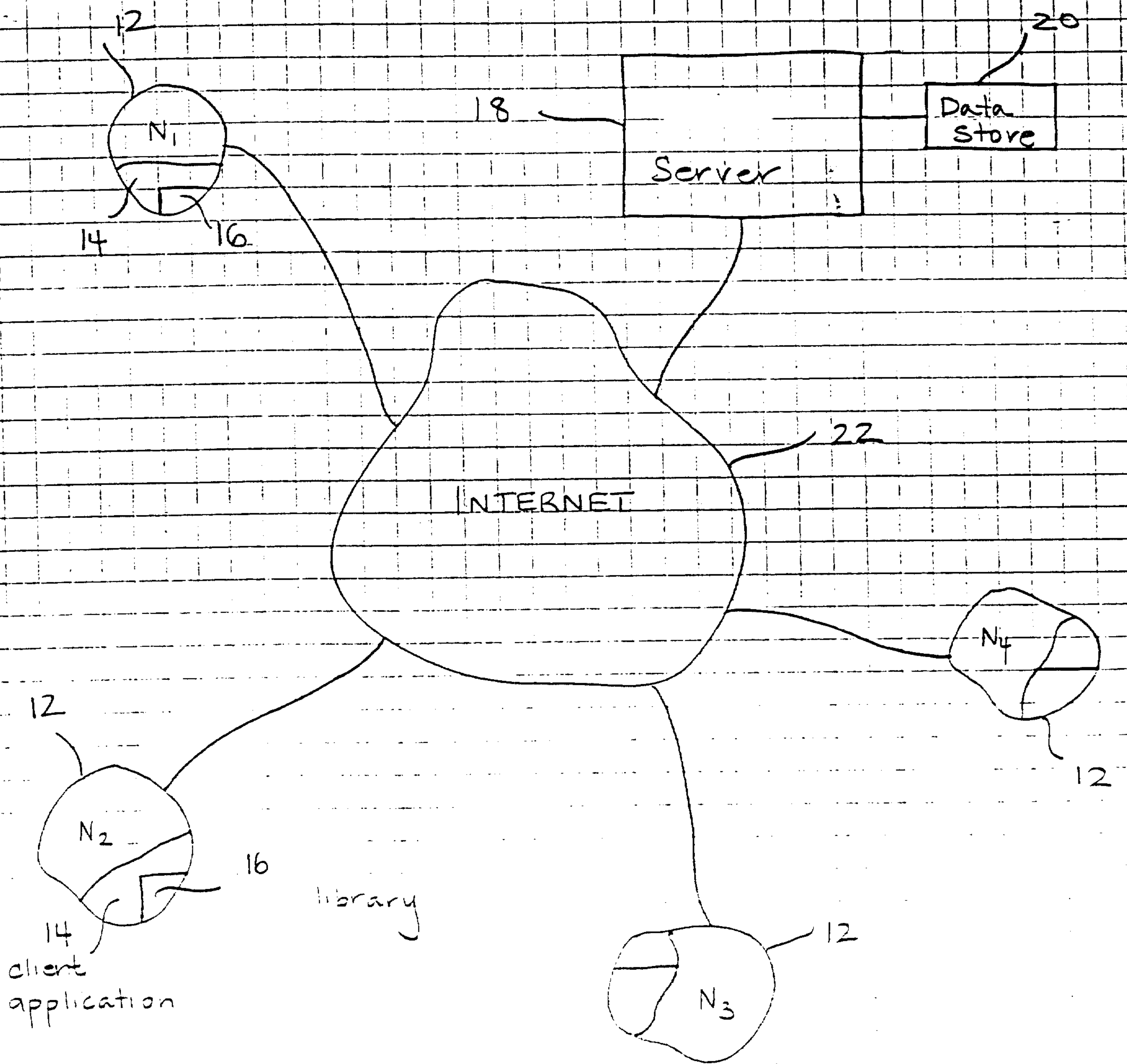


FIG. 1

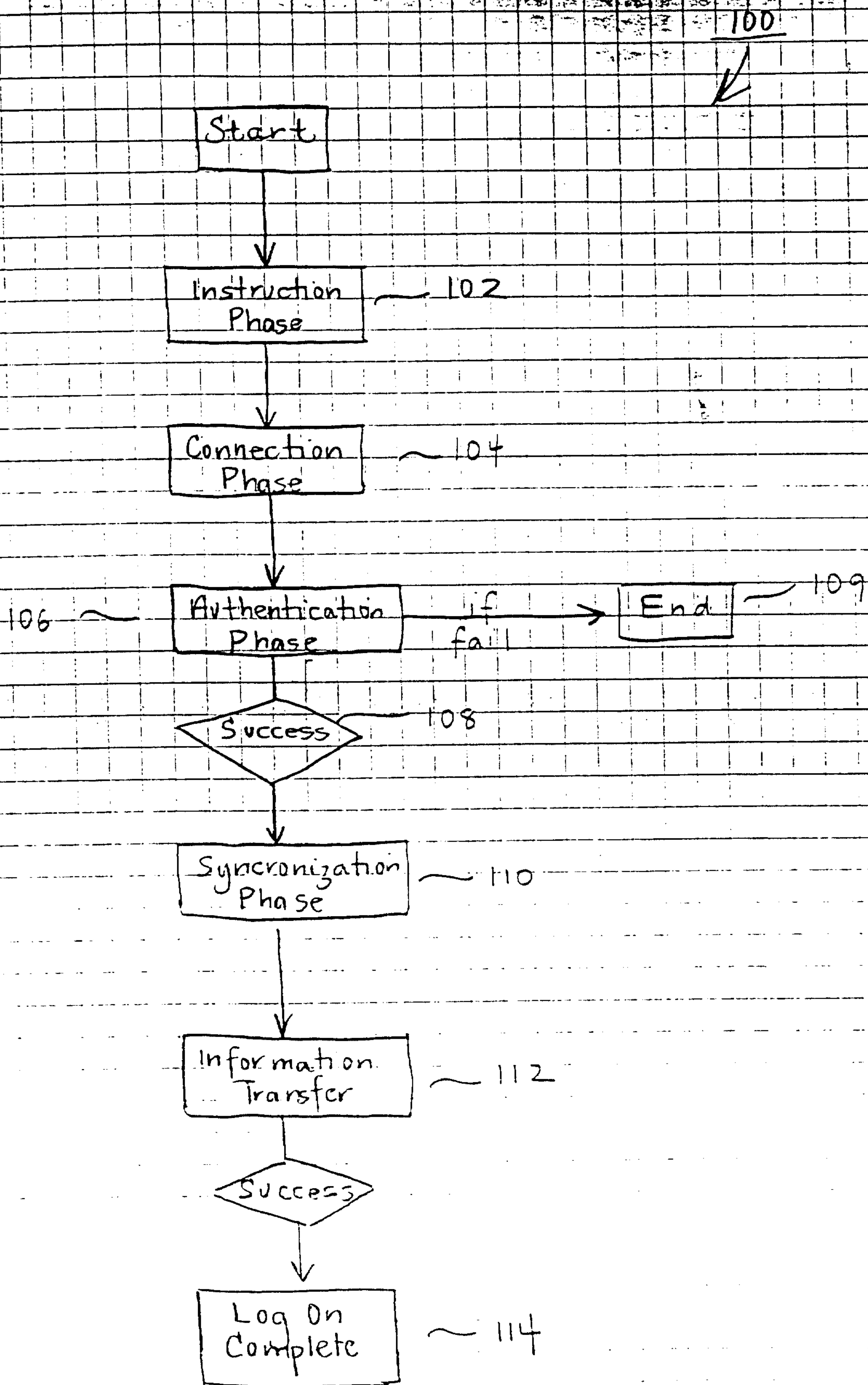


FIG. 2

10

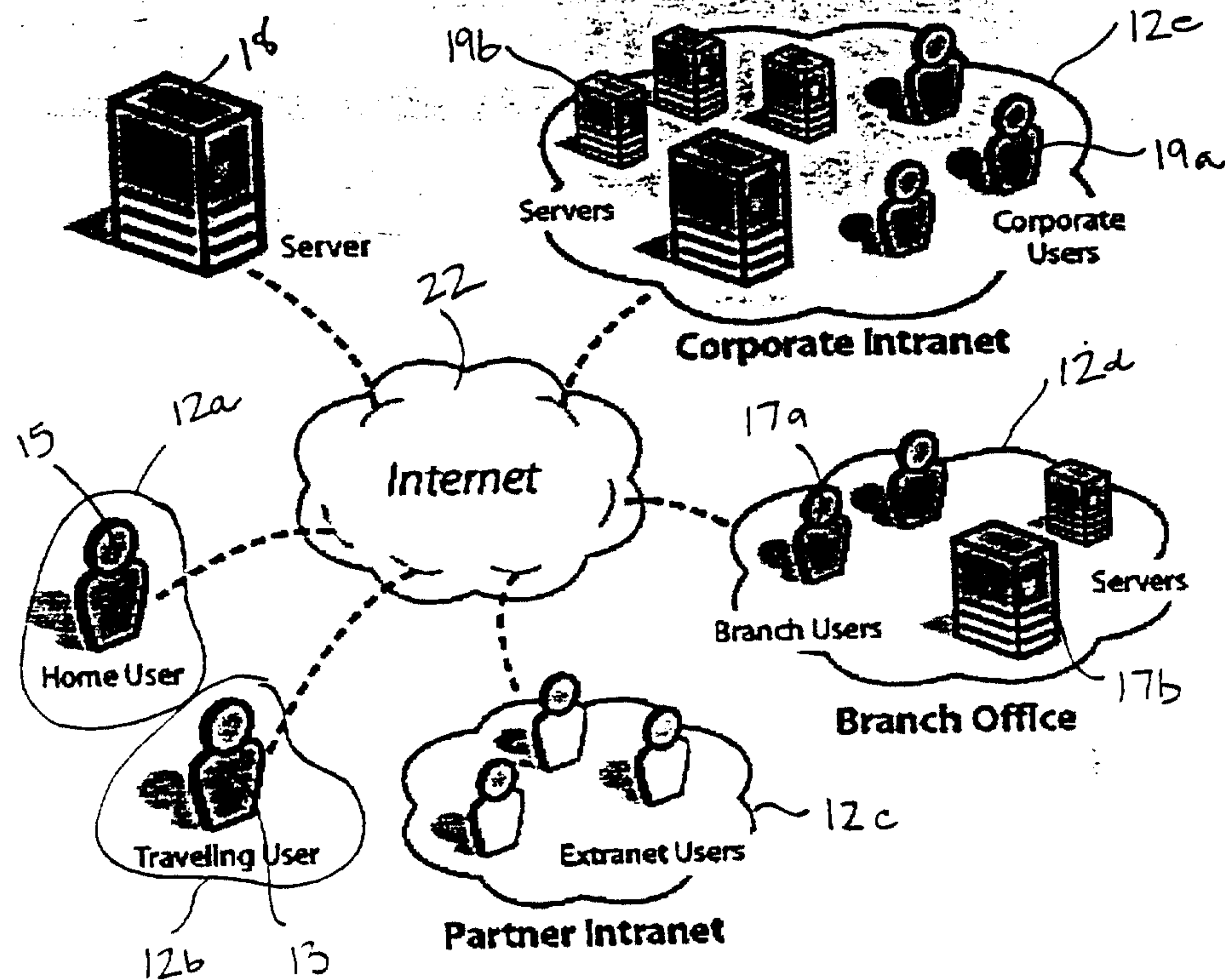


FIG. 3

10

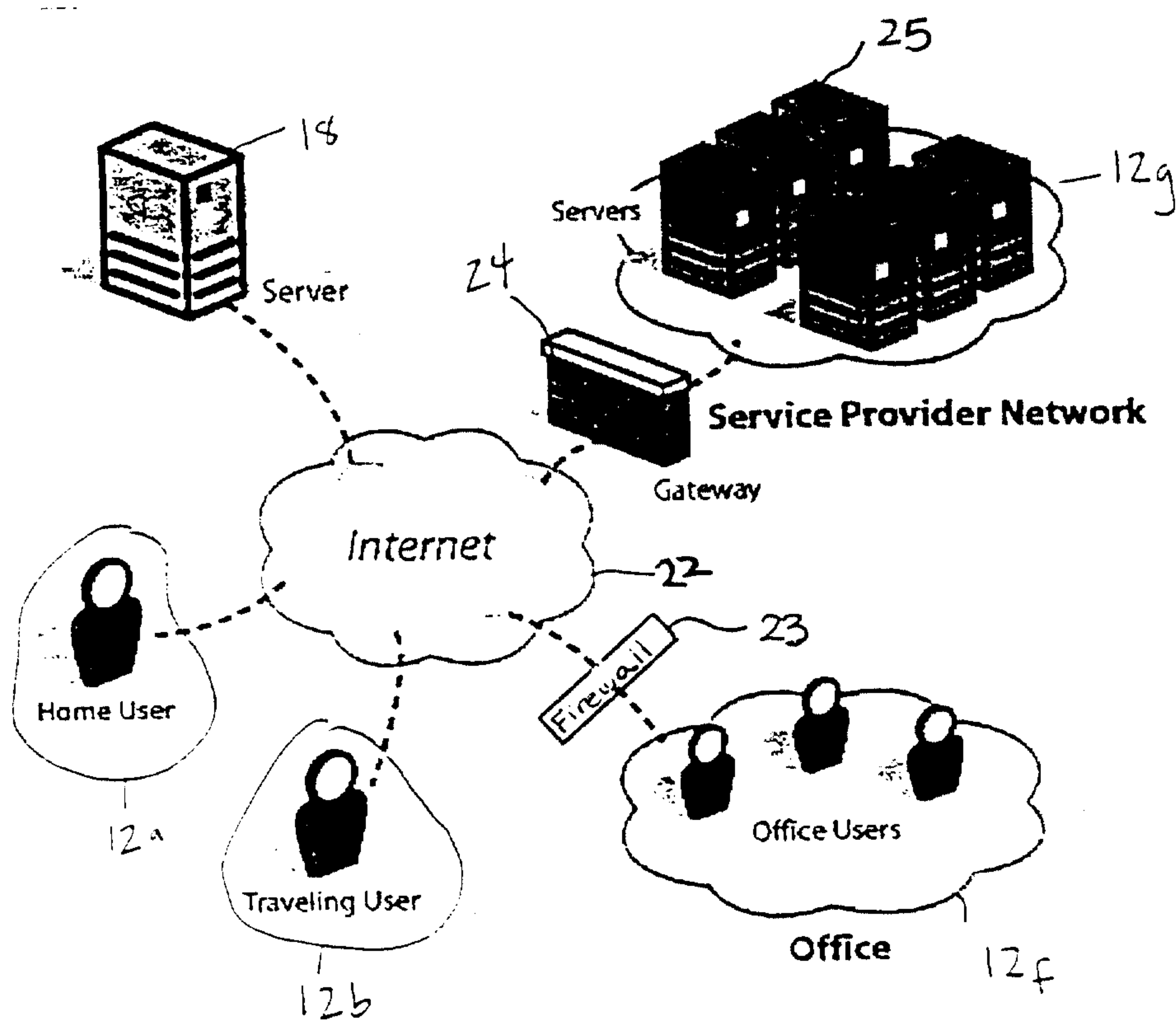


FIG. 4

Operating System Layer

Application Layer

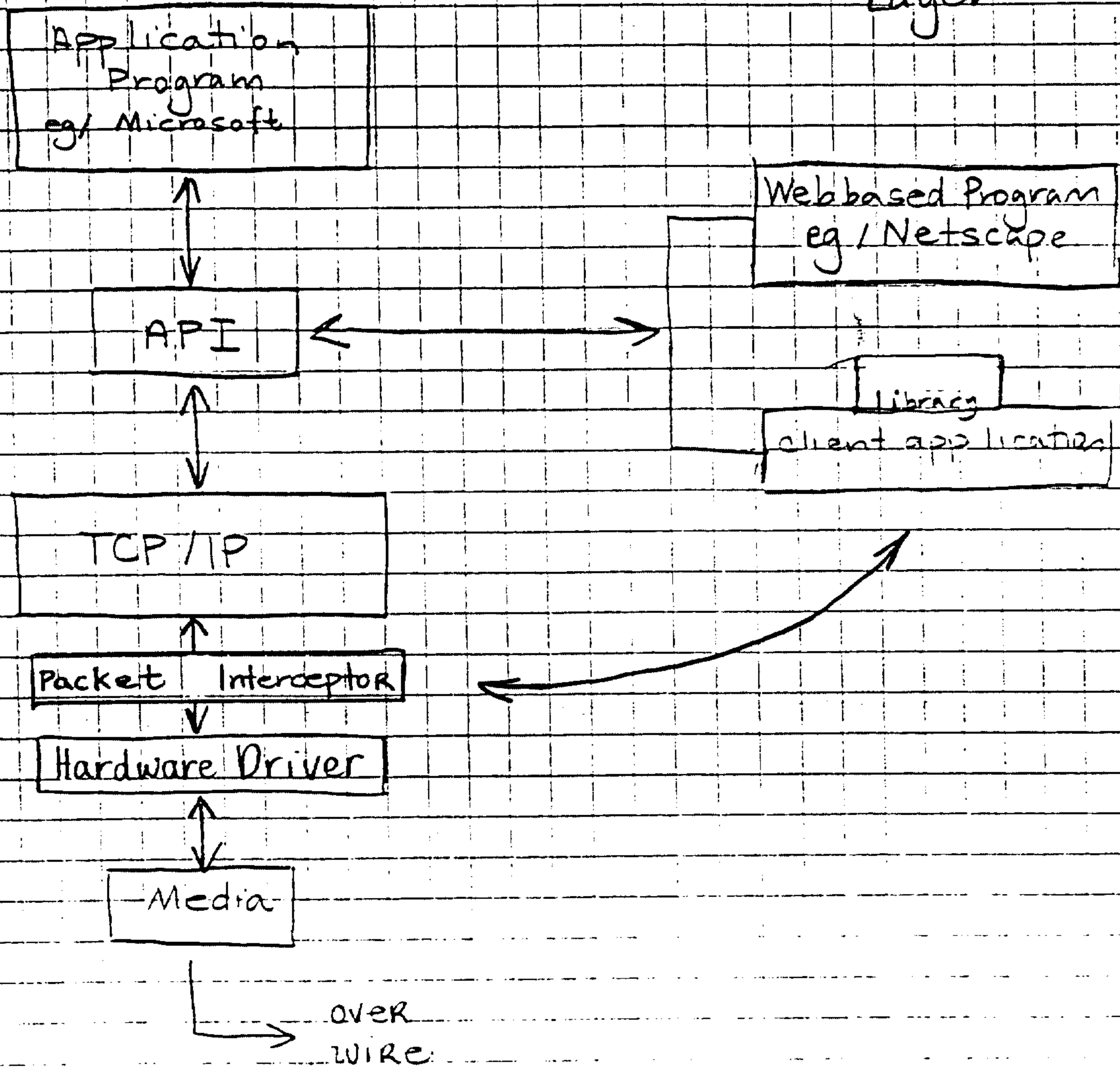


FIG. 5

200

Start

Login to VPN 202

Assess
Connectivity 204

yes

Send
Data 212

No

Assess
SA 206

Intercept 207

Rewrite
Packet
Header 208

Masquerade
Act 1 210

Send Data 212

Fig. 6

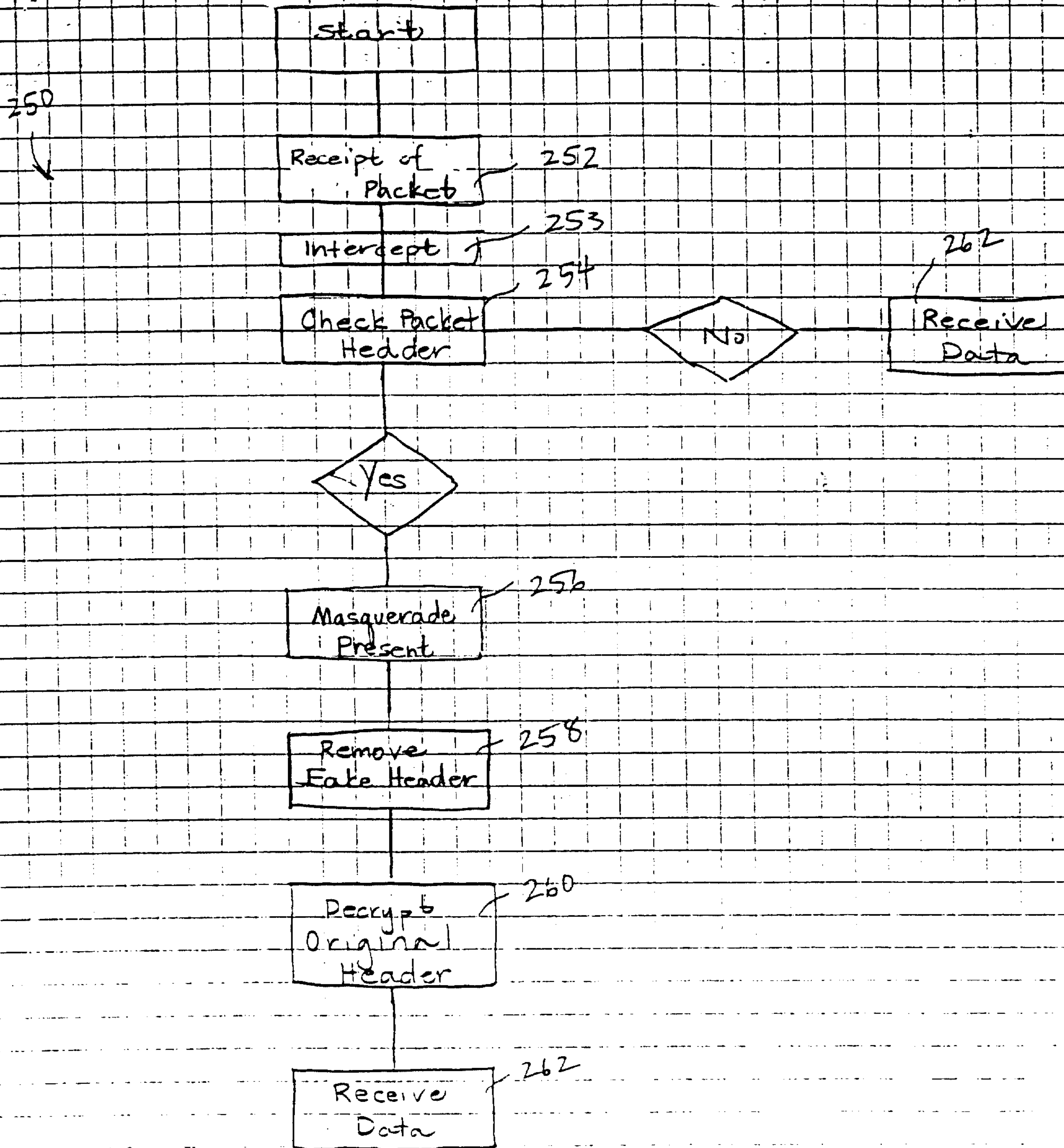
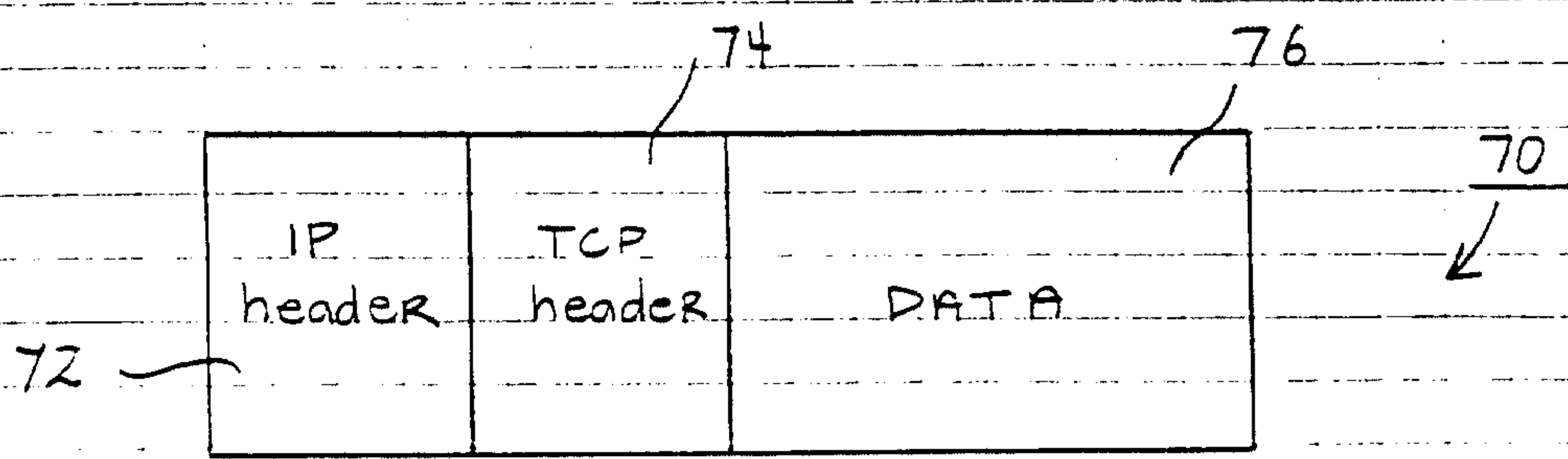


Fig. 7

Fig. 3a



Modify

Fig. 3b

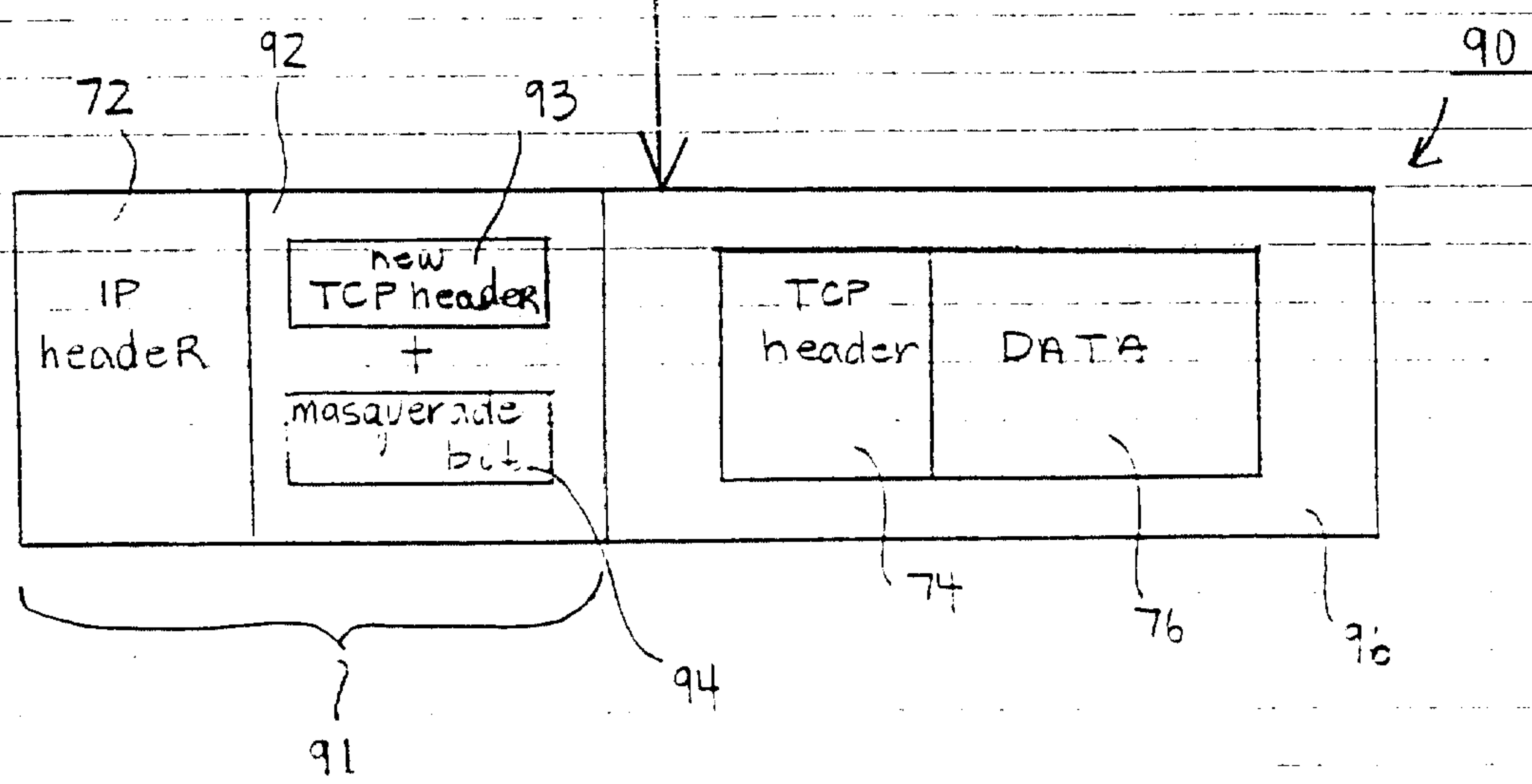


FIG. 3

