```
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a tunnel between hosts
behind SW1
# and hosts behind SW2.
src=172.16.0.0 localSPI=666 peer=192.168.100.5
peerSPI=777 \
     realsrcaddr=192.168.100.5 localaddrs=0.0.0.0
     key=0xdeadbeeffadebabe

#  Hypothetical SW2 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
     realsrcaddr= localaddr= key=

#  The following entry sets up a tunnel between hosts
behind SW1 and
#  hosts behind SW2.
src=172.17.0.0 localSPI=777 peer=192.168.20.1
peerSPI=666 \
     realsrcaddr=192.168.20.1 localaddr=0.0.0.0 \
     key=0xdeadbeeffadebabe
```

With this setup, all traffic is encrypted using one key, no matter who is talking to whom. For example, traffic from H2 to Hl as well as traffic from H3 to Hl will be encrypted with one key. Although this setup is small and simple, it may not be enough.

What happens if H2 cannot trust H3? In this case, the administrator can set up security associations at the host level. In this case, we have to rely on the SPI field of the SA, since the receiving firewall cannot tell from the datagram header which host behind the sending firewall sent the packet. Since the SPI is stored in IPSEC datagrams, we can do a lookup to obtain its value. Below are the sample configuration files for both firewalls again, but this time, each host combination communicates with a different key. Moreover, H2 excludes H3 from communications with Hl, and H3 excludes H2 in the same way.

```
#  Hypothetical SW1 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
and H1
src=172.16.0.2 localSPI=666 peer=192.168.100.5
peerSPI=777 \
     realsrcaddr=192.168.100.5
localaddrs=178.17.128.71 \
     key=0x0a0a0a0a0a0a0a0a

# The following entry sets up a secure link between H3
and H1
src=172.16.0.1 localSPI=555 peer=192.168.100.5
peerSPI=888 \
     realsrcaddr=192.168.100.5
localaddrs=178.17.128.71 \
     key=0x0b0b0b0b0b0b0b0b

#  Hypothetical SW2 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
and H1
src=172.17.128.71 localSPI=777 peer=192.168.20.1
peerSPI=666 \
     realsrcaddr=192.168.20.1 localaddrs=172.16.0.2 \
     key=0x0a0a0a0a0a0a0a0a

# The following entry sets up a secure link between H3
and H1
src=172.17.128.71 localSPI=888 peer=192.168.20.1
peerSPI=555 \
     realsrcaddr=192.168.20.1 localaddrs=172.16.0.1 \
     key=0x0b0b0b0b0b0b0b0b
```

Figure 4 is a block diagram showing in more detail one embodiment of an IPSEC-enabled application level gateway firewall 18. Application level gateway firewall 18 provides access control checking of both encrypted and

unencrypted messages in a more secure environment due to its network-separated architecture. Network separation divides a system into a set of independent regions or burbs, with a domain and a protocol stack assigned to each burb. Each protocol stack 40x has its own independent set of data structures, including routing information and protocol information. A given socket will be bound to a single protocol stack at creation time and no data can pass between protocol stacks 40 without going through proxy space. A proxy 50 therefore acts as the go-between for transfers between domains. Because of this, a malicious attacker who gains control of one of the regions is prevented from being able to compromise processes executing in other regions. Network separation and its application to an application level gateway is described in "SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION", U.S. Application No. 08/599,232, filed February 9, 1996 by Gooderum et al.

In the system shown in Figure 4, the in-bound and out-bound datagram processing of a security association continues to follow the conventions defined by the network separation model. Thus all datagrams received on or sent to a given burb remain in that burb once decrypted. In one such embodiment SADB socket 78 has been defined to have the type 'sadb'. Each proxy 50 that requires access to SADB socket 78 to execute its query as to whether the received message was encrypted must have create permission to the sadb type.

The following is list of specific requirements that a system such as is shown in Figure 4 must provide. Many of the requirements were discussed in the information provided earlier in this document.

1. Firewall applications may query the IPSEC subsystem to determine if traffic with a given address is guaranteed to be encrypted.
2. Receipt of an unencrypted datagram from an address that has a SA results in the datagram being dropped and an audit message being generated.
3. On receipt of encrypted protocol datagrams the SADB searches will be done using the SPI as the primary key. The source address will a secondary key. The SA returned by the search will be the SA which matches the SPI exactly and has the longest match with the address.

4. A search of the SADB for a SPI that finds an entry that is marked as SA for a dynamic IP will not consider the address in the search process.

5. A search of the SADB for a SPI that finds an entry that is marked as a SA for a tunnel mode connection will to consider the address if it is (0.0.0.0) i.e INADDR.

6. On receipt of a non-IPSEC datagram the SADB will be searched for an entry that matches the src address. If a SA is found the datagram will be dropped and an audit message sent.

7. SADB searches on output will be done using the DST address as key. If more than one SA entry in the SADB has that address the first one with the maximum address match will be returned.

8. The SADB must be structured so that searches are fast regardless if the search is done by SPI or by address.

9. The SADB must provide support for connections to a site with a fixed SPI but changing IP address. SA entries for such connections will be referred to as Dynamic Address Sites, or just Dynamic entries.

10. When a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted, will be recorded in the SA only after the AH checking has passed successfully. (This is because if the address is recorded before AH passes then an attacker can cause return packets of an outgoing connection to be transmitted in the clear.)

11. A failure of an AH check on a dynamic entry results in an audit message.

12. In an embodiment where the firewall requires that all connections use both AH and ESP, on receipt the order should be AH first ESP second.

13. The processing structure on both input and output should try to minimize the number of SADB required lookups.

Returning to Figure 4, in one embodiment firewall 18 includes a crypto engine interface 80 used to encrypt an IPSEC payload. Crypto engine interface 80 may be connected to a software encryption engine 82 or to a hardware

encryption engine 84. Engines 82 and 84 perform the actual encryption function using, for example, DES-CBC. In addition, software encryption engine 82 may include the keyed MD5 algorithm used for AH.

In one embodiment, crypto engine interface 80 is a utility which provides a consistent interface between the software and hardware encryption engines. As shown in Figure 4, in one such embodiment interface 80 only supports the use of the use of hardware cryptographic engine 84 for IPSEC ESP processing. The significant design issue that interface 80 must deal with is that use of a hardware encryption engine requires that the processing be down in disjoint steps operating in different interrupt contexts as engine 84 completes the various processing steps.

The required information is stored in a request structure that is bound to the IP datagram being processed. The request is of type `crypto_request_t`. This structure is quite large and definitely does not contain a minimum state set.

In addition to the definition of the request data structure, this software implementing interface 80 provides two functions which isolate the decision of which cryptographic engine to use. The `crypt_des_encrypt` function is for use by the IP output processing to encrypt a datagram. The `crypt_des_decrypt` function is for use by the IP input processing to decrypt a datagram. If hardware encryption engine 84 is present and other hardware usage criteria are met the request is enqueued on a hardware processing queue and a return code indicating that the cryptographic processing is in progress is returned. If software engine 82 is used, the return code indicates that the cryptographic processing is complete. In the former case, the continuation of the IP processing is delayed until after hardware encryption is done. Otherwise it is completed as immediately in the same processing stream.

There are two software cryptographic engines 82 provided in the IPSEC software. One provides the MD5 algorithm used by the IPSEC AH processing, and the other provides the DES algorithm used by the IPSEC ESP processing. This software can be obtained from the US Government IPSEC implementation.

In one embodiment hardware cryptographic engine 84 is provided by a Cylink SafeNode processing board. The interface to this hardware card is provided by the Cylink device driver. A significant aspect of the Cylink card that plays a major part in the design of the IPSEC Cylink driver is that the card functions much like a low level subroutine interface and requires software support to initiate each processing step. Thus to encrypt or decrypt an individual datagram there are a minimum of two steps, one to set the DES initialization vector and one to do the encryption. Since the IP processing can not suspend itself and wait while the hardware completes and then be rescheduled by the hardware interrupt handler, in one embodiment a finite state machine is used to tie sequences of hardware processing elements together. In one such embodiment the interrupt handler looks at the current state, executes a defined after state function, transitions to the state and then executes that state's start function.

One function, `cyl_enqueue_request`, is used to initiate either an encrypt or a decrypt action. This function is designed to be called by cryptographic engine interface 80. All of the information required to initiate the processing as well as the function to be performed after the encryption operation is completed is provided in the request structure. This function will enqueue the request on the hardware request queue and start the hardware processing if necessary.

A system 30 which can be used for firewall-to-workstation encryption is shown in Figure 5. In Figure 5, system 30 includes a workstation 12 communicating through a firewall 14 to an unprotected network 16 such as the Internet. System 30 also includes a workstation 32 communicating directly with firewall 14 through unprotected network 16. Firewall 14 is an application level gateway incorporating IPSEC handling as described above. (It should be noted that IPSEC security cannot be used to authenticate the personal identity of the sender for a firewall to firewall transfer. When IPSEC is used, however, on a single user machine such as a portable personal computer, IPSEC usage should

be protected with a personal identification number (PIN). In these cases IPSEC can be used to help with user identification to the firewall.)

According to the IPSEC RFC's, you can use either tunnel or transport mode with this embodiment based on your security needs. In certain situations, the communications must be sent in tunnel mode to hide unregistered addresses.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiment shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is intended that this invention be limited only by the claims and the equivalents thereof.

What is claimed is:

1. A method of regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

determining, at the IP layer, if a message is encrypted;

if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy; and

if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message.

2. A method of authenticating the sender of a message within a computer system having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

determining, at the IP layer, if the message is encrypted;

if the message is encrypted, decrypting the message, wherein the step of decrypting the message includes the step of executing a process at the IP layer to decrypt the message;

passing the decrypted message up the network protocol stack to an application level proxy;

determining an authentication protocol appropriate for the message; and

executing the authentication protocol to authenticate the sender of the message.

3. The method according to claim 2 wherein the step of determining an authentication protocol appropriate for the message includes the steps of:

determining a source IP address associated with the message; and

determining the authentication protocol associated with the source IP address.

4. The method according to claim 2 wherein the message includes security parameters index and wherein the step of determining an authentication protocol appropriate for the message includes the steps of:

determining the authentication protocol associated with a dynamic IP address, wherein the step of determining the authentication protocol includes the step of looking up a security association based on the security parameters index;

determining a current address associated with the dynamic source IP address; and

binding the current address to the security parameters index.

5. A firewall, comprising:

a first communications interface;

a second communications interface;

a network protocol stack connected to the first and the second communications interfaces, wherein the network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a decryption procedure, operating at the IP layer, wherein the decryption procedure decrypts encrypted messages received at one of said first and second communications interfaces and outputs decrypted messages; and

a proxy, connected to the transport layer of said network protocol stack, wherein the proxy receives decrypted messages from the decryption procedure and executes an authentication protocol based on the content of the decrypted message.

6. A firewall, comprising:

a first communications interface;

a second communications interface;

a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and

a proxy, connected to the transport layers of said first and second network protocol stacks, the proxy receiving decrypted messages from the decryption procedure and executing an authentication protocol based on the content of the decrypted message.

7. The firewall according to claim 6 wherein the firewall further includes:

a third communications interface; and

a third network protocol stack connected to the third communications interface and to the proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively.

8. A method of establishing a virtual private network between a first and a second network, wherein each network includes an application level gateway firewall which uses a proxy operating at the application layer to process traffic through the firewall, wherein each firewall includes a network protocol stack and wherein each network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

transferring a connection request from the first network to the second network;

determining, at the IP layer of the network protocol stack of the second network's firewall, if the connection request is encrypted;

if the connection request is encrypted, decrypting the request, wherein the step of decrypting the request includes the step of executing a procedure at the IP layer of the second network's firewall to decrypt the message;

passing the connection request up the network protocol stack to an application level proxy;

determining an authentication protocol appropriate for the connection request;

executing the authentication protocol to authenticate the connection request; and

if the connection request is authentic, establishing an active connection between the first and second networks.

9. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code within the firewall of the second network to mimic a challenge/response protocol executing on a server internal to the second network.

10. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code to execute the authentication protocol in line to the session.

11. The method according to claim 8 wherein the step of determining an authentication protocol includes the step of determining if the connection request arrived encrypted and selecting the authentication protocol based on whether the connection request was encrypted or not encrypted.

The Patent Office

28

Application No: GB 9719816.2 **Examiner:** B.J.SPEAR
Claims searched: 1-11 **Date of search:** 21 January 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PPEB,PDCSA,PDCSC)

Int Cl (Ed.6): H04L 9/00, 9/32, 29/06, 29/08

Other: Online:WPI, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
XP	WO97/26734A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 6-12	1,2.5,6,8 at least
XP	WO97/26731A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 7-12	1,2.5,6,8 at least
XP	WO97/26735A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 4-10	1,2.5,6,8 at least
XP	WO97/23972A1	(V-ONE Corp) Whole document, eg Figs 1,2 and claim 1.	1,2.5,6,8 at least
XP	WO97/13340A1	(Digital Secured Networks) Whole document, eg pages 7-13	1,2.5,6,8 at least

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family

A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04Q 11/04, H04L 12/22**

A1

(11) International Publication Number: **WO 98/27783**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/IB97/01563

(22) International Filing Date: 12 December 1997 (12.12.97)

(30) Priority Data:
08/769,649 19 December 1996 (19.12.96) US

(71) Applicant *(for all designated States except US)*: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: TELLO, Antonio, G. [US/US]; 114 Fountain Hills Drive, Garland, TX 75044 (US). HUI, Margaret [US/US]; 9920 Forest Lane #208, Dallas, TX 75243 (US). HOLMES, Kim [US/US]; 5409 Scenic Drive, Rowlett, TX 75088 (US).

(74) Agents: MCCOMBS, David et al.; Haynes and Boone, L.L.P., Suite 3100, 901 Main Street, Dallas, TX 75202–3789 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

(57) Abstract

A virtual private network service provider is used to transfer data over a data network to a final destination, with third–party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; sending a set–up message to the data network; selecting a virtual private network provider through the data network; the virtual private network provider giving an encryption key to the user, and then prompting the user for a password and a user identification; encrypting the password, and sending the user identification and the encrypted password to the virtual private network provider; the virtual private network provider decrypting the encrypted password, and verifying the password; the virtual private network provider providing an authorization code; and the data terminal transferring the data through the data network to the final destination, using the authorization code.

FOR THE PURPOSES OF INFORMATION ONLY

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

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

VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

Technical Field

The invention relates generally to asynchronous transfer mode ("ATM") networks and virtual private networks ("VPN"), such as those offered by MCI and Sprint, and, more particularly, to a method of using a VPN to transfer data over a data network, with third-party billing.

Background of the Invention

Telephone service providers offer third-party billing. For example, local and long distance telephone companies offer calling cards for third party billing.

VPNs exist to provide the sense of a private network among a company's locations. The lines/trunks of a VPN are actually shared among several companies, to reduce costs, yet to each company the VPN appears to be that company's own private network. However, a user at a remote data terminal, such as a portable computer in a hotel room, can not immediately charge his company for the access time to a data net, such as the Internet. Instead, his access time is charged to his hotel room, and so he must pay the inflated rates that hotels charge for phone service.

What is needed is a VPN service provider that offers remote access for users belonging to a VPN, user authorizations to prevent delinquent access into the VPN, and convenient third-party billing.

Summary of the Invention

The present invention, accordingly, provides a system and method for using a VPN service provider to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; selecting a VPN through the data network; giving an encryption key to the user, and then prompting the user for a password and a user identification; verifying the password, and providing an authorization code to

the user; and allowing the user to transfer the data through the data network to the final destination, using the authorization code.

In another feature of the invention, the method further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

In another feature of the invention, the method further comprises encrypting the user's password, and sending the user identification and the encrypted password to the VPN service provider.

In another feature of the invention, the method further comprises a step of sending a set-up message to the data network.

In another feature of the invention, the method further comprises a step of the VPN service provider decrypting the encrypted password.

A technical advantage achieved with the invention is that it shifts or defers costs from an end user to a bulk purchaser of data network services. Another technical advantage achieved with the invention is that it permits end users mobility while attaining a virtual appearance on a corporate intranet.

Brief Description of the Drawings

Fig. 1 is a system block diagram of a VPN service provider of the present invention.

Fig. 2 is a flow chart depicting the method of the present invention, as implemented by application software on a user terminal.

Fig. 3 is the initial screen display of the user interface of the application software.

Figs. 4A and 4B are call flow diagrams, illustrating the preferred sequence of steps of the method of the present invention.

Figs. 5A, 5B, 5C, 5D, 5E, and 5F comprise a flow chart depicting the method of the present invention, as implemented by switching control point software.

Description of the Preferred Embodiment

In Fig. 1, the VPN service provider system of the present invention is designated generally by a reference numeral 10. The VPN service provider system 10 includes a VPN 12. The VPN 12 may be a corporate, government, association, or other organization's telephone/data line network. The VPN service provider system 10 also includes access lines 13 from the VPN 12 to a data network 14, such as the Internet, or an ATM network. The VPN service provider system 10 also includes access lines 16 from the data network 14 to a long distance phone company 18, such as AT&T, MCI, or Sprint. The VPN service provider system 10 also includes access lines 20 from the data network 14 to a called party 22, such as, for example, American Express reservations service. The VPN service provider system 10 also includes access lines 24 from the data network 14 to a remote user terminal 26, such as a portable computer in a hotel room. The user terminal 26 includes user application software 28, which provides the interface for the user to enter the number to be called, the user identification number, and the user's authorization code. The VPN service provider system 10 also includes VPN service provider software 30, located in a switching control point (SCP) device 32, which, in the preferred embodiment may be physically located anywhere. The SCP 32 connects to the data network 14 via access lines 36. One possible physical location for the SCP 32 is on the premises of a local phone company central switch building 34. However, even when located within the building 34, the SCP 32 connects to the local phone company switches via the data network 14. The local phone company switches connect to the data network 14 via access lines 38.

In an alternate embodiment, the VPN service provider software 30 and the SCP device 32 may be located on the premises of an independent provider of local phone service, or on the premises of an independent VPN service provider.

Referring now to Fig. 2, the application software 28 begins the data transfer process in step 50. In step 52, the user is presented with a screen display.

Referring now to Fig. 3, a screen display 100 displays the following information requests: whether the call is a direct call 102 or a VPN call 104, the number the user desires to call 106, the VPN user ID 108, and the user password 110. The user is also presented with the option to make the call 112, or to quit 114.

Referring back to Fig. 2, in step 54 the user terminal sends to the SCP 32 the information captured through the graphical user interface ("GUI") in step 52 within a user network interface ("UNI") setup message. In step 56 the user terminal 26 waits for a connect message from the SCP 32. In step 58 the user terminal 26 determines if a connection was made. If no connection was made, then in step 60 the user application software 28 displays an error message to the user, and returns to step 50 to begin again the data transfer process.

If a connection was made, then in step 62 the user terminal 26 sends the VPN user ID to the SCP 32. In step 64 the user terminal 26 waits for an encryption key from the SCP 32. In step 66, having received the encryption key from the SCP 32, the user application software 28 encrypts the user's password, and sends it to the SCP 32. In step 68 the user terminal 26 waits for authentication of the user. In step 70 the user application software 28 determines if the SCP 32 authorizes the user to make the call.

If the user is not authorized, then in step 72 the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If the user is authorized, then in step 74 the VPN service provider software 30 sets up the billing, and authorizes it. In step 76 the user terminal 26 sends a "release", meaning to terminate or disconnect the connection, to the SCP 32. In step 78 the user terminal 26 sends a setup message to the number listed by

the user as the "number to call", that is, to the final destination. In step 80 the user terminal 26 waits for a connection. In step 82 the user terminal 26 determines if a connection was made.

If a connection to the final destination was not made, then the user application software 28 returns to step 72, in which step the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If a connection to the final destination was made, then in step 84 the user terminal 26 exchanges user data, services, and/or value added or user specific applications with the computer at the address, that is, the telephone number, of the final destination. In step 86 the user selects the option presented to him to release, or terminate, the call. In step 88 the user terminal 26 sends a release message to the final destination. In step 90 the data network 14 sends billing information to the SCP 32. In step 92 the application software 28 ends the data transfer process.

Fig. 4A and Fig. 4B are call flow diagrams, showing the sequence of messages in the method of the preferred embodiment. These diagrams present the same method as the flow chart of Fig. 2. The horizontal arrows represent the messages sent and received. The vertical lines represent the various devices involved in sending and receiving the messages. For example, the top left arrow in Fig. 4A represents a message sent from the user terminal 26, labeled "Macintosh" in Fig.4A, to an interface with a public network. The user terminal 26 can be any brand of a work station computer, a desktop computer, a laptop computer, or even a notebook computer. The interface could be any interface, but in the example of Fig. 4A and Fig. 4B, the interface is imagined to be at a hotel, where a business traveler is using the method of the present invention. Thus, the interface is labeled "Hotel ATM Interface", which is not shown in Fig. 1. The vertical line labeled "Public ATM Network" is the same as the data network 14 in Fig. 1. The vertical line labeled "Moe's VPN Service" represents the VPN service provider software 30

within the SCP 32. The vertical line labeled "Travel ATM Interface" is not shown in Fig. 1, but is located between the called party 22 and the data network 14. The vertical line labeled "Travel Service" is one example of the called party 22 shown in Fig. 1. In the example of Fig. 4A and Fig. 4B, the business traveler is imagined to be using the method of the present invention to contact a travel service to make reservations for his next airline flight. In Figs. 4A and 4B the designation "Ack" represents "acknowledge", and the designation "Cmp" represents "complete".

Referring now to Fig. 5, the VPN service provider software 30 begins the data transfer process in step 300 by waiting for an event. The event it waits for is a setup message on a signaling port of the SCP 32, to be received from the user terminal 26. In step 302, having monitored the signaling ports, and the SCP 32 having received a setup message, the VPN service provider software 30 assigns a call condense block ("CCB") to the setup message, based on a call reference number. The CCB is a software data structure for tracking resources associated with the call. The call reference number is a number, internal to the SCP, for tracking calls. In step 304 the VPN service provider software 30 compiles the connect message. In step 306 the VPN service provider software 30 sends a connect message to the calling address, that is, the hotel room from which the user is calling. In step 308 the VPN service provider software 30 condenses, that is, it remains in a wait state for that call.

Referring now to Fig. 5B, in step 310 the VPN service provider software 30 waits for an event by monitoring the signaling ports of the SCP 32. After the SCP 32 receives a connect acknowledge message from the user terminal 26, then in step 312 the VPN service provider software 30 accesses the CCB, based on the call reference number. In step 314 the VPN service provider software 30 condenses.

Referring now to Fig. 5C, in step 316 the VPN service provider software 30 waits for dialog on a data port of the SCP 32. After the SCP 32 receives a

VPN ID on a data port, the VPN service provider software 30 verifies the VPN ID in step 318. In step 320 the VPN service provider software 30 determines if the VPN ID is valid. If the VPN ID is not valid, then in step 322 the SCP 32 sends a reject message over an assigned switch virtual circuit ("SVC"). The SVC is a channel over the data network 14. In step 324 the VPN service provider software 30 waits for dialog. In step 326, because the VPN ID is valid, the VPN service provider software 30 assigns an encryption key to the user terminal 26, in step 328 sends the encryption key over the assigned SVC to the user terminal 26, and in step 330 waits for dialog.

Referring now to Fig. 5D, in step 332 the VPN service provider software 30 waits for dialog. When the SCP 32 receives the encrypted password from the user terminal 26 at a data port, then in step 334 the VPN service provider software 30 verifies the password, and determines in step 336 if the password is valid. If the password is not valid, then in step 338 the SCP 32 sends a reject message over the assigned SVC to the user terminal, and in step 340 waits for dialog. If the password is valid, then in step 342 the VPN service provider software 30 assigns an authorization token to the user terminal 26, in step 344 sends the token over an assigned SVC to the user terminal 26, and in step 346 waits for dialog.

Referring now to Fig. 5E, in step 348 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a release message from the user terminal 26, then in step 350 the VPN service provider software 30 accesses the CCB, based on the call reference number of the user terminal 26, in step 352 compiles a release complete message, in step 354 sends a release complete message to the user terminal 26, and in step 356 condenses.

Referring now to Fig. 5F, in step 358 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a third-party billing setup message from the user terminal 26, then in step 360 the VPN service provider

software 30 verifies the token just received from the user terminal 26, to determine, in step 362, if it is the same token that the VPN service provider software 30 sent to the user terminal 26 in step 344. If the token is not valid, then in step 364 the SCP 32 sends a release message to the terminal 26, and in step 366 condenses. If the token is valid, then in step 368 the SCP 32 sends a modified third-party billing setup message to the data network 14, and in step 370 condenses.

Although an illustrative embodiment of the invention has been shown and described, other modifications, changes, and substitutions are intended in the foregoing disclosure. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

WHAT IS CLAIMED IS:

1. A computerized method of a virtual private network service provider with third party billing, using a virtual private network to transfer data over a data network to a final destination, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

2. The method of claim 1, wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

3. The method of claim 2, wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

4. The method of claim 3, further comprising, after step (a), the step of sending a set-up message to the data network.

5. The method of claim 4, further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

6. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. an interface between the user terminal and the data network;

b. a switching control point device connected to the data network, the switching control point device connected to a computer; and

c. a computer-readable medium encoded with a method of using the virtual private network and the data network, with third party billing, the computer-readable medium accessible by the computer.

7. The apparatus of claim 6, wherein the method comprises negotiating for more bandwidth for the user, and including within an authorization code a grant of additional bandwidth.

8. The apparatus of claim 7, wherein the method further comprises encrypting a user's password, and temporarily storing the user identification and the encrypted password.

9. The apparatus of claim 8, wherein the method further comprises sending a set-up message to the data network.

10. The apparatus of claim 9, wherein the method further comprises decrypting the encrypted password.

11. A computer-readable medium encoded with a method of using a virtual private network, with third party billing, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

12. The computer-readable medium of claim 11 wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

13. The computer-readable medium of claim 12 wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

14. The computer-readable medium of claim 13 further comprising, after step (a), the step of sending a set-up message to the data network.

15. The computer-readable medium of claim 14 further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

16. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. means for prompting a user at the data terminal to select a destination, password, and call type;

b. means for selecting the virtual private network through the data network;

c. means for giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. means for verifying the password, and providing an authorization code to the user; and

e. means for allowing the user to transfer data through the data network to a final destination, using the authorization code.

17. The apparatus of claim 16, further comprising means for negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

18. The apparatus of claim 17, further comprising means for encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

19. The apparatus of claim 18, further comprising means for sending a set-up message to the data network.

20. The apparatus of claim 19, further comprising means for decrypting the encrypted password.

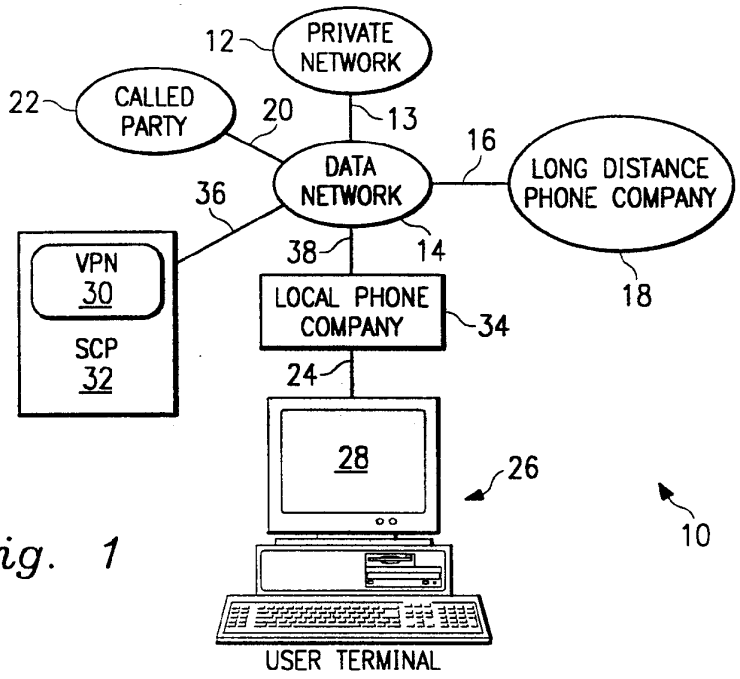

12
PRIVATE NETWORK
22
CALLED PARTY
20
13
16
DATA NETWORK
LONG DISTANCE PHONE COMPANY
36
38
14
18
VPN 30
SCP 32
LOCAL PHONE COMPANY
34
24
28
26
10
USER TERMINAL

Fig. 1

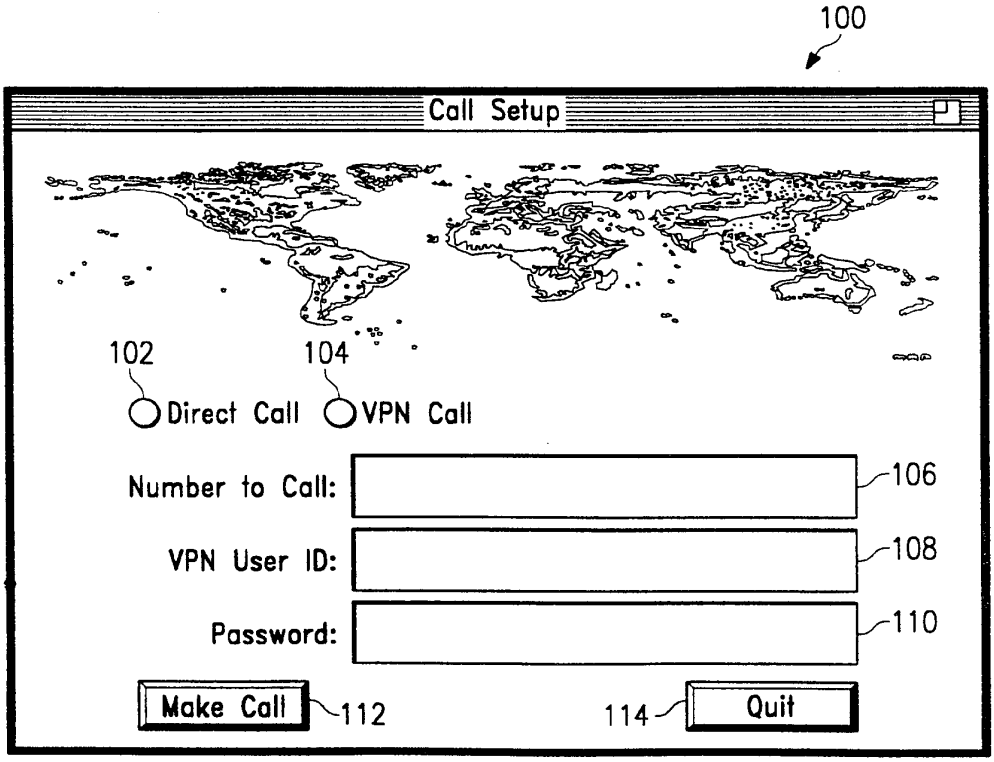

100
Call Setup
102
104
Direct Call
VPN Call
Number to Call:
106
VPN User ID:
108
Password:
110
Make Call
112
114
Quit

Fig. 3

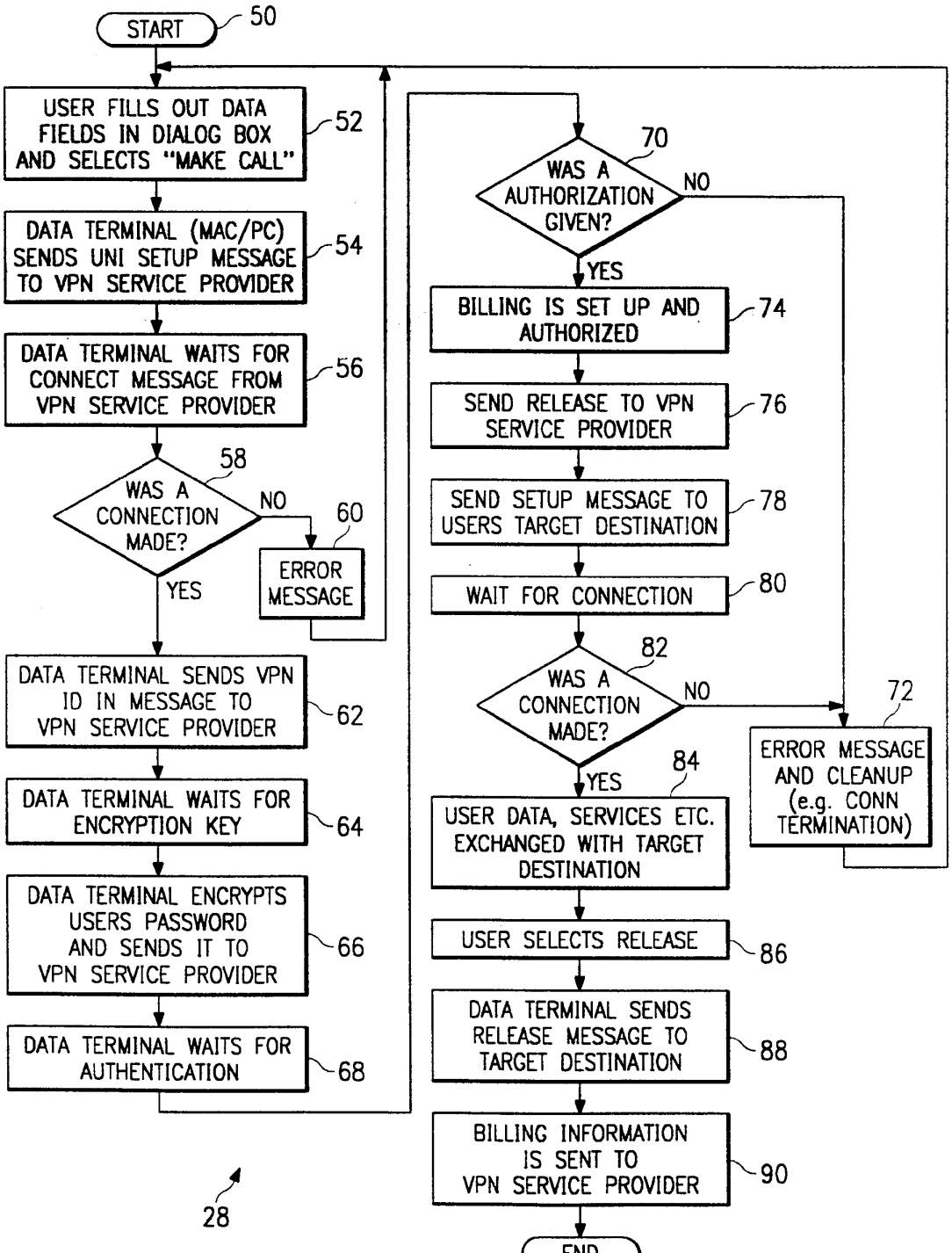

START
50
USER FILLS OUT DATA FIELDS IN DIALOG BOX AND SELECTS "MAKE CALL"
52
DATA TERMINAL (MAC/PC) SENDS UNI SETUP MESSAGE TO VPN SERVICE PROVIDER
54
DATA TERMINAL WAITS FOR CONNECT MESSAGE FROM VPN SERVICE PROVIDER
56
WAS A CONNECTION MADE?
58
NO
60
ERROR MESSAGE
YES
DATA TERMINAL SENDS VPN ID IN MESSAGE TO VPN SERVICE PROVIDER
62
DATA TERMINAL WAITS FOR ENCRYPTION KEY
64
DATA TERMINAL ENCRYPTS USERS PASSWORD AND SENDS IT TO VPN SERVICE PROVIDER
66
DATA TERMINAL WAITS FOR AUTHENTICATION
68
28
WAS A AUTHORIZATION GIVEN?
70
NO
YES
BILLING IS SET UP AND AUTHORIZED
74
SEND RELEASE TO VPN SERVICE PROVIDER
76
SEND SETUP MESSAGE TO USERS TARGET DESTINATION
78
WAIT FOR CONNECTION
80
WAS A CONNECTION MADE?
82
NO
72
ERROR MESSAGE AND CLEANUP (e.g. CONN TERMINATION)
YES
84
USER DATA, SERVICES ETC. EXCHANGED WITH TARGET DESTINATION
USER SELECTS RELEASE
86
DATA TERMINAL SENDS RELEASE MESSAGE TO TARGET DESTINATION
88
BILLING INFORMATION IS SENT TO VPN SERVICE PROVIDER
90
END
92

Fig. 2

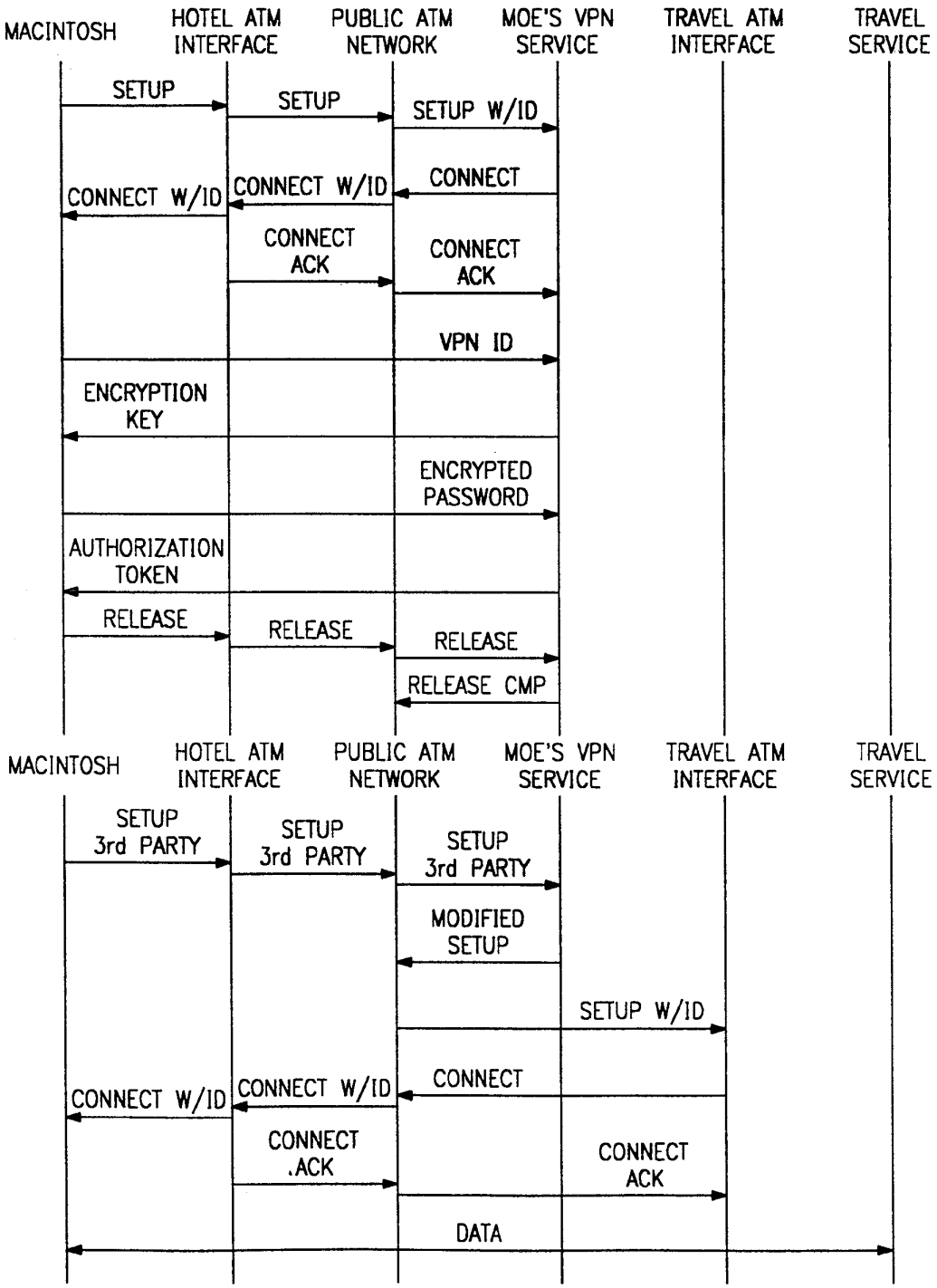

MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP
SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT ACK
CONNECT ACK
VPN ID
ENCRYPTION KEY
ENCRYPTED PASSWORD
AUTHORIZATION TOKEN
RELEASE
RELEASE
RELEASE
RELEASE CMP
MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP 3rd PARTY
SETUP 3rd PARTY
SETUP 3rd PARTY
MODIFIED SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT .ACK
CONNECT ACK
DATA

Fig. 4A

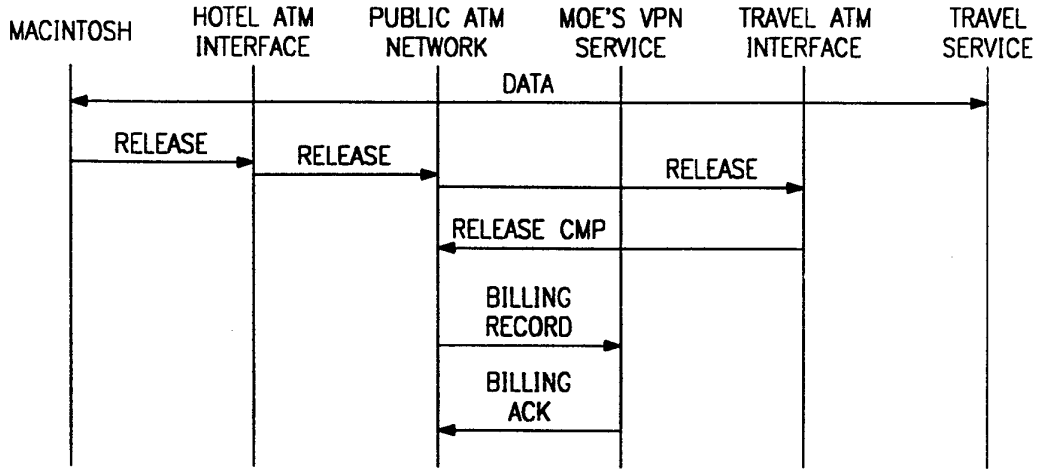


Fig. 4B

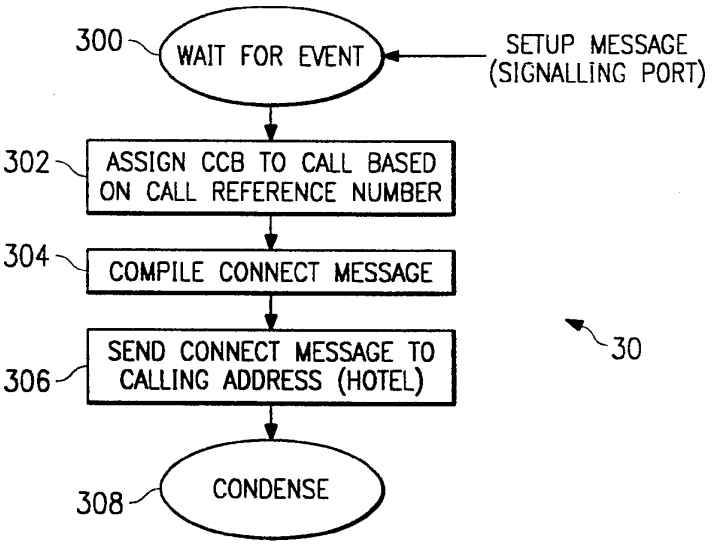


Fig. 5A

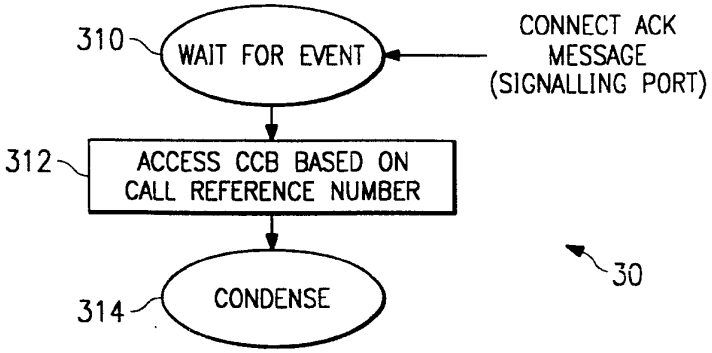


Fig. 5B

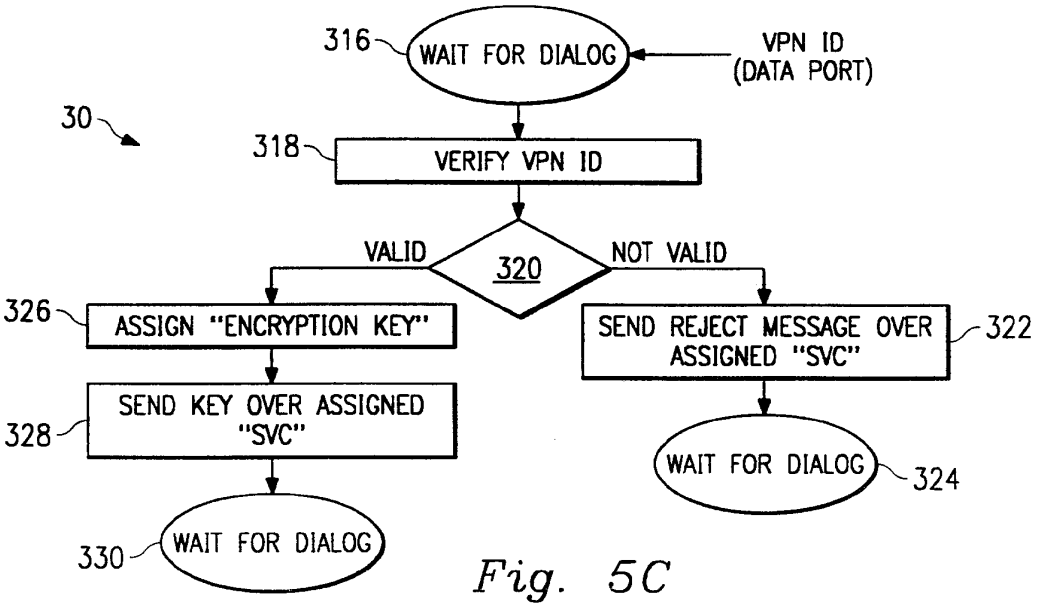

316
WAIT FOR DIALOG
VPN ID
(DATA PORT)
30
318
VERIFY VPN ID
VALID
320
NOT VALID
326
ASSIGN "ENCRYPTION KEY"
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
322
328
SEND KEY OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
324
330
WAIT FOR DIALOG

Fig. 5C

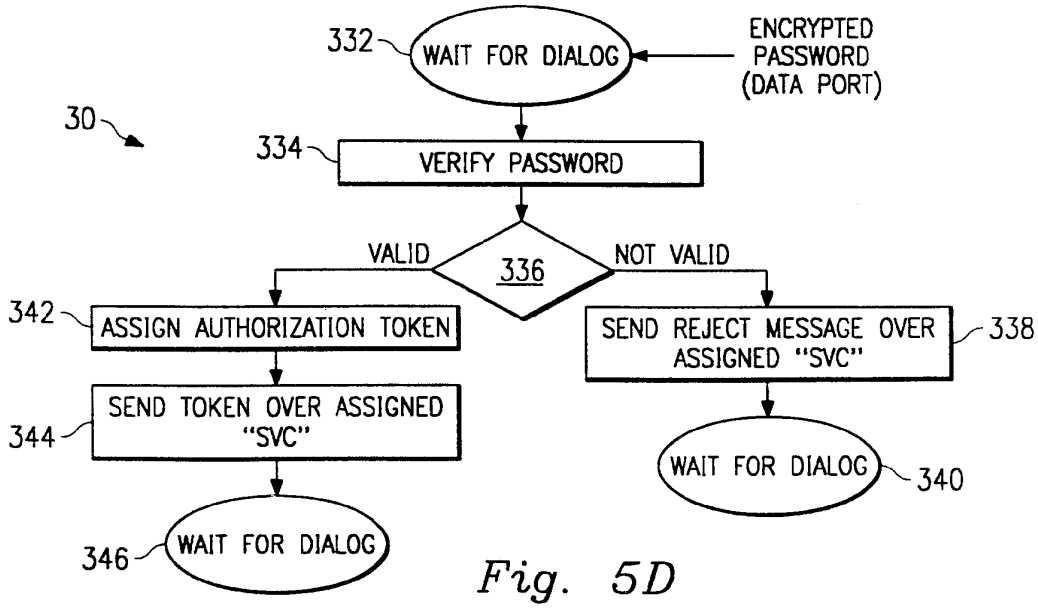

332
WAIT FOR DIALOG
ENCRYPTED
PASSWORD
(DATA PORT)
30
334
VERIFY PASSWORD
VALID
336
NOT VALID
342
ASSIGN AUTHORIZATION TOKEN
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
338
344
SEND TOKEN OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
340
346
WAIT FOR DIALOG

Fig. 5D

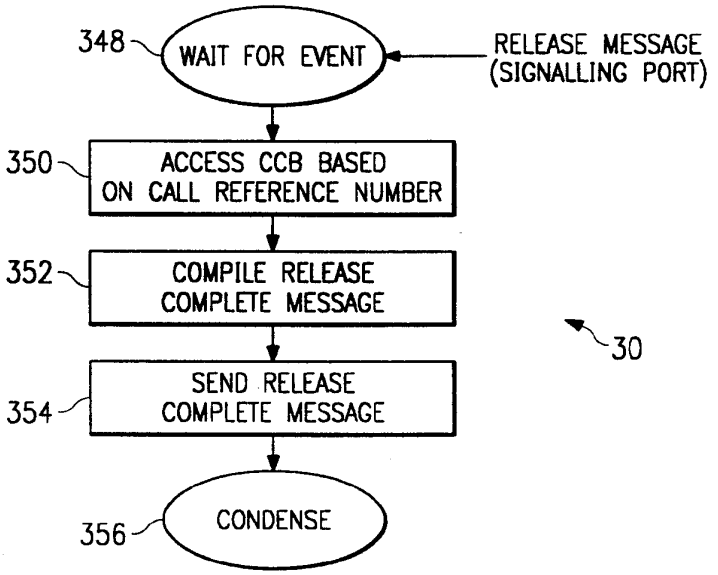

348
WAIT FOR EVENT
RELEASE MESSAGE (SIGNALLING PORT)
350
ACCESS CCB BASED ON CALL REFERENCE NUMBER
352
COMPILE RELEASE COMPLETE MESSAGE
30
354
SEND RELEASE COMPLETE MESSAGE
356
CONDENSE

Fig. 5E

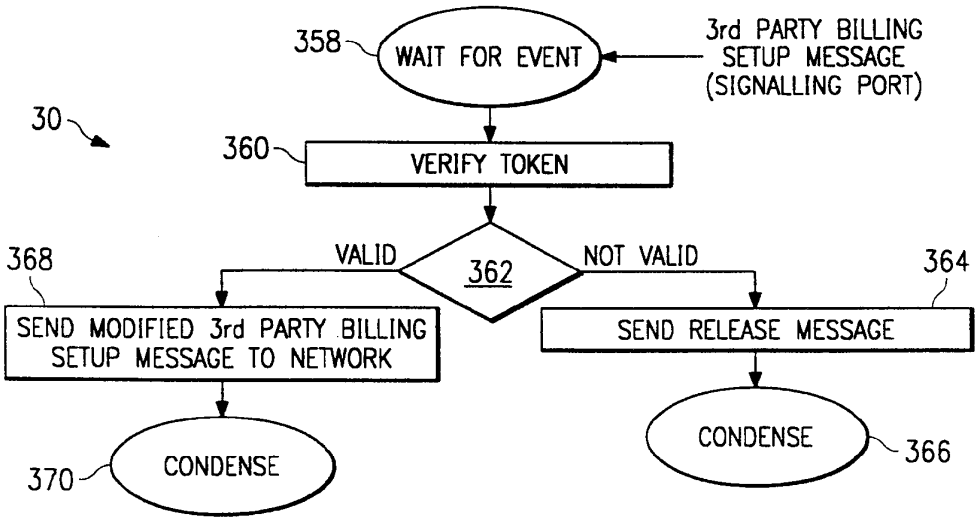

358
WAIT FOR EVENT
3rd PARTY BILLING SETUP MESSAGE (SIGNALLING PORT)
30
360
VERIFY TOKEN
368
VALID
362
NOT VALID
364
SEND MODIFIED 3rd PARTY BILLING SETUP MESSAGE TO NETWORK
SEND RELEASE MESSAGE
CONDENSE
366
370
CONDENSE

Fig. 5F

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/IB 97/01563

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q11/04 H04L12/22

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUN CHOON CHAN ET AL: "AN ARCHITECTURE FOR BROADBAND VIRTUAL NETWORKS UNDER CUSTOMER CONTROL" NOMS '96 IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM , vol. 1, 15 April 1996, KYOTO, JP, pages 135-144, XP000641086 see abstract ---	1-20
A	BIC V: "VOICE PERIPHERALS IN THE INTELLIGENT NETWORK" TELECOMMUNICATIONS, vol. 28, no. 6, June 1994, page 29/30, 32, 34 XP000600293 see the whole document --- -/--	1-20

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 1998	02/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 97/01563

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 729 256 A (NEDERLAND PTT) 28 August 1996 see abstract figures of pages 136 and 140	1-20
A	CROCETTI P ET AL: "ATM VIRTUAL PRIVATE NETWORKS: ALTERNATIVES AND PERFORMANCES COMPARISONS" SUPERCOMM/ICC '94, 1 May 1994, NEW ORLEANS, US, pages 608-612, XP000438985 see abstract	1-20

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ɔnal Application No
PCT/IB 97/01563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0729256 A	28-08-96	NL 9500339 A	01-10-96

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	WO 99/11019
H04L 9/00	A1	(43) International Publication Date:	4 March 1999 (04.03.99)

(21) International Application Number: PCT/US98/17198

(22) International Filing Date: 24 August 1998 (24.08.98)

(30) Priority Data:
08/917,341 26 August 1997 (26.08.97) US

(71) Applicant: V–ONE CORPORATION [US/US]; Suite 300, 20250 Century Boulevard, Germantown, MD 20874 (US).

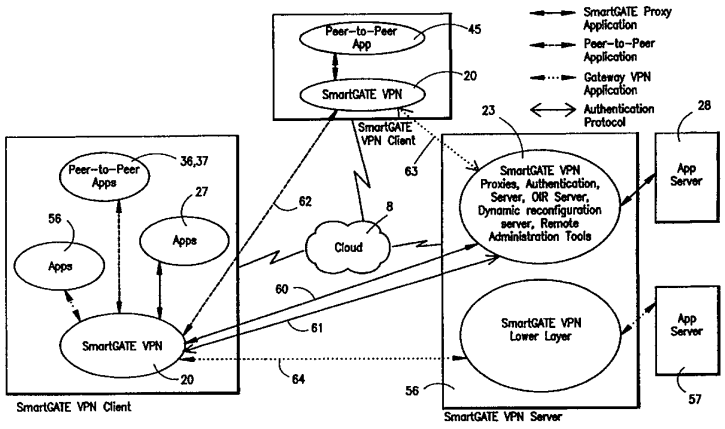
(72) Inventors: CHEN, James, F.; 12648 Tavilah Road, Potomac, MD 20854 (US). WANG, Jieh–Shan; 10903 Silent Wood Place, N. Potomac, MD 20878 (US). BROOK, Christopher, T.; 7308 Pomander Lane, Chevy Chase, MD 20815 (US). GARVEY, Francis; 2908 S. Buchanan Street, Arlington, VA 22206 (US).

(74) Agents: URCIA, Benjamin, E. et al.; Bacon & Thomas, PLLC, 4th floor, 625 Slaters Lane, Alexandria, VA 22314 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: MULTI–ACCESS VIRTUAL PRIVATE NETWORK



(57) Abstract

A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program (20) and at least one shim (50, 53) positioned above either the layers of a client computer to intercept function calls, communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer–to–peer applications (36, 37, 45), the intercepted function calls, request for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer–to–peer communications (62).

FOR THE PURPOSES OF INFORMATION ONLY

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

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

MULTI-ACCESS VIRTUAL PRIVATE NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates a system and method for allowing private communications over an open network, and in particular to a virtual private network which provides data encryption and mutual authentication services for both client/server and peer-to-peer applications at the applications, transport driver, and network driver levels.

2. Discussion of Related Art

A virtual private network (VPN) is a system for securing communications between computers over an open network such as the Internet. By securing communications between the computers, the computers are linked together as if they were on a private local area network (LAN), effectively extending the reach of the network to remote sites without the infrastructure costs of constructing a private network. As a result, physically separate LANs

can work together as if they were a single LAN, remote computers can be temporarily connected to the LAN for communications with mobile workers or telecommuting, and electronic commerce can be carried out without the risks inherent in using an open network.

In general, there are two approaches to virtual private networking, illustrated in Figs. 1A and 1B. The first is to use a dedicated server 1, which may also function as a gateway to a secured network 2, to provide encryption and authentication services for establishment of secured links 3 between the server 1 and multiple clients 4-6 over the open network 7, represented in Fig. 1A as a cloud, while the second is to permit private communications links 8 to be established between any two computers or computer systems 9-12 on network 7, as illustrated in Fig. 1B.

The advantages of a client/server arrangement such as the one shown in Fig. 1A are that the server can handle functions requiring the majority of the computing resources, increasing the number of potential clients, and that management of the network, including key management is centralized. The disadvantage of a client/server network of this type is that peer-to-peer communications links between applications on the client computers cannot utilize the security and management functions provided by the server, leaving such communications unprotected. On the

other hand, the advantage of the direct peer-to-peer approach illustrated in Fig. 1B is that it permits secured links to be established between any computers capable of carrying out the required security functions, with the disadvantages being the cost of configuring each computer to carry-out encryption, authentication, and key management functions, and the lack of central control.

In both the client/server and peer-to-peer approaches, a virtual private network can in theory be based either on applications level technology or can operate at a lower level. Generally, however, peer-to-peer "tunneling" arrangements require modification of the lower layers of a computer's communications architecture, while client/server arrangements can use the applications level approach because less modification of the clients is required, and thus the two approaches are in practice mutually exclusive. The present invention, on the other hand, seeks to provide a virtual private network which utilizes a client/server approach, including centralized control of encryption, authentication, and key management functions, while at the same time enabling secured peer-to-peer communications between applications, by utilizing the server to provide authentication and session key generation functions for both client to server communications and peer-to-peer communications, providing a virtual private network capable of serving both as an extended intranet or wide area network (WAN), and as a commercial mass marketing network,

with high level mutual authentication and encryption provided for all communications.

In order to completely integrate the two approaches and maximize the advantage of each approach, the invention maintains the applications level infrastructure of prior client server private networking arrangements, while adding shims to lower levels in order to accommodate a variety of peer-to-peer communications applications while utilizing the applications level infrastructure for authentication and session key generation purposes. This results in the synergistic effect that not only are existing peer-to-peer tunneling schemes and applications level client server security arrangements combined, but they are combined in a way which greatly reduces implementation costs

In order to understand the present invention, it is necessary to understand a few basic concepts about computer to computer communications, including the concepts of "layers" and communications protocols, and of mutual authentication and file encryption. Further information about layers and protocols can be found in numerous sources available on the Internet, a few of which are listed at the end of this section, while a detailed description of a mutual authentication and encryption system and method suitable for use in connection with the present invention can be found in U.S. Patent No. 5,602,918, which is incorporated herein by reference. In general, the basic

communications protocols and architecture used by the present invention, as well as authentication, encryption, and key management schemes, are already well-known, and can be implemented as a matter of routine programming once the basic nature of the invention is understood. The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out.

Having explained the key differences between the present invention and existing systems, the basic concepts of layers and so forth will now be briefly explained by way of background. First, the concept of "layers," "tiers," and "levels," which essential to an understanding of the invention, simply refers to libraries or sets of software routines for carrying out a group of related functions, and which can conveniently be shared or called on by different programs at a higher level to facilitate programming, avoiding duplication and maximizing computer resources. For example, the Windows NT device driver architecture is made up of three basic layers, the first of which is the Network Driver Interface Specification (NDIS 3.0) layer, the second of which is called the Transport Driver Interface (TDI) layer, and the third being the file

systems. These layers are generically referred to as the network driver layer, the transport or transport driver layer, and the applications layer.

In the Windows NT architecture, the TDI layer formats data received from the various file systems or applications into packets or datagrams for transmission to a selected destination over the open network, while the NDIS layer controls the device drivers that send the data, packets, or IP datagrams, for example by converting the stream of data into a waveform suitable for transmission over a telephone line or a twisted pair cable of the type known as an Ethernet.

By providing layers in this manner, an applications software programmer can design an application program to supply data to the TDI layer without having to re-program any of the specific functions carried out by that layer, and all of the transmission, verification, and other functions required to send a message will be taken care of the TDI layer without further involvement by the applications software. In a sense, each "layer" simply accepts data from the higher layer and formats it by adding a header or converting the data in a manner which is content independent, with retrieval of the data simply involving reverse conversion or stripping of the headers, the receiving software receiving the data as if the intervening layers did not exist.

In the case of Internet communications, the most commonly used set of software routines for the transport or TDI layer, which takes care of the data formatting and addressing, is the TCP/IP protocol, in which the transport control protocol (TCP) packages the data into datagrams and provides addressing, acknowledgements, and checksum functions, and the internet protocol (IP) further packages the TCP datagrams into packets by adding additional headers used in routing the packets to a destination address. Other transport protocols which can be included in the TDI layer include the user diagram protocol (UDP), the internet control message protocol (ICMP), and non-IP based protocols such as Netbeui or IPX.

Additional "protocols" are may be used at the applications level, although these protocols have nothing to do with the present invention except that they may be included in the applications programs served by the network. Common applications level protocols which utilize the TCP/IP protocol include hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP), all of which operate at the layer above the transport layer.

Some applications are written to directly call upon the TCP functions. However, for most applications utilizing a graphical user interface conveniently rely on a set of software routines which are considered to operate

above the TDI layer, and are known as sockets. Sockets serve as an interface between the TCP set of functions, or stack, and various applications, by providing libraries of routines which facilitate TCP function calls, so that the application simply has to refer to the socket library in order to carry out the appropriate function calls. For Windows applications, a commonly used non-proprietary socket is the Windows socket, known as Winsock, although sockets exist for other operating systems or platforms, and alternative sockets are also available for Windows, including the Winsock 2 socket currently under development.

In order to implement a virtual private network, the encryption and authentication functions must be carried out at one of the above "levels," for example by modifying the network drivers to encrypt the IP datagrams, by inserting authentication headers into the TCP/IP stacks, or by writing applications to perform these functions using the existing drivers. If possible, it is generally desirable to minimize modification of the existing levels by adding a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a "shim."

As indicated above, the preferred approach to implementing client/server virtual private networks is to

use an applications level security system to encrypt files to be transmitted, and to then utilize existing communications layers such as Winsock, or TCP/IP directly. This is the approach taken by the commercially available access control system known as SmartGATE™, developed by V-One Corp. of Germantown, Md., which provides both encryption and mutual authentication at the applications level utilizing a dedicated server known as an authentication server and authentication client software installed at the applications level on the client computers. A description of the manner in which encryption and mutual authentication is carried out may be found in the above-cited U.S. Patent No. 5,602,918. While the principles of the invention are applicable to other client/server based virtual private networks, SmartGATE™ is used as an example because it provides the most complete range of mutual authentication and encryption services currently available.

The present invention can be implemented using the existing SmartGATE™ system, but adds mutual authentication and encryption services to lower layers by intercepting function calls or data packets and, during initialization of a communications link, establishing separate channels between the party initiating the communication and the authentication server, and between the authentication server and the party which is to share in the communication, so as to mutually authenticate the parties

with respect to the server, and so as to establish a session key which can be used for further direct communications between the parties.

A number of protocols exist which can be used, in total or in part, to implement the mutual authentication and encryption services at the lower layers, using the same basic authentication and encryption scheme currently implemented by SmartGATE™ at the applications level. These include, by way of example, the SOCKS protocol, which places a shim between the TDI or transport layer and the applications, and the commercially available program, known as SnareNet, which operates at the network driver level and can be directly utilized in connection with the present invention.

On the other hand, a network level implementation such as the SKIP protocol, which operates below the TDI layer to encrypt the datagrams, and which in its description explicitly precludes the generation of session keys (see the above cited U.S. Patent No. 5,602,918), is fundamentally different in concept than the present invention. Similarly, alternative implementations such as Point-to-Point Tunneling Protocol (PPTP) which involve modifying the TCP/IP stack and/or hardware to provide encryption, as opposed to inserting shims, are not utilized by the preferred embodiment of the present invention, although individual aspects of the protocol could perhaps

be used, and the present system could be added to computers also configured to accept PPTP communications.

The SmartGATE™ system uses public key and DES encryption to provide two-way authentication and 56-bit encrypted communications between a server equipped with the SmartGATE program and client computers equipped with a separate program. Currently, SmartGATE™ operates at the highest level, or applications level, by using shared secret keys to generate a session key for use in further communications between the authentication server or gateway and the client program. Since the session key depends on the secret keys at the gateway and client sides of the communication, mutual authentication is established during generation of the session key, which can then be used to encrypt further communications.

When installed on a client system, the SmartGATE™ client software reads a request for communications by an applications program, such as a browser program, and then proceeds to establish its own communications link with the destination server to determine if the server is an authentication server. If it is not, control of communications is relinquished, but if it is, then the security program and the server carry out a challenge/response routine in order to generate the session key, and all further communications are encrypted by the security program. Although this program is placed between

the Winsock layer and the applications, it does not function as a shim, however, because it only affects communications directed to the authentication server.

Having briefly summarized the concepts used by the present invention, including the concepts of layers, protocols, and shims, and having described a specific applications level security program which is to be modified according to the present invention by adding shims in a way which enables secured authentication and session key generation channels to be set up from the lower layers, it should now be possible to understand the nature of the invention, and in particular how it integrates the two approaches to virtual private networking in a way which greatly expands the concept and yet can easily be implemented. More details will be given below, but as a final observation in this background portion of the patent specification, it should be noted that while the overall concept of the invention is in a sense very simple, it is fundamentally at odds with present approaches. For example, the literature is replete with references to conflicts between VPN standards and implementations, as exemplified by the title of an article from LAN Times On-Line, 9/96, (http://www.wcmh.com/), which reads *Clash Over VPN Supremacy*. Even a cursory search of the available literature indicates that the amount of information and choices available to those wishing to set up a virtual private network is overwhelming. One can choose between

Netscape Communications Secure Socket Layer, Open Market Inc.'s Secure HTTP, Microsoft's PPTP, among others. However, all of these approaches operate at a single level, and force a choice between establishing a network of the type shown in Fig. 1A and a network of the type shown in Fig. 1B. Only the present invention offer the advantages of both approaches, without the inflexibility of client/server arrangements or the costs of more distributed architectures.

For further information on the various competing VPN protocols and systems, see also *The Development of Network Security Technologies*, Internet Smartsec, 2/97 (http://www.smartsec.se), which compares SmartGATE™ to other application level security systems, including PPTP, SSL, and S-HTTP; *Point-To-Point Tunneling Protocol (PPTP) Frequently Asked Questions*, Microsoft Corp., date unknown, (http://www.microsoft.com), *Simple Key-Management for Internet Protocols (SKIP)*, Aziz *et al.*, date unknown, (http://skip.incog.com), and *SOCKS Protocol Version 5, RFC 1928*, Leech *et al.*, 3/96 (http://andrew2.andrew.cmu.edu) (this document describes a protocol involving a TDI shim). For more general information on security problems, Internet protocols, and sockets, see *Introduction to the Internet Protocols*, Charles L. Hedrick, Rutgers University, 1987 (http://oac3.hsc.uth.tmc.edu); *Windows Sockets - Where Necessity is the Mother of Reinvention*, Stardust

Technologies, Inc., 1996, (http//www.stardust.com), and *Secure Internet Connections*, LAN Times, 6/17/96 (Ibid).

SUMMARY OF THE INVENTION

It is accordingly a principal objective of the invention to provide a client/server virtual private network which is capable not only of carrying out authenticated secure communications over an open network between an authentication server and clients, but also authenticated secure peer-to-peer communications.

It is also an objective the invention to provide a virtual private network that provides data encryption and mutual authentication for both client/server and peer-to-peer communications for different-types of applications, using both the applications level and lower levels of a communications hierarchy.

It is a further objective of the invention to provide a client/server virtual private network which can provide both client/server and peer-to-peer encryption and authentication services for any application sharing a specified socket or sockets, whether or not the application is recognized by the encryption and authentication program.

It is a still further objective of the invention to provide a client/server virtual private network which can

provide encryption and authentication services at the applications level, transport driver interface level, and network interface level, without the need for modifying either the communication driver or network driver, or any sockets utilizing the communications driver interface.

It is yet another objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications while maintaining centralized control of key distribution and management functions.

Finally, it is also an objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications and in which registration is carried out by a central gateway server.

These objectives of the invention are accomplished by providing a virtual private network for communicating between a server and clients over an open network and in which the clients are equipped with an applications level encryption and mutual authentication program which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which intercepts function calls or data packets in order to authenticate the parties to the communication by

establishing secured channels between the server and the parties to the communication, prior to establishment of the secured communications link between the parties, in order to carry out mutual authentication and session key generation functions.

More particularly, according to the principles of a preferred embodiment of the invention, client communications software is provided which, at the socket or transport driver interface levels, intercepts function calls to the socket or transport driver and directs calls to the authentication server in order to perform encryption and authentication routines, and at the network driver interface, performs encryption and authentication functions by intercepting the datagrams or data portions of the packets transmitted by the transport driver interface based on communications between the authentication server and the client. According to this aspect of the invention, a system of providing authentication and encryption services for the purpose of establishing a virtual private network includes a plurality of shims arranged to operate at different protocol levels in order to establish a common secure communications link to an authentication server.

In one especially preferred embodiment of the invention, the client software includes a Winsock shim arranged to intercept function calls to the Winsock library on a client machine and redirect initial communications

through the authentication client software to the authentication server, so that any function calls to the Winsock library of programs are intercepted by the shim and carried out by the applications level security program. In this embodiment, the client authentication software substitutes its own function calls for the original function calls in order to establish a secured communications link to the authentication server over which such functions as mutual authentication between the client and server, indirect authentication of peer applications by the now trusted server, session key generation, are carried out, as well as ancillary functions such as on-line registration (OLR), utilizing the unmodified original Winsock library and TCP/IP communications stacks.

By inserting a shim at the Winsock level, an applications level client/server based security program such as SmartGATE™ can be used to provide secure communications for any application which utilizes the Winsock library. In addition, by including analogous shims at other levels, the invention can be used to secure virtually any communications application, including those which by-pass the TDI layer and communicate directly with the network driver level.

Instead of the current array of mutually exclusive alternative methods and systems of establishing secured communications over an open network, the invention thus

provides a single integrated method and system capable of carrying out both client/server communications and peer-to-peer communications between a wide variety of communications applications regardless of whether the applications use a socket or even commonly accepted internet protocols, with complete mutual authentication and encryption of data files at all levels and between all parties to the network.

It will be appreciated that the term "virtual private network" is not to be taken as limiting, and that the principles of the invention can be applied to any remote access schemes which utilize the Internet or other relatively insecure networks to provide access for remote users, corporate intranets, and electronic commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is a schematic diagram of a client/server virtual private network.

Fig. 1B is a schematic diagram of an alternative virtual private network based on peer-to-peer communications.

Fig. 2 is a functional block diagram showing the operation of an applications level security program in a conventional communications network hierarchy.

Fig. 3 is a functional block diagram showing the communications network hierarchy of Fig. 1, modified to provide a second layer of service in accordance with the principles of a preferred embodiment of the invention.

Fig. 4 is a functional block diagram showing the communications network hierarchy of Fig. 2, modified to provide a third layer of service in accordance with the principles of the preferred embodiment.

Fig. 5 is a functional block diagram showing the communication network hierarchy of Fig. 3, modified to provide a fourth layer of service in accordance with the principles of the preferred embodiment.

Fig. 6 is a schematic diagram of a virtual private network utilizing the principles of the preferred embodiment of the invention.

Fig. 7 is a flowchart illustrating a method of implementing the system of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 2 illustrates the operation of a client authentication program which is utilized in the present invention. An example of such a program is the SmartGATE™ program discussed briefly above, although other

applications level security programs, whether or not token based, could be modified in a manner similar to that discussed in the following description. The illustrated hierarchy is the Windows NT architecture, although versions of SmartGATE™ exist for other architectures, and the invention could easily be adapted for use with any version of SmartGATE™, including UNIX and MacIntosh versions, as well as for use with applications level security programs designed for communications architectures other than those supported by SmartGATE™. Conversely, it is intended that the present invention can be used with authentication and encryption schemes other than that used by SmartGATE™ and disclosed in U.S. Patent No. 5,602,918. For purposes of convenience, therefore, the software represented by SmartGATE™ is simply referred to as client authentication software.

In addition, it noted that the client computer architectures illustrated in Figs. 3-6, which are modified versions of the architecture of Fig. 2, is to be used with an overall network layout such as the one illustrated in Fig. 6, which includes an authentication server that may be a SmartGATE™ server, or another server depending on the client authentication software. The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.

Turning to Fig. 2, which provides background for the description of the invention illustrated in Figs. 3-6, the client authentication software 20 is situated above the boundary of the transport or TDI layer 21 and is designed to utilize a socket 22, such as Winsock, to carry out communications with the authentication server 23 shown in Fig. 6 by means of a transport protocol such as TCP/IP, UDP, or the like, which in turn supply datagrams or packets to a hardware driver layer 24, such as NDIS 3.0, of a network or modem connection 25.

In operation, the client authentication software 20 intercepts interconnect calls 26 form client authentication software supported applications 27 and, if the calls are directed to the authentication server 23, or to a server 28 situated on a secured network whose access is controlled by the authentication server, establishes a secured communications link to the server by executing appropriate function calls 29 to the socket library, which in turn transmits function calls 30 to the TDI layer, causing the TDI layer to form datagrams or packets 31. Datagrams or packets 31 are then formatted over packaged for transmission by the hardware drivers 24 and sent to the communications network in the form of Ethernet packets or analog signals 32 containing the original datagrams from the TDI layer. Once the secured communications link has been established, client authentication software 20 encrypts all further data communications 34 from

applications 27, which are indicated by dashed lines, before handing them off to the next lower layer in the form of encrypted files 35. The dashed lines are shown in Fig. 2 as extending only to the TDI layer 21, because the datagrams formed by the TDI layer are indistinguishable as to content, but it is to be understood that datagrams or packets 31 carry both the communications used to establish the secure channel, and the encrypted files subsequently sent therethrough.

Finally, in the case of SmartGATE™, the authentication client software utilizes either a smart card or secured file to supply the secret keys used during authentication to generate a session key for encryption of further communications, and also to carry out certain other encryption and authentication functions, although it is of course within the scope of the invention to use key distribution and authentication methods which do not rely on smartcards or tokens, and the tokens are not involved in any of the basic communications functions of the client authentication software 20.

In addition to the applications 27 which communicate with the server via the authentication/encryption software 20, a typical system will have a number of additional software applications 36 and 37 capable of carrying out communications over the open network, but which the authentication client software is not configured to handle,

and which are not specifically adapted or intended to carry out communications with the authentication server. These are referred to herein as peer-to-peer applications, and can include applications which use the same sockets as the authentication client software, applications which directly call upon a transport driver interface stack, whether using the same protocol as the authentication client software or another protocol, all of which are intended to be represented by the TDI layer, and applications which are written to call directly upon the hardware drivers. These peer-to-peer applications may have their own encryption and authentication capabilities, but cannot utilize the services of the authentication server or client software, and therefore the function calls made by the applications and the files transmitted are indicated by separate reference numerals 40-43.

It will be appreciated by those skilled in the art that lower layer application programs which generate packets in forms other than those represented by the TDI layer are also possible, and should be considered within the scope of the invention, but at present virtually all open network applications use at least one of the TDI protocols, and thus while these programs may interact directly with the network driver layer, and require a network driver layer shim, as will be discussed below, are illustrated for purposes of convenience as part of the TDI layer applications.

Turning now to a preferred embodiment of the invention, the arrangement shown in Fig. 3 modifies the arrangement of Fig. 2 by adding a socket shim 50 between the socket 22 utilized by the authentication client software 20, the peer-to-peer applications 36 which also utilize the socket 20, and the authentication client software itself. The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23, shown in Fig. 6, in order to carry out the authentication protocol, as will be discussed in more detail below. Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server, and transmission as encrypted files 51 addressed to the peer application, also shown in Fig. 6, which could also be an application on the application server 28.

Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with "peers" 45 and not with the authentication server, the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication

client software and to authentication server, even though the peer application assumes that it is communicating only with the peer application. This function permits session key encrypted communications to be forwarded directly to the peer application, as illustrated in Fig. 6, while the latter function provides the authentication server with the client address so that the authentication server can establish a secured and authenticated link with the peer application, via authentication client software on the peer computer, and transmit the session key to the peer application or at least enable the peer application to recreate the session so that it can decrypt the encrypted files received directly from the client application.

Thus, while it is appreciated that the use of socket shims is well-known, as mentioned above, the socket shim shown in Fig. 2 has the unique function of enabling direct peer-to-peer communications with mediation by the authentication server, permitting the highest level of authentication service and collateral functions. In addition, because of the mediation by the key server, the peer applications do not need to have a shared secret key, allowing centralized key management, with only the authentication server having access to all of the client's secret keys.

Figs. 4 shows the variation of the client authentication software 20 in which a TDI shim 52 similar

in function to the socket shim 50 is provided above the TDI layer. Like the socket shim, implementation of the TDI shim essentially simply involves diverting certain information to the client software in order to establish a communications link with the authentication server, and subsequently perform encryption to obtain encrypted files 54 for transmission directly through the TDI layer in the usual manner. As with the socket shim, TDI shims are not new and can be implemented in known manner, by intercepting TDI service requests, but with the difference from prior TDI shims that the TDI shim works with the authentication software 20 and authentication server to authenticate communications and generate a session key.

Finally, as shown in Fig. 5, a further layer of authentication and encryption may be added by adding a network driver shim 55, either to the arrangement shown in Fig. 3 without the TDI shim, in combination with the TDI shim shown in Fig. 4, or in combination with the TDI shim of Fig. 4 but not the socket shim, to provide for authentication of communications at the network driver layer. At this layer, the shim 55 intercepts IP packets from applications 56, but instead of referring back to the applications level routine, checks the destination address (which can be in TCP format, UDP format, and so forth), establishes a session key by communications with the authentication server, converts the session key into a format which can be used to encrypt the IP packet, and

sends the IP packet towards the destination, all by carrying out the necessary operations at the network driver level, in a manner similar to that utilized by the above-mentioned SnareNet software program, but with the difference that the authenticating communications link and key generation is carried out by packets addressed to a corresponding layer 56 of the authentication server, which may be further connected to an applications server 57.

It will be noted that since the IP packets are not distinguishable by content, the network driver layer shim could be used as an additional level of security, rather than as an alternative to applications level encryption, with the encrypted files generated by software 20 being further encrypted by shim 55 before transmission to the authentication server or associated gateway.

The overall system utilizing the authentication client software illustrated in Figs. 3-5 is schematically illustrated in Fig. 6. The principal components of the overall system are the client computers containing software of the type illustrated in Figs. 2-5, including client authentication software 20 and shims 50, 53, and/or 55, and applications with communications capabilities (represented by applications 27, 36, 37, and 56 on one client, and application 45 on the other). For purposes of illustration, the client of Figs. 6 is thus depicted as including applications for communicating at the highest

levels, such as the SmartGATE™ proxy application, applications for communicating at the network driver level with corresponding applications connected to the lower layer of the authentication server, and peer-to-peer applications with no capability of communicating with SmartGATE™, but which use sockets or TDI protocols recognized by the shims.

In the case of the SmartGATE™ proxy application, communications are established in the same manner as in the currently available version of the SmartGATE™ authentication client software, and as described in U.S. Patent No. 5,602,918, the communications link being indicated by arrows 60 and 61, with arrow 60 representing the client/server response channel used to authenticate the parties and generate the session key.

In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62, the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23. Server 23 then opens a secured channel 63 to the authentication client software 20 associated with peer application 45 by performing the same mutual authentication procedure performed for the purpose of establishing channel 63, and once the channel is established with its own session key, transmits information using the channel 63

session key which allows the client to recreate the channel 60 session key for use in decrypting communications sent over channel 62. Alternatively, after establishing channel 63, the channel 60 session key could be used to transmit back to the original sending party information necessary to recreate the channel 63 session key. In either case, the authentication server is thus used to establish a fully authenticated "tunnel" between the peer applications without the need to modify any of the sockets, TDI protocols, or hardware drivers on either of the client computers. While the transmitting peer application has no way of directly authenticating the receiving peer, only a receiving peer authenticated by the authentication server will be able to generate the necessary session keys, and thus each of the parties to the communication is effectively authenticated.

For the lower layer application 56, a similar protocol may be employed, in which the attempted communication between lower layer applications is intercepted, and the communications link to the authentication server is used to generate a session key, which is then used to encrypt the packets or datagrams being sent. In this case, the destination must be the lower layer of the authentication server, and thus the communications link is indicated by a separate channel 67.

Finally, the procedures associated with the network illustrated in Fig. 6 are summarized in the flowchart of Fig. 7. For communications directly with the applications level portion of the server 23, steps 100-103 are used, while for peer-to-peer communications, steps 104-109 are used, and for network driver level communications, steps 110-114 are used.

In particular, step 100 by which the applications level authentication program 20 illustrated in Figs. 3-5 receives a call initiation request, either directly from a supported applications program 27 or from a programs 36 and 37 via one of the shims 50 and 53, step 101 is step by which the program 20 addresses the authentication server, step 102 is the step by which the client and server are mutually authenticated and the session keys generated using, for example, the procedure described in U.S. Patent No. 5,602,918, and step 103 is the step by which program 20 encrypts further communications received directly or via shims 50 and 53 from the applications programs 27, 36, and 37.

For peer-to-peer communications, step 105, which is part of step 100, is the step by which the peer address is supplied to program 20, steps 106 and 107 are identical to steps 101 and 102, step 108 is the step by which communications channel 63 shown in Figure 6 is established, step 109 is the step by which the destination computer

authenticated by the server is enabled to decrypt communications received over channel 62, and step 110 is the step by which program 20 encrypts the communications. It will of course be appreciated that these steps represent only a summary of the steps involved in carrying out the present invention, and that further steps will be apparent to those skilled in the art based on the above description of the apparatus and software portions of the preferred embodiment of the invention.

Having thus described various preferred embodiments of the invention, those skilled in the art will appreciate that variations and modifications of the preferred embodiment may be made without departing from the scope of the invention. It is accordingly intended that the invention not be limited by the above description or accompanying drawings, but that it be defined solely in accordance with the appended claims.

I claim:

1. Apparatus for carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising:

means for intercepting function calls and requests for service sent by an applications program on one of said client computers to a lower level set of communications drivers; and

means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

2. Apparatus as claimed in claim 1, further comprising means for intercepting files packaged by a transport driver interface layer to form packets and encrypting the packets using a session key generated during communications with a lower layer of the server.

3. A method as claimed in claim 1, further comprising

means for intercepting a destination address during initialization of communications between said one of said

client computers and a second of said client computers on said virtual private network;

means for causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key; and

means for transmitting the encrypted files directly to the destination address.

4. Apparatus as claimed in claim 3, wherein said means for intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program and a layer of a communications driver architecture of said one of the two client computers.

5. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for

transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

at least one lower level set of communications drivers;

and a shim arranged to intercept function calls and requests for service sent by an applications program to the lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

6. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, a transport driver

interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

7. A multi-tier virtual private network as claimed in claim 6, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

35

8. A multi-tier virtual private network as claimed in claim 6, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

9. A multi-tier virtual private network as claimed in claim 8, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

10. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned

between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

11. A multi-tier virtual private network as claimed in claim 10, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

12. A multi-tier virtual private network as claimed in claim 10, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and

encrypt the files using a session key generated during communications with a lower layer of the server.

13. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a

network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

14. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

15. A multi-tier virtual private network as claimed in claim 14, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

16. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a socket,

the socket being positioned above a transport driver layer of said communications driver architecture.

17. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

18. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

and a shim arranged to intercept function calls and requests for service sent by an applications program to a lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate

said session key, and encrypt files sent by the applications program before transmittal over said open network.

19. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

20. Computer software as claimed in claim 19, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the

server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

21. Computer software as claimed in claim 19, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

22. Computer software as claimed in claim 21, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

23. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a

network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

24. Computer software as claimed in claim 23, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

25. Computer software as claimed in claim 23, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

26. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer

arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

27. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client

computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

28. Computer software as claimed in claim 27, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

29. Computer software as claimed in claim 27, wherein said shim is positioned above a socket, the socket being positioned above a transport driver layer of said communications driver architecture.

30. Computer software as claimed in claim 27, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

31. A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:

intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;

causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

32. A method as claimed in claim 31, further comprising the step of intercepting files packaged by a transport driver interface layer to form packets and encrypting the

packets using a session key generated during communications with a lower layer of the server.

33. A method as claimed in claim 31, further comprising the step of intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network;

causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

transmitting said destination address to said server;

causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

enabling said second of said two client computers to recreate the session key;

causing said authentication software to encrypt files to be sent to the destination address using the session key; and

transmitting the encrypted files directly to the destination address.

34. A method as claimed in claim 33, wherein said step of intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program

and a layer of a communications driver architecture of said one of the two client computers.

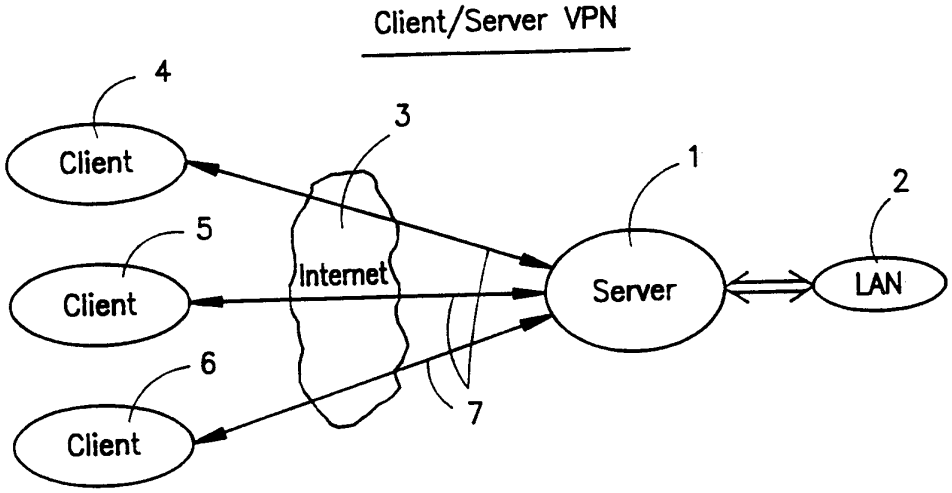


FIG. 1A
(PRIOR ART)

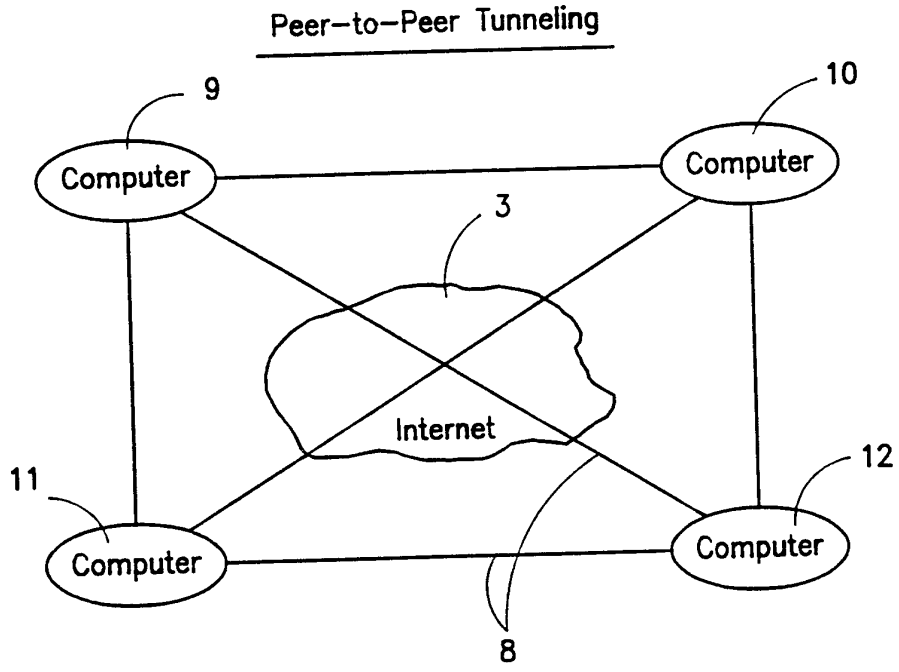


FIG. 1B
(PRIOR ART)

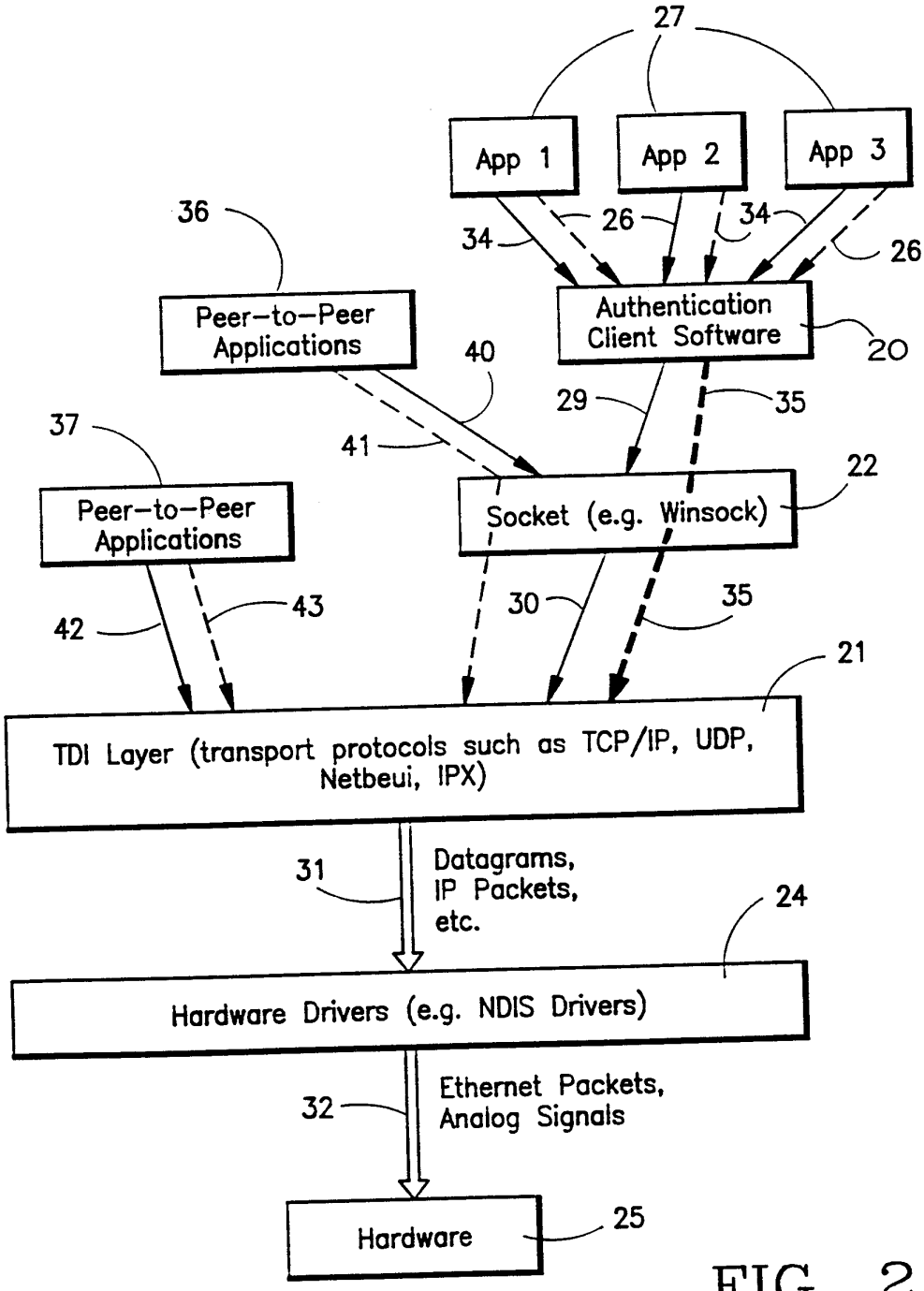


FIG. 2
(PRIOR ART)

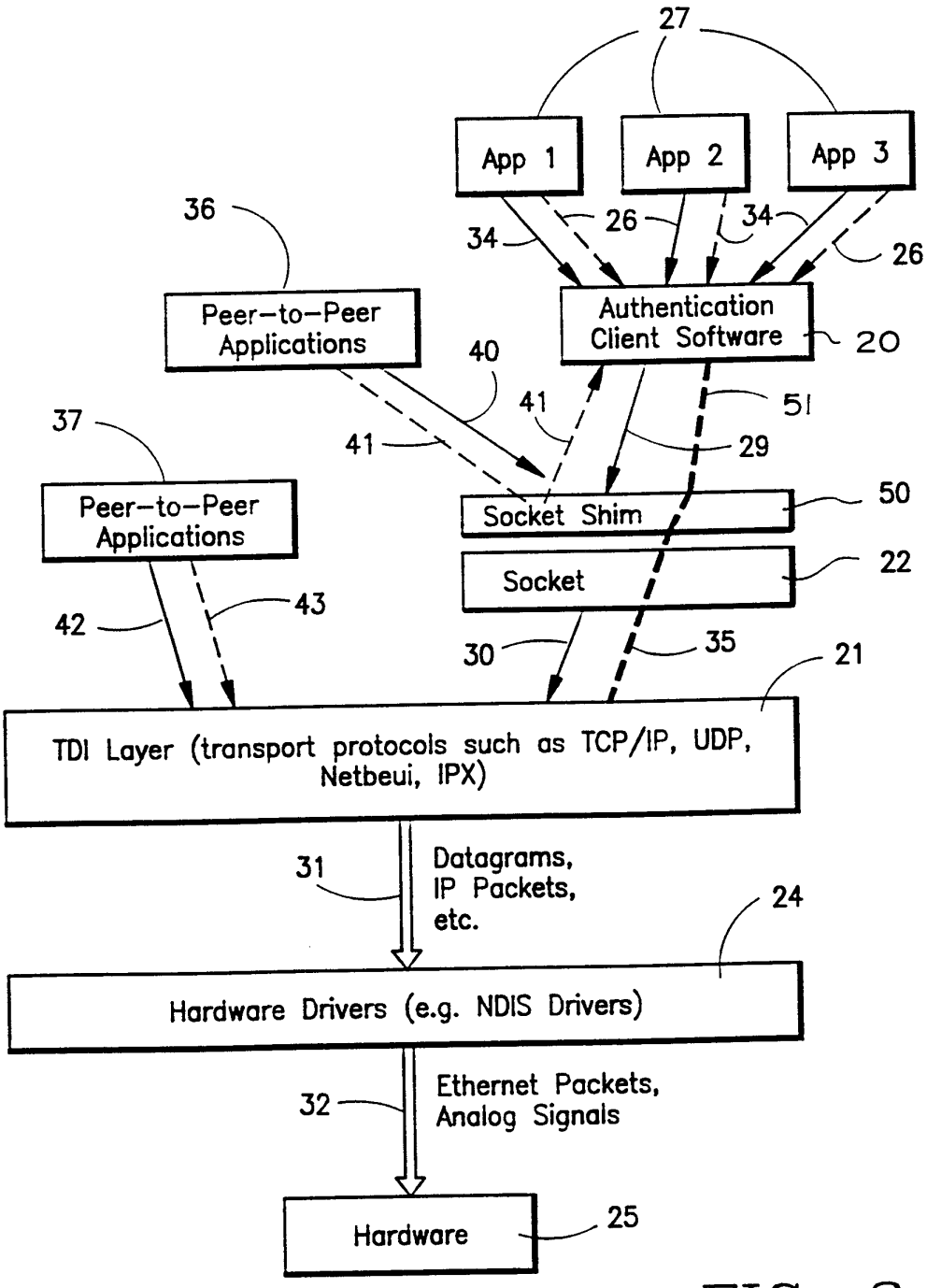

27
App 1
App 2
App 3
36
34
26
34
26
Peer–to–Peer Applications
Authentication Client Software
20
40
41
51
37
41
29
Peer–to–Peer Applications
Socket Shim
50
Socket
22
42
43
30
35
21
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 3

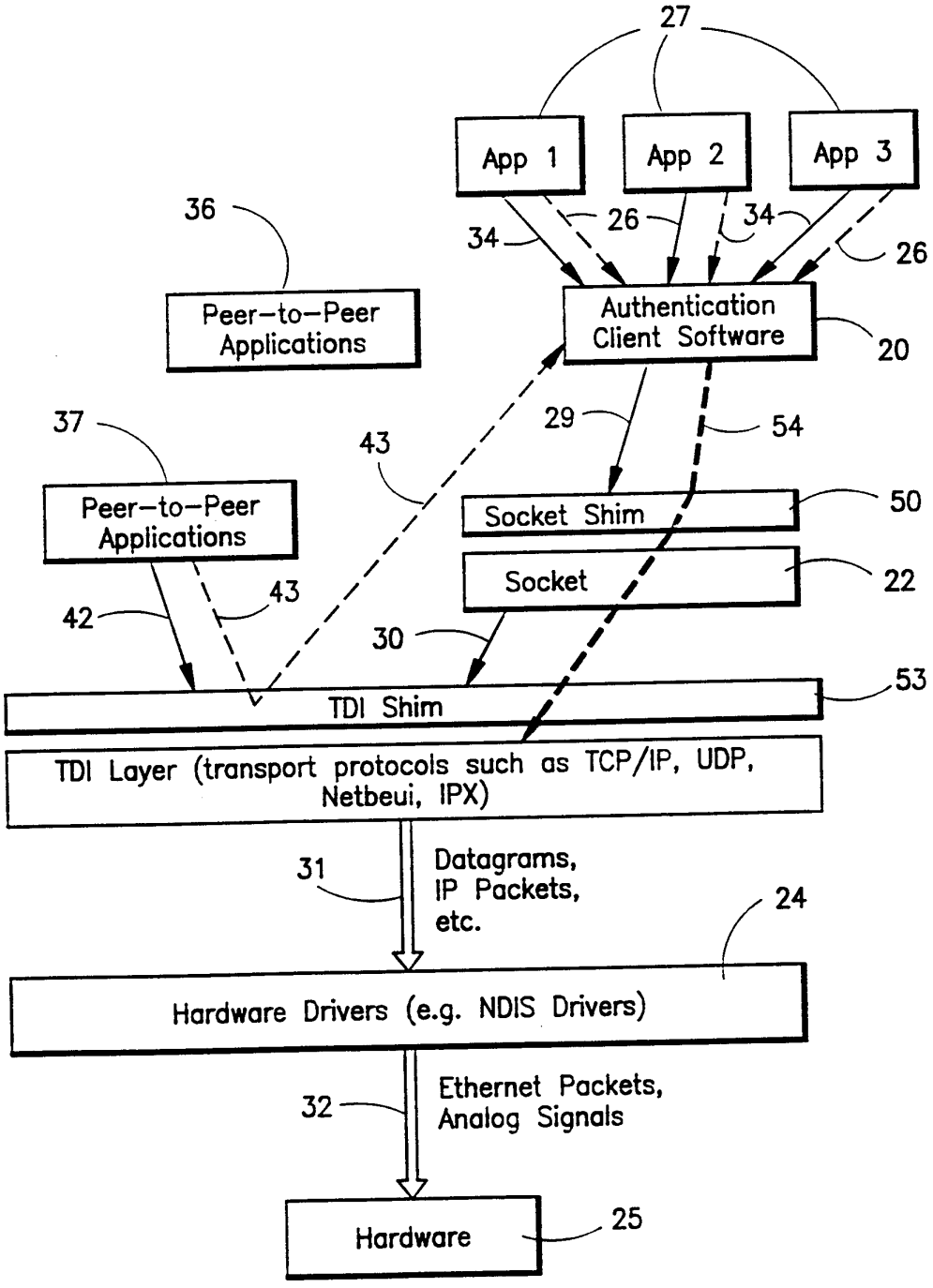

27
App 1
App 2
App 3
36
34
26
34
26
Peer–to–Peer Applications
Authentication Client Software
20
37
29
54
43
Peer–to–Peer Applications
Socket Shim
50
Socket
22
43
42
30
TDI Shim
53
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 4

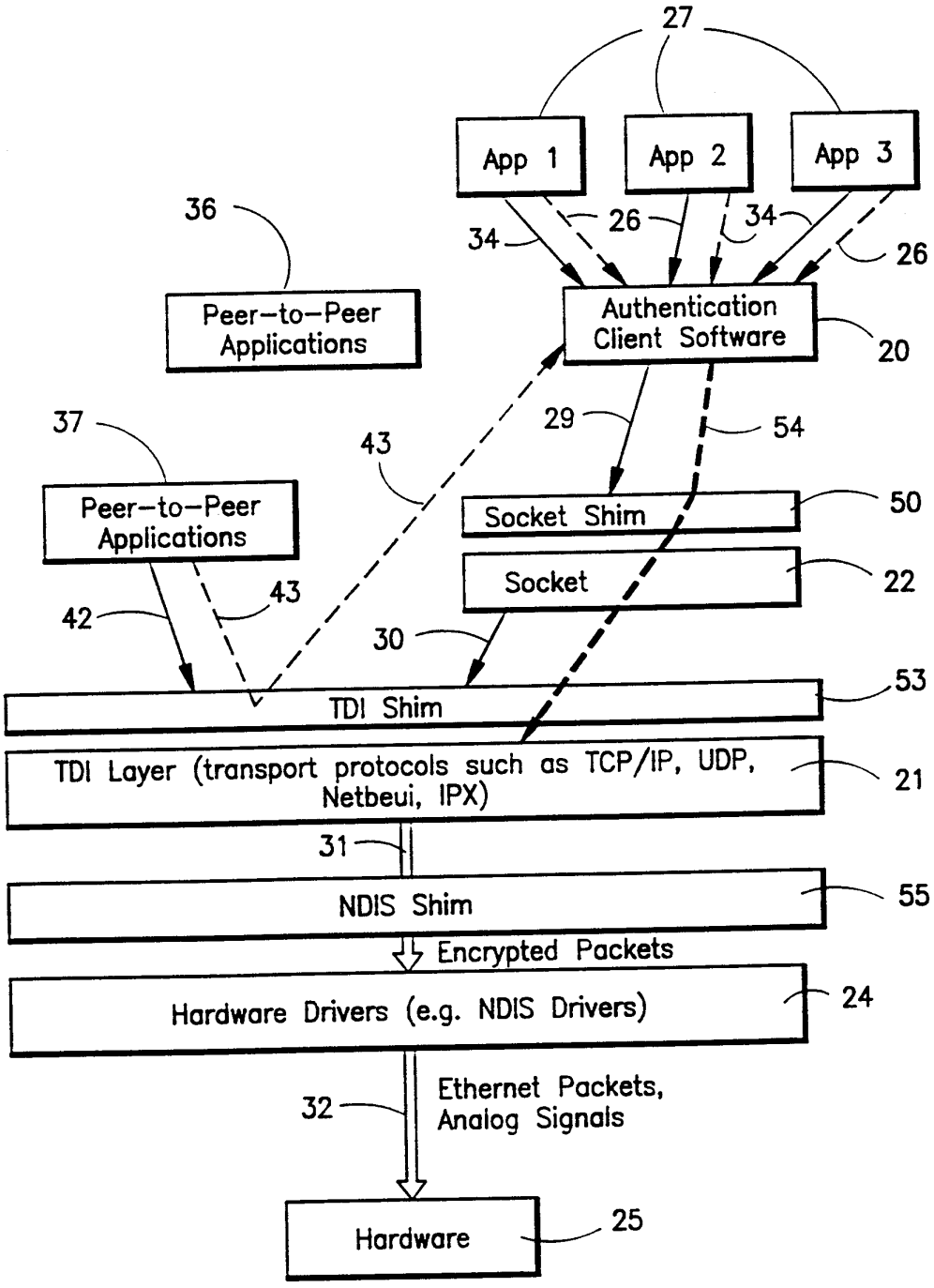

27
App 1
App 2
App 3
36
34
26
34
26
Peer–to–Peer Applications
Authentication Client Software
20
37
29
54
43
Peer–to–Peer Applications
Socket Shim
50
Socket
22
42
43
30
TDI Shim
53
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
21
31
NDIS Shim
55
Encrypted Packets
Hardware Drivers (e.g. NDIS Drivers)
24
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 5

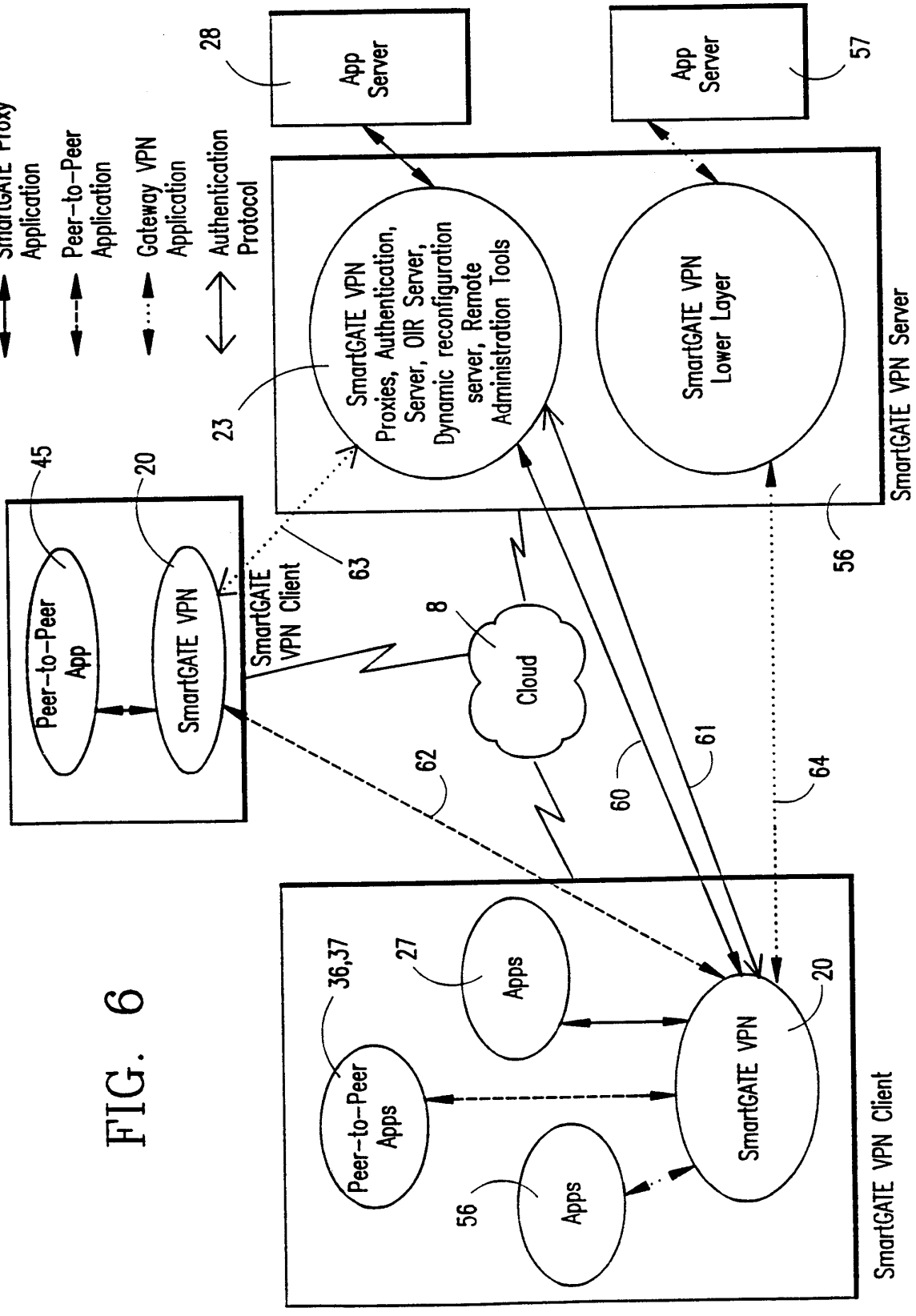

SmartGATE Proxy Application
Peer-to-Peer Application
Gateway VPN Application
Authentication Protocol
28
App Server
57
App Server
23
SmartGATE VPN Proxies, Authentication, Server, OIR Server, Dynamic reconfiguration server, Remote Administration Tools
SmartGATE VPN Lower Layer
SmartGATE VPN Server
56
45
20
Peer-to-Peer App
SmartGATE VPN
SmartGATE VPN Client
63
8
Cloud
62
60
61
64
36,37
27
Apps
Peer-to-Peer Apps
56
Apps
SmartGATE VPN
20
SmartGATE VPN Client

FIG. 6

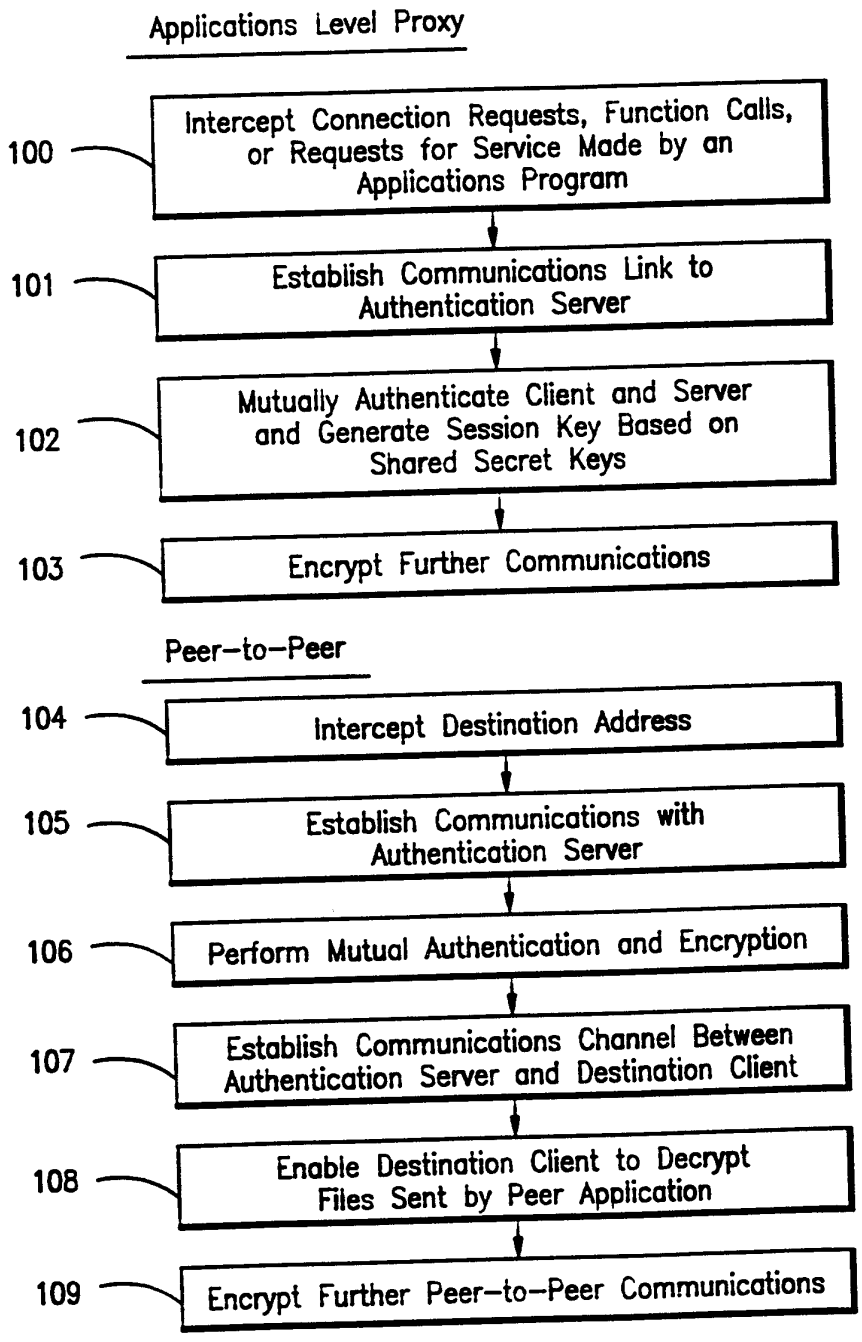

Applications Level Proxy
100
Intercept Connection Requests, Function Calls, or Requests for Service Made by an Applications Program
101
Establish Communications Link to Authentication Server
102
Mutually Authenticate Client and Server and Generate Session Key Based on Shared Secret Keys
103
Encrypt Further Communications
Peer-to-Peer
104
Intercept Destination Address
105
Establish Communications with Authentication Server
106
Perform Mutual Authentication and Encryption
107
Establish Communications Channel Between Authentication Server and Destination Client
108
Enable Destination Client to Decrypt Files Sent by Peer Application
109
Encrypt Further Peer-to-Peer Communications

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17198

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :395/187.01

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 186, 188.01, 200.17, 200.12; 380/49, 21, 25, 4

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

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

APS, STN, IEEE ProQuest
search terms: virtual private network, shims, DLLs, protocol layers, Winsock, sockets, encryption, authentication.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,657,390 A (ELGAMAL ET AL) 12 AUGUST 1997, FIGURES 1-8, COL. 3, LINES 20-55, COL. 5, LINE 15 TO COL. 8, LINE 32, COL. 11, LINE 1 TO COL. 16, LINE 49.	1,5,6,16,17,18,19,23,31
A	US 5,602,918 A (CHEN ET AL) 11 FEBRUARY 1997, SEE ENTIRE PATENT.	1-34
A	US 5,550,984 A (GELB) 27 AUGUST 1996, ABSTRACT, COL. 3, LINE 52 TO COL. 4, LINE 45, COL.6, LINES 27-55.	1-34
Y	HURWICZ, A VIRTUAL PRIVATE AFFAIR, BYTE MAGAZINE, JULY 1997, PAGES 79-87.	1,5,6,16,17,18,19,23,31

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
22 OCTOBER 1998

Date of mailing of the international search report
12 NOV 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
JOSEPH PALYS
Telephone No. (703) 305-9600

Form PCT/ISA/210 (second sheet)(July 1992)*

(12) UK Patent Application (19) GB (11) 2 334 181 (13) A

(43) Date of A Publication 11.08.1999

(21) Application No 9802545.5

(22) Date of Filing 06.02.1998

(51) INT CL[6]
H04Q 7/32

(52) UK CL (Edition Q)
H4L LDSC

(56) Documents Cited
US 5613204 A US 5109403 A

(58) Field of Search
UK CL (Edition P) H4L LDSC LDSU LECC LECX
INT CL[6] H04Q 7/32 7/38
Online: WPI

(71) Applicant(s)
NEC Technologies (UK) Ltd
(Incorporated in the United Kingdom)
Castle Farm Campus, Priorslee, TELFORD, Shropshire,
TF2 9SA, United Kingdom

(72) Inventor(s)
Charles Marie Herve Noblet

(74) Agent and/or Address for Service
J W White
NEC Technologies (UK) Ltd, Level 3, The Imperium,
Imperial Way, READING, Berks, RG2 0TD,
United Kingdom

(54) Abstract Title
Over-the-air re-programming of radio transceivers

(57) A method of downloading reprogramming data from a network for installation in a mobile station makes use of a dedicated small bandwidth pilot channel. The mobile station obtains from the base station the radio access parameters of a second channel. The second channel is a large bandwidth (bootstrap) channel suitable for fast transfer of data. The bootstrap channel is logically mapped onto a local transmission mode such as DECT or GSM by the mobile station and re-programming data may be downloaded from the base station via the bootstrap channel.

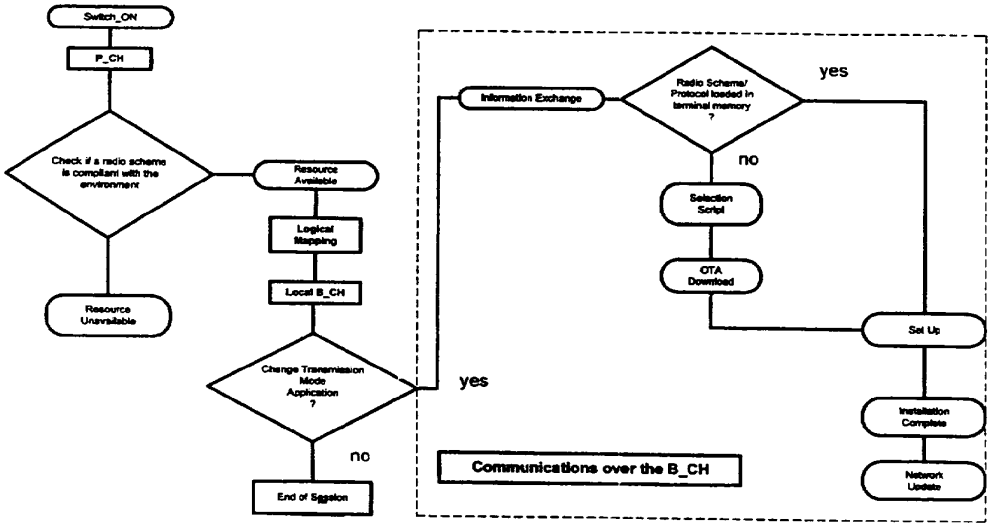


Figure 2

GB 2 334 181 A

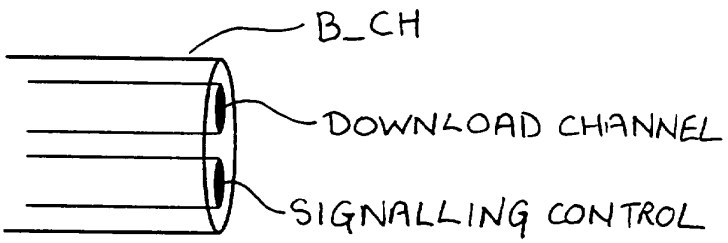


Figure: 1

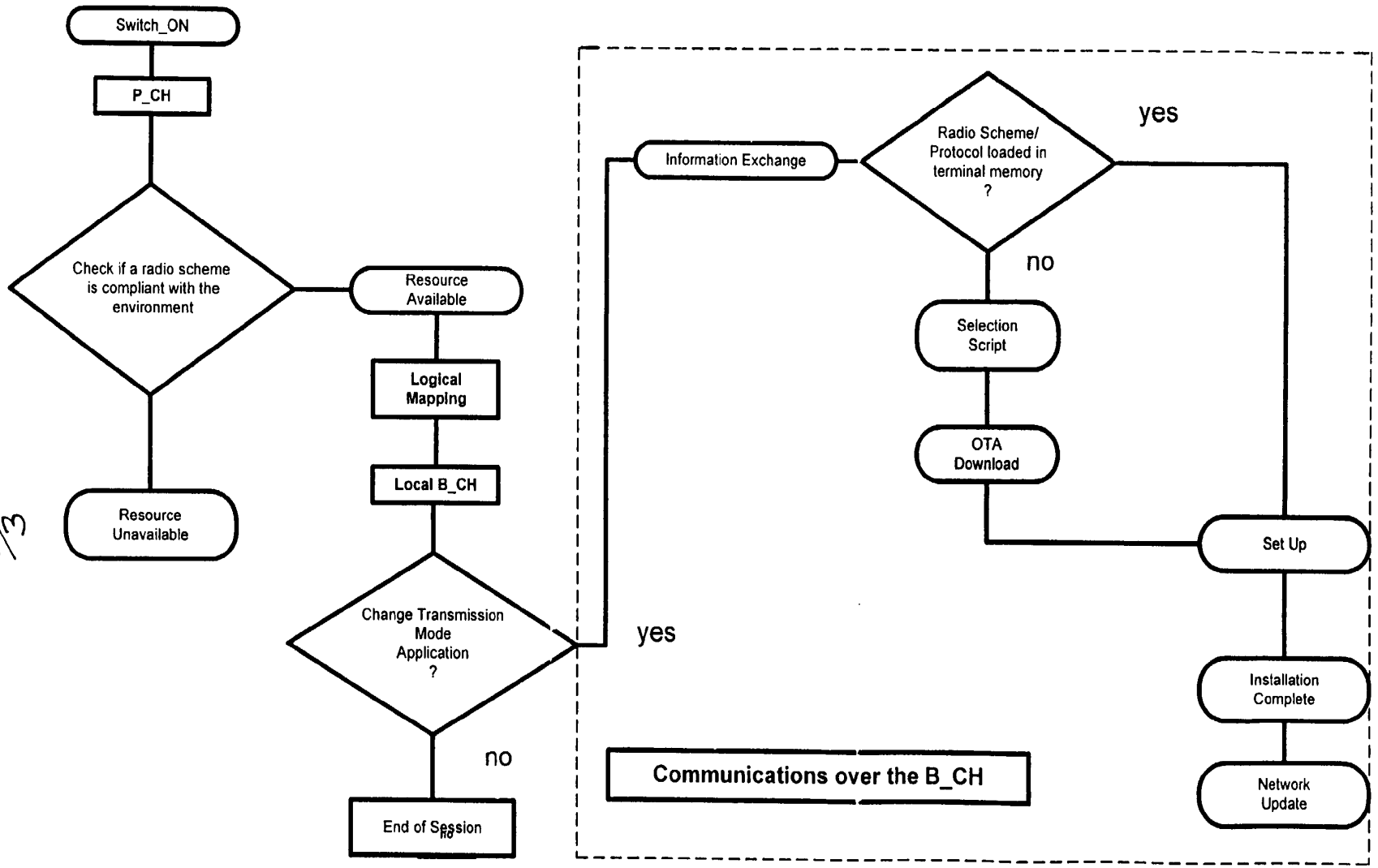
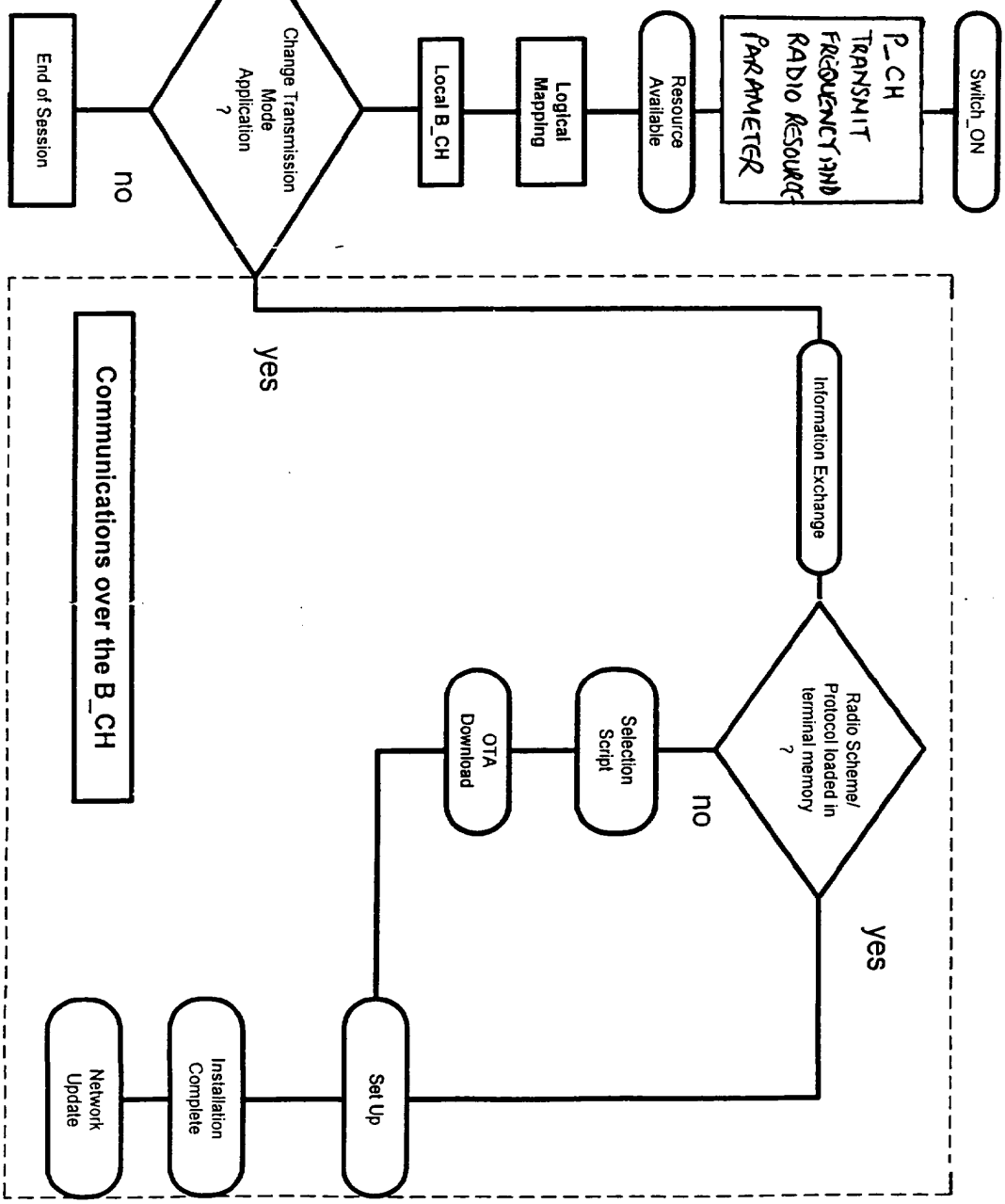


Figure 2

2/3

385

Figure 3


Switch_ON
P_CH TRANSMIT FREQUENCY AND RADIO RESOURCE PARAMETER
Resource Available
Logical Mapping
Local B_CH
Change Transmission Mode Application ?
no
End of Session
yes
Information Exchange
Radio Scheme/ Protocol loaded in terminal memory ?
no
Selection Script
OTA Download
yes
Set Up
Installation Complete
Network Update
Communications over the B_CH

Over-the-air re-programming of radio transceivers

This invention relates to radio transmitter/receivers and in particular it relates to a method of re-programming radio transmitter/receivers over-the-air.

A radio transmitter/receiver (transceiver) such as a radiotelephone is designed for operation with particular types of networks such as GSM 900 or DCS 1800. Intended use of the radiotelephone with a particular network(s) in a restricted geographical area, however, requires that the telephone be configured so as properly to communicate with the particular network (s). The user of a radiotelephone will usually have a telephone which has been configured for communication with a so called "home network". The home network is the local network usually most used by the subscriber.

The area within which a user of e.g. a GSM radiotelephone may operate, however, is considerable and is not limited to the home network but may be used on many other networks throughout the world. Use of a handset outside the home network is known as "roaming".

When the radiotelephone is to be used in roaming it is often necessary for it to have a configuration different to that for use with the home network. It is possible for re-configuration of radio transmitter/receivers to be effected by means of signals received across the air interface.

It is also convenient for the radio to be re-configurable over the air interface so as to support different types of communication and user applications e.g. addition of address book manager, whether or not it is located in the home network.

Over the air re-programming of radio receivers is well known in the art and reference may be made to US patent 5 381 138 for example. The capability to obtain programming data from a network is particularly useful for a roaming radio transmitter/receiver.

When beginning operation in an area for which the radiotelephone is not configured and it is required to download the data for reconfiguration from one of the available networks, a communication link must first be established with the network of interest. It has been proposed that a pilot channel be established in all areas from which the roaming radiotelephone may obtain the data necessary for reconfiguration.

A pilot channel of this type, however, will require a relatively large bandwidth to allow a sufficiently fast transfer of the data required.

According to the invention there is provided a method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.

Examples of the invention will now be described in more detail with reference to the accompanying figures in which

figure 1 Illustrates the logical structure of the bootstrap channel

figure 2 Is a flow diagram of a reconfiguration process

figure 3 Is a flow diagram of an alternative reconfiguration process

A roaming radio transmitter/receiver (mobile) is located in a region served by one or more networks and the user wishes to communicate with a network from which he can obtain reprogramming data and subsequently begin communicating with the network in the communication mode selected.

A pilot channel broadcast is maintained in the region and contained in the pilot channel broadcast there is at least sufficient information for the mobile to connect to a second channel which we shall call the bootstrap channel. Conveniently the pilot channel will be broadcast in all regions over a standardised radio interface. Only a small bandwidth is required for the pilot channel because of the small amount of information contained in the broadcast.

The small bandwidth requirement makes the task of standardisation much easier with respect to the pilot channel. The wider bandwidth channels are more conveniently assigned locally for ease of implementation.

The Pilot Channel (P_CH) broadcasts a list of sets of parameters corresponding to networks available in the region. The mobile receives the network transmission through the P_CH. If the existing configuration of the mobile is matched to the available regional radio schemes, then a second channel the bootstrap channel (B_CH) is logically mapped onto the selected transmission mode. The base station and mobile exchange information over this dedicated logical channel.

The Bootstrap channel is logically mapped on top of one of the default modes of the terminal; a mapping of a logical B_CH onto the physical GSM channel for instance may be implemented. Once the mapping has been effected the terminal may download data from the base station. The bootstrap channels provided by each operator may accommodate differing services with regard to the applications available for downloading.

The flow diagram shown at fig 3 depicts a reconfiguration procedure.

When the mobile is switched on, it reads the Pilot Channel broadcast. The mobile must be configured to support the (standardised) radio interface of the Pilot Channel. The Pilot Channel carries local radio parameters (standards supported in the regional environment in which the mobile is located). After processing the received information, the mobile

communicates with the base station through the Bootstrap Channel, provided that the mobile has the minimum resources required by its local radio environment. Prior to the change of channel, P_CH to B_CH, a logical mapping of the Bootstrap Channel is performed within the mobile on the selected air interface.

When operation on a local B_CH transmission has been established, the user may wish to change some properties or the performance of his mobile and can request supply of the desired services from the network. If no changes are required then the mobile adopts the default transmission mode in stand-by and releases the allocated B_CH.

If the user requests a change then communication between the base station and mobile is maintained for the exchange, the nature of which will depend on the capabilities of both mobile and network. At least 3 conditions can affect the nature of this information exchange.

Firstly, the mobile may not be able to support the required software. Where the mobile is not able to support the required software, no communication channel is available to the mobile from the existing network resources and use of the mobile within the region will therefore not be possible.

Secondly, the required software may be stored already in the mobile's memory. In this situation there is no need to download a software module but the allocated B_CH connection is maintained for further operations as described.

Thirdly, the software module required to support a different type of communication or user application may need to be downloaded from the base station. Where the download of a software module is required, initially a selection script is downloaded to the mobile followed by downloading and installation of the required software.

When the installation of the required software into the mobile has been completed, the mobile signals to the network the achievement of correct reconfiguration. On receipt of the "correct reconfiguration" signal from the mobile details of the mobile identity and its present configuration are entered on the network database (to license the product for instance) .

With reference to figure 1, the logical structure of the bootstrap channel will include 2 logical sub-channels : a download channel and a signalling control channel (S_CH). The signalling control channel assists in the reduction of errors in transmission so as to allow correct software download.

In the above example, the first channel, the Pilot Channel, is standardised and the mobile must be configured to support the radio interface for the Pilot Channel. The second (bootstrap) channel may be subject to local definition through logical mapping on a local transmission mode e.g. GSM, DECT and the mobile is not initially configured to support the radio interface for the bootstrap channel..

An example of a method of reprogramming providing greater flexibility will now be given. In this example the mobile is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth (Pilot) channel and the second relatively large bandwidth (bootstrap) channel. That is to say that when the mobile is switched on in most and preferably all regions, the network can communicate with the mobile via both pilot and bootstrap channels.

In order for the mobile always to have the appropriate radio interface for the bootstrap channel then this channel would need also to be standardised (in addition to the Pilot Channel). The parameters of the bootstrap channels provided in different regions may have local variations in terms of e.g. allocated frequency, data rate and available user applications.

With reference to figure 3 which is a flow diagram of the reconfiguration process for this example, the mobile when switched on reads the Pilot Channel broadcast. The allocated frequency and radio resource parameters for the bootstrap channel contained in the pilot channel broadcast are processed and any required logical mapping effected. After processing the received information, the mobile communicates with the base station through the Bootstrap Channel.

The condition likely to be experienced in the previous example whereby the mobile is not able to support the required software and no communication channel is available to the mobile from the existing network resources does not apply in this arrangement. The communication via the bootstrap

channel allows the request for and supply of the software module necessary to establish communication with the network. The transfer to the bootstrap channel does not depend on the existing configuration of the mobile since the bootstrap channel is standardised in this example and the mobile is equipped to interface, via the pilot channel, with the bootstrap channel.

The services and structure offered by the Bootstrap Channel are common for both of the above examples, however, the requirements on the terminals and networks differ.

The bootstrap channel will provide the following services by means of over -the-air (OTA) reconfiguration :
capability Exchange - the terminal provides some information to the network on its current configuration and capabilities.
module Selection : at this stage the user specifies the software that his terminal requires to download. This operation could be compared to an installation script.
data download : transfer of the data. In some cases software code will have to be downloaded whilst in other cases the software may already be implemented in the mobile. In the latter case, a set-up mechanism would be sufficient to initiate the reconfiguration.

Once the mobile and the base station are synchronised on the bootstrap channel, information exchange can begin.

Claims

1. A method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.

2. A method of downloading reprogramming data from a network as in claim 1 where first, dedicated relatively small bandwidth channel has a standard radio interface common to many network locations.

3. A method of downloading reprogramming data from a network as in claim 2 where second relatively large bandwidth channel has a standard radio interface common to many network locations.

4. A method of downloading reprogramming data from a network as in claims 1 to 3 where first, dedicated relatively small bandwidth channel broadcasts a list of sets of parameters corresponding to networks available in the region.

5. A method of downloading reprogramming data from a network as in claim 1 where the radio transmitter/receiver is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth channel and the second relatively large bandwidth channel.

The Patent Office

10

Application No: GB 9802545.5 **Examiner:** Glyn Hughes
Claims searched: 1 to 5 **Date of search:** 17 August 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4L (LDSC, LDSU, LECC, LECX)

Int Cl (Ed.6): H04Q 7/32, 7/38

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	US 5613204	(HABERMAN ET AL) see in particular column 15 lines 48 to 50	1
X	US 5109403	(SUTPHIN) see abstract	1

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

(12) UK Patent Application (19) GB (11) 2 340 702 (13) A

(43) Date of A Publication 23.02.2000

(21) Application No 9912200.4

(22) Date of Filing 25.05.1999

(30) Priority Data
(31) 09087823 (32) 29.05.1998 (33) US

(51) INT CL[7]
H04L 29/06 // H04L 9/00 12/22 12/46

(52) UK CL (Edition R)
H4P PPEB

(56) Documents Cited
EP 0887979 A2 EP 0825748 A2 WO 98/31124 A1

(58) Field of Search
UK CL (Edition Q) H4P PPA PPEB PPEC PPG
INT CL[6] H04L 12/22 12/46 12/66 29/06
ONLINE DATABASES: WPI, EPODOC, JAPIO

(71) Applicant(s)
Sun Microsystems Inc
(Incorporated in USA - Delaware)
901 San Antonio Road, MS Palo Alto-521,
California 94303, United States of America

(72) Inventor(s)
Joseph E Provino

(74) Agent and/or Address for Service
D Young & Co
21 New Fetter Lane, LONDON, EC4A 1DA,
United Kingdom

(54) Abstract Title
Accessing a server in a virtual private network protected by a firewall

(57) A virtual private network 15 has a firewall 30, at least one server 31 and a nameserver 32 each having a network address (eg. an n-bit integer address). The server 31 also has a secondary address (eg. a human readable address) and the nameserver 32 provides an association between the secondary address and the network address. An authorised external device 12 establishes a secure tunnel between itself and the firewall for communication using encryption. When the external device requests connection to server 31 using the secondary address of server 31, the firewall provides external device 12 with the network address of the nameserver 32. The external device 12 transmits a request for resolution of the network address associated with the secondary address to the nameserver through the firewall. The nameserver then transmits the network address of the server 31 through the firewall to the external device using the secure tunnel. The external device can thereafter use the network address of server 31 in subsequent communications.

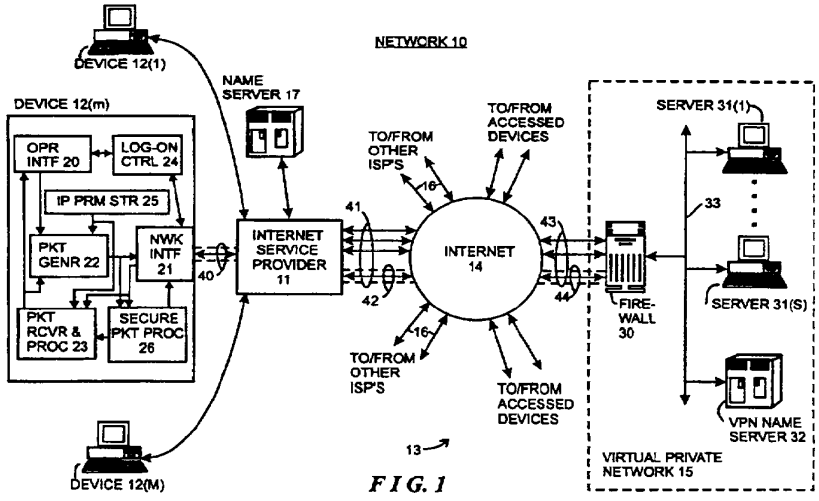


FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 340 702 A

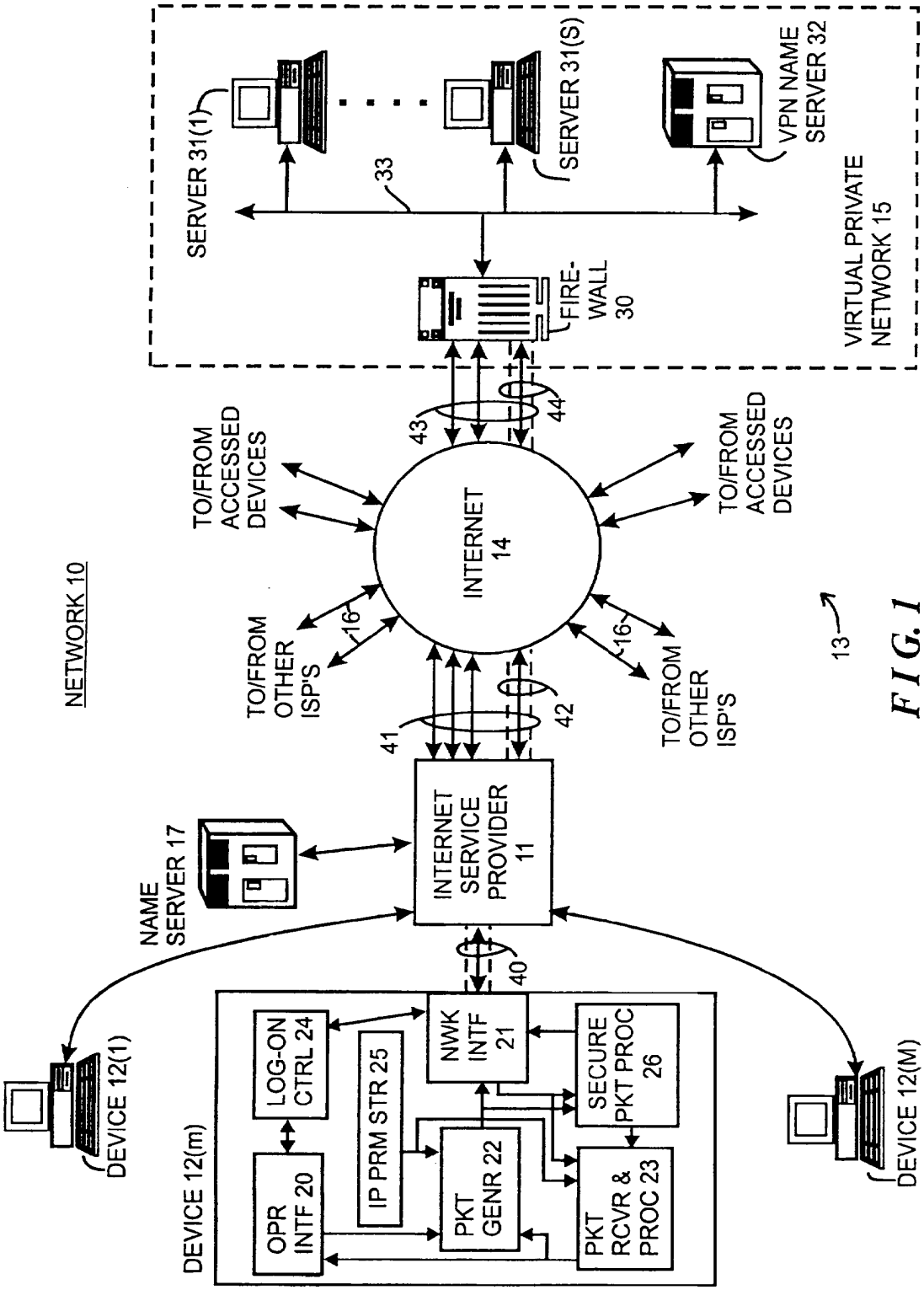

NETWORK 10
VIRTUAL PRIVATE NETWORK 15
SERVER 31(1)
SERVER 31(S)
VPN NAME SERVER 32
33
FIRE-WALL 30
43
44
TO/FROM ACCESSED DEVICES
TO/FROM ACCESSED DEVICES
INTERNET 14
TO/FROM OTHER ISP'S
16
16
TO/FROM OTHER ISP'S
41
42
13
NAME SERVER 17
INTERNET SERVICE PROVIDER 11
40
DEVICE 12(1)
DEVICE 12(m)
DEVICE 12(M)
LOG-ON CTRL 24
NWK INTF 21
SECURE PKT PROC 26
IP PRM STR 25
OPR INTF 20
PKT GENR 22
PKT RCVR & PROC 23

FIG. 1

FIELD OF THE INVENTION

The invention relates generally to the field of digital communications systems and methods, and more particularly to systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.

BACKGROUND OF THE INVENTION

Digital networks have been developed to facilitate the transfer of information, including data and programs, among digital computer systems and other digital devices. A variety of types of networks have been developed and implemented, including so-called "wide-area networks" (WAN's) and "local area networks" (LAN's), which transfer information using diverse information transfer methodologies. Generally, LAN's are implemented over relatively small geographical areas, such as within an individual office facility or the like, for transferring information within a particular office, company or similar type of organization. On the other hand, WAN's are generally implemented over relatively large geographical areas, and may be used to transfer information between LAN's as well as between devices that are not connected to LAN's. WAN's also include public networks, such as the Internet, which can carry information for a number of companies.

Several problems have arisen in connection with communication over a network, particularly a large public WAN such as the Internet. Generally, information is transferred over a network in message packets, which are transferred from one device, as a source device, to another device as a destination device, through one or more routers or switching nodes (generally, switching nodes) in the network. Each message packet includes a destination address which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" may be thirty two or 128), which are difficult for a person to remember and enter when he or she wishes to enable a message packet to be transmitted. To relieve a user of the necessity of remembering and entering specific integer Internet

addresses, the Internet provides second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism, Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate the use of human-readable names, nameservers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. When an operator at one device, wishing to transmit a message packet to another device, enters the other device's human-readable name, the device will initially contact a nameserver. Generally, the nameserver may be part of the ISP itself or it may be a particular device which is accessible through the ISP over the Internet; in any case, the ISP will identify the nameserver to be used to the device when the device logs in to the ISP. If, after being contacted by the device, the nameserver has or can obtain an integer Internet address for the human-readable domain name, it (that is, the nameserver) will provide the integer Internet address corresponding to the human-readable domain name to the operator's device. The device, in turn, can thereafter include the integer Internet address returned by the nameserver in the message packet and provide the message packet to the ISP for transmission over the Internet in a conventional manner. The Internet switching nodes use the integer Internet address to route the message packet to the intended destination device.

Other problems arise, in particular, in connection with the transfer of information over a public WAN such as the Internet. One problem is to ensure that information transferred over the WAN that the source device and the destination device wish to maintain confidential, in fact, remains confidential as against possible eavesdroppers which may intercept the information. To maintain confidentiality, various forms of encryption have been developed and are used to encrypt the information prior to transfer by the source device, and to decrypt the information after it has been received by the destination device. If it is desired that, for example, all information transferred between a particular source device and a particular destination device is maintained confidential, the devices can establish a "secure tunnel" therebetween, which essentially ensures that all information to be transferred by the source device to the destination device is encrypted (except for certain

protocol information, such as address information, which controls the flow of network packets through the network between the source and destination devices) prior to transfer, and that the encrypted information will be decrypted prior to utilization by the destination device. The source and destination devices may themselves perform the encryption and decryption, respectively, or the encryption and decryption may be performed by other devices prior to the message packets being transferred over the Internet.

A further problem that arises in particular in connection with companies, government agencies, and private organizations whose private networks, which may be LAN's, WAN's or any combination thereof, are connected to public WAN's such as the Internet, is to ensure that their private networks are secure against others whom the companies do not wish to have access thereto, or to regulate and control access by others whom the respective organizations may wish to have limited access. To accommodate that, the organizations typically connect their private networks to the public WAN's through a limited number of gateways sometimes referred to as "firewalls," through which all network traffic between the internal and public networks pass. Typically, network addresses of domains and devices in the private network "behind" the firewall are known to nameservers which are provided in the private network, but are not available to nameservers or other devices outside of the private network, making communication between a device outside of the private network and a device inside of the private network difficult.

SUMMARY OF THE INVENTION

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.

The invention provides a new and improved system and method for easing communications between devices connected to public networks such as the Internet and devices connected to private networks by facilitating resolution of secondary addresses, such as the Internet's human-readable addresses, to network addresses by nameservers or the like connected to the private networks.

In brief summary, an embodiment of the invention provides a system comprising a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the invention are described hereinafter, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 is a functional block diagram of a network constructed in accordance with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. 1 is a functional block diagram of a network 10 constructed in accordance with the invention. The network 10 as depicted in FIG. 1 includes an Internet service provider ("ISP") 11 which facilitates the transfer of message packets among one or more devices 12(1) through 12(M) (generally identified by reference numeral 12(m)) connected to ISP 11, and other devices, generally identified by reference numeral 13, over the Internet 14, thereby to facilitate the transfer of information in message packets among the devices 12(m) and 13. The ISP 11 connects to the Internet 14 over one or more logical connections or gateways or the like (generally referred to herein as "connections") generally identified by reference numeral 41. The ISP 11 may be a public ISP, in which case it connects to devices 12(m) which may be controlled by operators who are members of the general public to provide access by those operators to the Internet. Alternatively, ISP 11 may be a private ISP, in which case the devices 12(m) connected thereto are generally operated by, for example, employees of a particular company or governmental agency, members of a private organization or the like, to provide access by those employees or members to the Internet.

As is conventional, the Internet comprises a mesh of switching nodes (not separately shown) which interconnect ISP's 11 and devices 13 to facilitate the transfer of message packets thereamong. The message packets transferred over the Internet 14 conform to that defined by the so-called Internet protocol "IP" and include a header portion, a data portion, and may include a error detection and/or correction portion. The header portion includes information used to transfer the message packet through the Internet 14, including, for example, a destination address that identifies the device that is to receive the message packet as the destination device and a source address that identifies the device which generated the message packet. For each message packet, the destination and source addresses are each in the form of an integer that uniquely identifies the respective destination and source devices. The switching nodes comprising the Internet 14 use at least the destination address of each respective message packet to route it (that is, the respective message packet) to the destination device, if the destination device is connected to the Internet, or to an ISP 11 or other device connected to the Internet 14, which, in turn, will forward the message packet to the appropriate destination. The data portion of each message packet includes the data to be transferred

in the message packet, and the error detection and/or correction portion contains error detection and/or correction information which may be used to verify that the message packet was correctly transferred from the source to the destination device (in the case of error detection information), and correct selected types of errors if the message packet was not correctly transferred (in the case of error correction information).

The devices 12(m) connected to ISP 11 may comprise any of a number of types of devices which communicate over the Internet 14, including, for example, personal computers, computer workstations, and the like, with other devices 13. Each device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet, or the like. The devices 12(m) are generally constructed according to the conventional stored-program computer architecture, including, for example, a system unit, a video display unit and operator input devices such as a keyboard and mouse. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network and/or telephony interface devices for interfacing the respective device to the ISP 11. The processing devices process programs, including application programs, under control of an operating system, to generate processed data. The video display unit permits the device to display processed data and processing status to the user, and the operator input device enables the user to input data and control processing.

These elements of device 12(m), along with suitable programming, cooperate to provide device 12(m) with a number of functional elements including, for example, an operator interface 20, a network interface 21, a message packet generator 22, a message packet receiver and processor 23, an ISP log-on control 24, an Internet parameter store 25 and, in connection with the invention, a secure message packet processor 26. The operator interface 20 facilitates reception by the device

12(m) of input information from the operator input device(s) of device 12(m) and the display of output information to the operator on the video display device(s) of the device 12(m). The network interface 21 facilitates connection of the device 12(m) to the ISP 11 using the appropriate PPP or network protocol, to transmit message packets to the ISP 11 and receive message packets therefrom. The network interface 21 may facilitate connection to the ISP 11 over the public telephone network to allow for dial-up networking of the device 12(m) over the public telephone system. Alternatively or in addition, the network interface 21 may facilitate connection through the ISP 11 over, for example, a conventional LAN such as the Ethernet. The ISP log on control 24, in response to input provided by the operator interface 20 and/or in response to requests from programs (not shown) being processed by the device 12(m), communicates through the network interface 21 to facilitate the initialization ("log-on") of a communications session between the device 12(m) and the ISP 11, during which communications session the device 12(m) will be able to transfer information, in the form of, message packets with other devices over the Internet 14, as well as other devices 12(m') (m'≠m) connected to the ISP 11 or to other ISP's. During a log-on operation, the ISP log-on control 24 receives the Internet protocol ("IP") parameters which will be used in connection with message packet generation during the communications session.

During a communications session, the message packet generator 22, in response to input provided by the operator through the operator interface 20, and/or in response to requests from programs (not separately shown) being processed by the device 12(m), generates message packets for transmission through the network interface 21. The network interface 21 also receives message packets from the ISP 11 and provides them to message packet receiver and processor 23 for processing and provision to the operator interface 20 and/or other programs (not shown) being processed by the device 12(m). If the received message packets contain information, such as Web pages or the like, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit. In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.

Generally, elements such as the operator interface 20, message packet generator 22, message packet receiver and processor 23, ISP log-on control 24 and Internet parameter store 25 may comprise elements of a conventional Internet browser, such as Mosaic, Netscape Navigator and Microsoft Internet Explorer.

In connection with the invention, as noted above the device 12(m) also includes a secure message packet processor 26. The secure message packet processor 26 facilitates the establishment and use of a "secure tunnel," which will be described below, between the device 12(m) and another device 12 (m') (m'≠m) or 13. Generally, in a secure tunnel, information in at least the data portion of message packets transferred between device 12(m) and a specific other device 12(m') (m'≠m) or 13 is maintained in secret by, for example, encrypting the data portion prior to transmission by the source device. Information in other portions of such message packets may also be maintained in secret, except for the information that is required to facilitate the transfer of the respective message packet between the devices, including, for example, at least the destination information, so as to allow the Internet's switching nodes and ISP's to identify the device that is to receive the message packet.

In addition to ISP 11, a number of other ISP's may connect to the Internet, as represented by arrows 16, facilitating communications between devices which are connected to those other ISP's with other devices over the Internet, which may include the devices 12(n) connected to ISP 11.

The devices 13 which devices 12(m) access and communicate with may also be any of a number of types of devices, including personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks. In connection with the invention, at least one of the devices will include at least one private network, identified as virtual private network 15, which may be in the form of a LAN or WAN. The virtual private network 15 may comprise any of the devices 12(m') (m'≠m) (thereby connecting to the Internet 14

through an ISP) or 13 (thereby connecting directly to the Internet 14); in the illustrative embodiment described herein, the virtual private network 15 will be assumed to comprise a device 13. The virtual private network 15 itself includes a plurality of devices, identified herein as a firewall 30, a plurality of servers 31(1) through 31(S) (generally identified by reference numeral 31(s)) and a nameserver 32, all interconnected by a communication link 33. The firewall 30 and servers 31(s) may be similar to any of the various types of devices 12(m) and 13 described herein, and thus may include, for example, personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks.

As noted above, the devices, including devices 12(m) and devices 13, communicate by transferring message packets over the Internet. The devices 12(m) and 13 can transfer information in a "peer-to-peer" manner, in a "client-server" manner, or both. Generally, in a "peer-to-peer" message packet transfer, a device merely transfers information in one or more message packets to another device. On the other hand, in a "client-server" manner, a device, operating as a client, can transfer a message packet to another device, operating as a server to for example, initiate service by the other device. A number of types of such services will be appreciated by those skilled in the art, including, for example, the retrieval of information from the other device, to enable the other device to perform processing operations, and the like. If the server is to provide information to the client, it (that is, the server) may generally be referred to as a storage server. On the other hand, if the server is to perform processing operations at the request of the client, it (that is, the server) may generally be referred to as a compute server. Other types of servers, for performing other types of services and operations at the request of clients, will be appreciated by those skilled in the art.

In a client/server arrangement, device 12(m) requiring service by, for example, a device 13, generates one or more request message packets requesting the required service, for transfer to the device 13. The request message packet includes the Internet address of the device 13 that is, as the destination device, to receive the message packet and perform the service. The device 12(m)

transfers the request message packet(s) to the ISP 11. The ISP 11, in turn, will transfer the message packet over the Internet to the device 13. If the device 13 is in the form of a WAN or LAN, the WAN or LAN will receive the message packet(s) and direct it (them) to a specific device connected therein which is to provide the requested service.

In any case, after the device 13 which is to provide the requested service receives the request message packet (s), it will process the request. If the device 12(m) which generated the request message packet(s), or its operator, has the required permissions to request the service from the device 13 which generated the request message packet, if the requested service is to initiate the transfer of information from the device 13 as a storage server to the device 12(m) as client, the device 13 will generate one or more response message packets including the requested information, and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). On the other hand, if the requested service is to initiate processing by the device 13 as a compute server, the device 13 will perform the requested computation service(s). In addition, if the device 13 is to return processed data generated during the computations to the device 12(m) as client, the device 13 will generate one or more response message packet(s) including the processed data and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). Corresponding operations may be performed by the devices 12(m) and 13, ISP 11 and Internet 14 in connection with other types of services which may be provided by the server devices 13.

As noted above, each message packet that is generated by devices 12(m) and 13 for transmission over the Internet 14 includes a destination address, which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" currently may be thirty two or 128). To relieve, in particular, an operator of a device 12(m) of the necessity of remembering specific integer Internet addresses and providing them to the device 12(m) to initiate generation of a message packet for transmission over the Internet, the Internet provides a second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism,

Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate human-readable domain names, ISP 11 is associated with a nameserver 17 (which may also be referred to as a DNS servers), which can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name. Generally, the nameserver may be part of or connected directly to the ISP 11, as shown in FIG. 1, or it may be a particular device which is accessible through the ISP over the Internet. In any case, as noted above, when the device 12(m) logs on to the ISP 11 during a communications session, the ISP 11 will assign various Internet protocol ("IP") parameters which the device 12(m) is to use during the communications session, which will be stored in the Internet parameter store 25. These IP parameters include such information as

(a) an Internet address for the device 12(m) which will identify the device 12(m) during the communications session, and

(b) the identification of a nameserver 17 that the device 12(m) is to use during the communications session.

The device 12(m), when it generates message packets for transfer, will include its Internet address (item (a) above) as the source address. The device(s)13 which receives the respective message packets can use the source address from message packets received from the device 12(m) in message packets which they (that is, device(s) 13) generate for transmission to the device 12(m), thereby to enable the Internet to route the message packets generated by the respective device 13 to the device 12(m). If the device 12(m) is to access the nameserver 17 over the Internet 14, the nameserver identification provided by the ISP 11 (item (b) above) will be in the form of an integer Internet address which will allow the device 12(m) to generate messages to the nameserver 17 requesting resolution of human-readable Internet addresses into integer Internet addresses. The ISP 11 may also assign other IP parameters to the device 12(m) when it logs on to the ISP 11, including, for example, the identification of a connection to the Internet 14 that is to be used for messages transmitted by the

device 12(m), particularly if the ISP 11 has multiple gateways. Generally, the device 12(m) will store the Internet parameters in the Internet parameter store 25 for use during the communications session.

When an operator operating device 12(m) wishes to enable the device 12(m) to transmit a message packet to a device 13, he or she provides the Internet address for the device 13 to the device 12(m), through the operator interface 20, and information, or the identification of information maintained by the device 12(m) that is to be transmitted in the message. The operator interface 20, in turn, will enable the packet generator 22 to the required packets for transmission through the ISP 11 over the Internet 11. If

(i) the operator has provided the integer Internet address, or

(ii) the operator has provided the human-readable Internet address, but the packet generator 22 already has the integer Internet address which corresponds to the human-readable Internet address provided by the operator,

the packet generator 22 may generate the packets directly upon being enabled by the operator interface 20, and provide them to the network interface 21 for transmission to the ISP 11.

However, if the operator has provided the human-readable Internet address for the device 13 to which the packets are to be transferred, and if the packet generator 22 does not already have the corresponding integer Internet address therefor, the packet generator 22 will enable the network address to be obtained from the nameserver 17 identified in the IP parameter store 25. In that operation, the packet generator 22 will initially contact nameserver 17 to attempt to obtain the appropriate integer Internet address from the nameserver 17. In these operations, the device 12(m) will generate appropriate message packets for transmission to the nameserver 17, using the nameserver's integer Internet address as provided by the ISP 11 when it (that is, the device 12(m)) logs on at the beginning of the communications session. In any case, if the nameserver 17 has or can obtain the integer Internet address for the human-readable name, it (that is, the nameserver 17) will

provide the integer Internet address to the device 12(m). The integer Internet address will be received by the packet generator 22 through the network interface 21 and packet receiver and processor 23. After the packet generator 22 receives the integer Internet address, it can generate the necessary message packets for transmission to the device 13 through the network interface 21 and ISP 11.

As noted above, one of the devices 13 connected to the Internet 14 is virtual private network 15, the virtual private network 15 including a firewall 30, a plurality of devices identified as servers 31(s), and a nameserver 32 interconnected by a communication link 33. The servers 31(s), firewall 30 and nameserver 32 can, as devices connected in a LAN or WAN, transfer information in the form of message packets thereamong. Since the firewall 30 is connected to the Internet 14 and can receive message packets thereover it has an Internet address. In addition, at least the servers 31(s) which can be accessed over the Internet also have respective Internet addresses, and in that connection the nameserver 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Generally, the virtual private network 15 is maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14, but which also desires to limit access to the servers 31(s) by devices 12(m) and other devices over the Internet 14 in a controlled manner. The firewall 30 serves to control access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15. In that operation, the firewall 30 also connects to the Internet 14, receives message packets therefrom for transfer to a server 31(s). If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). The

firewall may be similar to other devices 31(s) in the virtual private network 15, with the addition of one or more connections to the Internet, which are generally identified by reference numeral 43.

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm

and key that it (that is device 12(m)) will use to the firewall 30 during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel.

Thereafter, the device 12(m) and firewall 30 can transfer message packets over the secure tunnel. The device 12(m), in generating message packets for transfer over the secure tunnel, makes use of the secure packet processor 26 to encrypt the portions of the message packets which are to be encrypted prior to transmission by the network interface 21 to the ISP 11 for transfer over the Internet 14 to the firewall 30, and to decrypt the encrypted portions of the message packets received by the device 12(m) which are encrypted. In particular, after the packet generator 22 generates a message packet for transmission to the firewall 30 over the secure tunnel, it will provide the message packet to the secure packet processor 26. The secure packet processor 26, in turn, encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key. After the firewall 30 receives a message packet from the device 12(m) over the secure tunnel, it will decrypt it and, if the intended recipient of the message packet is another device, such as a server 31(s), in the virtual private network 14, it (that is, the firewall 30) will transfer the message packet to that other device over the communication link 33.

For a message packet that is to be transferred by a device, such as a server 31(s), in the virtual private network 15 to the device 12(m) over the secure tunnel, the firewall 30 will receive such to the message packet over the communication link 33 and encrypt the message packet for transfer over the Internet 14 to the ISP 11. The ISP 11, in turn, forwards the message packet to the device 12(m), in particular to its network interface 21. The network interface 21 provides the message packet to the secure packet processor 26, which decrypts the encrypted portions of the message packet, using the decryption algorithm and key.

A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that nameserver 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Thus, the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(s) which is to be accessed from that nameserver 17.

To accommodate this problem, when the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween, in addition to possibly providing the device 12(m) with the identifications of the encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel, the firewall 30 also provides the device 12(m) with the identification of a nameserver, such as nameserver 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). The identification of nameserver 32 is also stored in the IP parameter store 25, along with the identification of nameserver 17 which was provided by the ISP 11 when the device 12(m) logged on to the ISP 11 at the beginning of a communications session. Thus, when the device 12(m) is to transmit a message packet to a device, such as a server 31(s) in the virtual private network 14 using a human-readable Internet address provided by, for example, an operator, the device 12(m) will initially access the nameserver 17, as described above, to attempt to obtain the integer Internet address associated with the human-readable Internet address. Since nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m), it will send a response message packet so indicating. The device 12(m) will thereafter generate a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message packet provided by the device 12(m), it will provide the integer Internet address in a manner that is generally similar to that described above in connection

with nameserver 18, except that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m). In the message packet transmitted by the firewall 30, it will be appreciated that the integer Internet address in the message packet will be in the data portion of the message packet transferred over the secure tunnel and, accordingly, will be in encrypted form. The message packet will be processed by the device 12(m) in a manner similar to that described above in connection with other message packets received by it over the secure tunnel, that is, the message packet will be decrypted by the secure packet processor 26 prior to being provided to the packet receiver and processor 23 for processing. The integer Internet address for the server 31(s) can be cached in an access control list ("ACL") in the IP parameter store 25, along with the association of the human-readable Internet address thereto, an indication that the server 31(s) associated with that human-readable Internet address is to be accessed through the firewall 30 of the virtual private network 15, and the identifications of the encryption and decryption algorithms and keys to be used for encrypting and decrypting the appropriate portions of the message packets transmitted to server 31(s) and received from server 31(s).

It will be appreciated that, if the nameserver 32, in response to a message packet from the device 12(m) requesting the nameserver 32 to provide an integer Internet address for a human-readable Internet address provided by the device 12(m), if the nameserver 32 does not have an association between the human-readable Internet address and an integer Internet address, the nameserver 32 can provide a response message packet so indicating. If the device 12(m) has identification of other nameservers, such as may be associated with other virtual private networks (not shown), to which it (that is, device 12(m)) may have access, then the device 12(m) can attempt to access the other nameservers in a similar manner as described above. If the device 12(m) is unable to obtain an integer Internet address associated with the human-readable Internet address from any of the nameservers to which it has access, and which generally will be identified in its IP parameter store 25, it will generally be unable to access a device having the human-readable Internet address, and may so notify its operator or program which requested the access.

With this background, operations performed by the device 12(m) and virtual private network 15 in connection with the invention will be described in detail. Generally, operations proceed in two phases. In the first phase, the device 12(m) and virtual private network 15 cooperate to establish a secure tunnel through the Internet 14. In that first phase, the virtual private network 15, in particular the firewall 30 provide the identification of a nameserver 32, and may also provide the encryption and decryption algorithm and key information, as described above. In the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution human-readable Internet addresses to integer Internet addresses as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase.

Thus, in the first (secure tunnel establishment) phase, the device 12(m) initially generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30. The message packet will include an integer Internet address for the firewall (which may have been provided by the device's operator or a program being processed by the device 12(m) or have been provided by a the nameserver 17 after a human-readable Internet address was provided by the operator or a program), and which, in particular, is to enable the firewall 30 to establish secure tunnels therewith. If the firewall 30 accepts the secure tunnel establishment request, and if the firewall 30 provides the encryption and decryption algorithms and keys as noted above, it (that is, the firewall) will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys; as noted above, this response message packet will not be encrypted. When the device 12(m) receives the response message, the identifications of the encryption and decryption algorithms and keys will be stored in the IP parameter store 25.

At some point later in the first phase, the firewall 30 will also generate a message packet for transmission to the device 12(m) that includes the integer Internet address of the nameserver 32. For this message packet, the portion of the message packet that contains the integer Internet address of

the nameserver 32 will be encrypted, using encryption algorithm and key that can be decrypted using the decryption algorithm and key provided in the response message packet described above. This message will generally have a structure

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "DNS_ADRS:IIA(NS) indicates that "IIA(NS_32)" represents the integer Internet address of the nameserver 32, the nameserver which the device 12(m) is authorized to use, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted.

The initial portion of the message "<IIA(FW),IIA(DEV_12(m))>" forms at least part of the header portion of the message, and "<ENCR<<IIA(FW),IIA(DEV_12(m))><IIA(NS)>>>" represents at least part of the data portion of the message. The "<SEC_TUN>" represents an indicator in the header indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

After the device 12(m) receives the message from the firewall 30 as described above, since the message packet contains the <SEC_TUN> indicator, its network interface 21 will transfer the encrypted portion "<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>" to the secure packet processor 26 for processing. The secure packet processor will decrypt the encrypted portion, determine that the portion "IIA(NS_32)" is the integer Internet address of a nameserver, in

particular nameserver 32, that the device 12(m) is authorized to use, and store that address in the IP parameter store 25, along with an indication that message packets thereto are to be transferred to the firewall 30 and that data in the message packets is to be encrypted using the encryption algorithm and key previously provided by the firewall 30. It will be appreciated that, since the integer Internet address of nameserver 32 is transferred from the firewall to the device 12(m) in encrypted form, it will be maintained in confidence even if the packet is intercepted by a third party.

Depending on the particular protocol used to establish the secure tunnel, the firewall 30 and device 12(m) may also exchange message packets containing other information than that described above.

As noted above, in the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m), or a program being processed by device 12(m), wishes to have device 12(m) transmit a message packet to a server 31(s) in the virtual private network 15, if the operator, through the operator interface 20, or the program provides a human-readable Internet address, the device 12(m), in particular the packet generator 22, will initially determine whether the IP parameter store 25 has cached therein an integer Internet address that is associated with the human-readable Internet address. If not, the packet generator 22 will generate a request message packet for transfer to the nameserver 17 requesting it to provide the integer Internet address associated with the human-readable Internet address. If the nameserver 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. This message will generally have a structure

"<IIA(DEV_12(m)),IIA(FW)><SEC_TUN>

<ENCR<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>>"

where

(i) "IIA(DEV_12(m))" represents the source address, that is, integer Internet address of the device 12(m)

(ii) "IIA(FW)" represents the destination address, that is, the integer Internet address of the firewall 30

(iii) "IIA(NS_32)" represents the address of the nameserver 32

(iii) "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet generated by the packet generator 22, where "<IIA(DEV_12(m)),IIA(NS_32)> represents the header portion of the request message packet, and "<IIA_REQ>" represents the data portion of the request message packet,

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted, and

(v) "<SEC_TUN>" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

When the firewall 30 receives the request message packet generated by the secure packet processor 26, it will decrypt the encrypted portion of the message packet to obtain <<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet as generated by the packet generator 22. After obtaining the request message packet, the firewall 30 will transmit it over the communication link 33 to the nameserver 32. In that process, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to modify the request message packet to conform to the protocol of communication link 33.

After the nameserver 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the nameserver determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall. Generally, the response message packet will have a structure:

<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>

where

(i) "IIA(NS_32)" represents the source address, that is, integer Internet address of the nameserver 32,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, integer Internet address of the device 12(m), and

(iii) "IIA_RESP" represents the integer Internet address associated with the human-readable Internet address.

After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the nameserver 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet. Generally, the message packet generated by the firewall 30 has the structure:

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "SEC_TUN" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" (which constitutes the response message packet received from the nameserver 32) is encrypted.

In addition, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to process and/or modify the message packet to conform to the protocol of Internet 14.

When the device 12(m) receives the message packet from the firewall 30, it (that is, the message packet) will be provided to the secure packet processor 26. The secure packet processor 26, in turn, will decrypt the encrypted portion of the message packet to obtain the integer Internet address associated with the human-readable Internet address, and load that information in the IP parameter store 25. Thereafter, the device can use that integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address.

It will be appreciated that, if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby. The firewall 30 will, in response to the response message packet provided by the nameserver 32, also generate a message packet for transmission to the device 12(m), the message packet including an encrypted portion comprising the response message packet generated by the nameserver 32. After the device 12(m) receives the message packet, the encrypted portion will be decrypted by the secure packet processor 26, which, in turn, will notify the packet generator 22 that the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address. Thereafter, if the IP parameter store 25 contains the identification of another nameserver, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. On the other hand, if the IP parameter store 25 does not contain the identification of another nameserver, the packet generator 22 can notify the operator interface 20 or program that it is will be unable to generate a message packet for transmission to a device associated with the human-readable Internet address provided thereby.

An embodiment of the invention can provide a number of advantages. For example, it can provide a system for easing communications between devices connected to a public network such as the Internet 14, and devices connected to private networks such as virtual private network 15, by facilitating resolution

of human-readable addresses to network addresses by a nameservers connected to the private networks over a secure tunnel.

It will be appreciated that numerous modifications may be made to the arrangement described above in connection with FIG. 1. For example, although the network 10 has been described such that the identification of the encryption and decryption algorithms and keys are exchanged by the device 12(m) and firewall 30 during the dialog during which the secure tunnel is established, it will be appreciated that that information may be provided by the device 12(m) and firewall 30 separately from the establishment of a secure tunnel therebetween.

In addition, although an embodiment of the invention has been described in connection with the Internet, it will be appreciated that an embodiment of the invention can be used in connection with any network. Further, although an embodiment has been described in connection with a network which provides for human-readable network addresses, it will be appreciated that an embodiment can be used in connection with any network which provides for any form of secondary or informal network address arrangements.

It will be appreciated that a system in accordance with the invention can be constructed in whole or in part from special purpose hardware or a general purpose computer system, or any combination thereof, any portion of which may be controlled by a suitable program. Any program may in whole or in part comprise part of or be stored on the system in a conventional manner, or it may in whole or in part be provided in to the system over a network or other mechanism for transferring information in a conventional manner. Thus, such a computer program can form a product operable, when run on a computer, to provide the required functionality of an embodiment of the invention. The computer program product can be provided on a carrier medium, for example, a computer readable medium such as, for example, a memory, disc or other storage medium, or a transmission medium such as a telecommunications channel providing, for example, electrical, optical, wireless or other transmission. In addition, it will be appreciated that the system may be operated and/or otherwise controlled by means of information provided by an operator using operator input elements (not shown) which may be connected directly to the system or which may transfer the information to the system over a network or other mechanism for transferring information in a conventional manner.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that various variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention.

CLAIMS

1. A system comprising a virtual private network and an external device which communicate over a digital network,

the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary address and the network address,

the firewall, in response to a request from the external device to establish a connection therebetween, being configured to provide the external device with the network address of the nameserver, and

the external device, in response to a request requesting access to the internal device including the internal device's secondary address, being configured to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address, the firewall being configured to provide the address resolution request to the nameserver, the nameserver being configured to provide the network address associated with the secondary address, the firewall in turn being further configured to provide the network address in a network address response message for transmission over the connection to the external device.

2. A system according to claim 1, wherein the external device is further configured to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

3. A system according to claim 1 or claim 2, wherein the external device is configured to connect to the network through a network service provider.

4. A system according to claim 3, wherein the external device is configured to establish a communications session with the network service provider, the network service provider providing the external device with the identification of a further nameserver, the further nameserver being configured to provide an association between a secondary address and a network address for at least one device.

5. A system according to any preceding claim, wherein the external device is configured to maintain a list of nameservers which have been identified to said external device, the external device being configured to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being configured to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

6. A system according to any preceding claim, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

7. A method of operating a system comprising a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a

secondary address, the nameserver being configured to provide an association between the secondary address and the network address, the method comprising the steps of:

A. enabling the firewall, in response to a request from the external device to establish a connection therebetween, provide the external device with the network address of the nameserver; and

B. enabling

(i) the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

(ii) the firewall to provide the address resolution request to the nameserver,

(iii) the nameserver to provide the network address associated with the secondary address, and

(iv) the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

8. A method according to claim 7, wherein the external device is further enabled to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

9. A method according to claim 7 or claim 8, wherein the external device is enabled to connect to the network through a network service provider.

10. A method according to claim 9, wherein the external device is enabled to establish a communications session with the network service provider, the network service provider being enabled to provide the external device with the identification of a further nameserver, the further nameserver being enabled to provide an association between a secondary address and a network address for at least one device.

11. A method according to any one of claims 7 to 10, wherein the external device is enabled to maintain a list of nameservers which have been identified to said external device, the external device being enabled to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

12. A method according to any one of claims 7 to 10, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

13. A computer program product for use in connection with a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary

address and the network address, the computer program product comprising :

A. a nameserver identification code module configured to enable the firewall, in response to a request from the external device to establish a connection therebetween, to provide the external device with the network address of the nameserver,

B. a network address request message generating code module for enabling the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

C an address resolution request forwarding module for enabling the firewall to provide the address resolution request to the nameserver,

D. a nameserver control module for enabling the nameserver to provide the network address associated with the secondary address, and

E. a network address response message forwarding module for enabling the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

14. A computer program product according to claim 13, further comprising a network address utilization module configured to enable the external device to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

15. A computer program product according to claim 13 or claim 14, further comprising a network service provider control module for enabling the external device to connect to the network through a network service provider.

16. A computer program product according to claim 15, wherein the network service provider control module includes a communications session establishment module for enabling the external device to a communications session with the network service provider and receive therefrom identification of a further nameserver.

17. A computer program product according to any one of claims 13 to 16, further including nameserver interrogation control module for enabling the external device to maintain a list of nameservers which have been identified to said external device, and to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

18. A computer program product according to any one of claims 13 to 16, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

19. A computer program product according to any one of claims 13 to 18 on a carrier medium.

20. A computer program product according to claim 19, wherein the carrier medium is a computer readable medium.

21. A computer program product according to claim 19, wherein the carrier medium is a transmissions medium.

22. A system substantially as hereinbefore described with reference to the accompanying drawings.

23. A method substantially as hereinbefore described with reference to the accompanying drawings.

24. A computer program product substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

34

INVESTOR IN PEOPLE

Application No:	GB 9912200.4	**Examiner:**	Gareth Griffiths
Claims searched:	All	**Date of search:**	7 December 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): H4P (PPA, PPEB, PPEC, PPG)

Int Cl (Ed.6): H04L 12/22, 12/46, 12/66, 29/06

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, P	EP0887979 A2	(SUN MICROSYSTEMS) col.15 line 35 - col.17 line 24	1, 2, 5-8, 11-14, 17-21
A	EP0825748 A2	(AT&T) col.6 line 46 - col.11 line 40	
A, P	WO98/31124 A1	(HANSON) p.5 line 2 - p.6 line 25	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Electronic Patent Application Fee Transmittal

Application Number:	11840560
Filing Date:	17-Aug-2007
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royaee/Melissa Molchan
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2

Filed as Large Entity

Utility under 35 USC 111(a) 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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	8151925
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Melissa Molchan
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	04-AUG-2010
Filing Date:	17-AUG-2007
Time Stamp:	13:03:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	8688
Deposit Account	501133
Authorized User	

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 (SB/08)	0063.pdf	65388 ceecf7884a35a2007848134d6dbf923ca54f35a2	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Foreign Reference	EP0838930A2.pdf	1724786 9a383b35683829ae78abb4965b90cde255795d93	no	34
Warnings:					
Information:					
3	Foreign Reference	EP0814589A2.pdf	1094602 10c06cd368d846b9f6c82e5622edd22ebc63e401	no	19
Warnings:					
Information:					
4	Foreign Reference	GB2317792A.pdf	1256657 d50989c41fac545a0929025d919331dfbf7136ef	no	34
Warnings:					
Information:					
5	Foreign Reference	WO9827783A1.pdf	846395 2a2ead44cf92a436d19c46f7f35211b7e6ad33cf	no	23
Warnings:					
Information:					
6	Foreign Reference	WO99011019.pdf	2034462 a88bd9be7182a86a8e75ebf9a5aa6e210b0962a5	no	60
Warnings:					
Information:					
7	Foreign Reference	GB2334181A.pdf	431753 98657594c9b37568cbca8e5569b8b1b6fd6f75a0	no	14
Warnings:					
Information:					
8	Foreign Reference	GB2340702A.pdf	1504772 b9d55f72785502abe4081ceb482776f5d62d0f15	no	36
Warnings:					
Information:					

9	NPL Documents	Baumgartner.pdf	535114 e1cfd368a442fe0e98ec5f0b34dc39d0d51aee53	no	20
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	NPL Documents	Chapman.pdf	1713700 39c5c492b168aa3e7de9fca2a4031545bed0e957	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	NPL Documents	Davila.pdf	461212 0300df8d7b65f715e893e7e8d5e7985e93b9ed97	no	18
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	NPL Documents	DeRaadt.pdf	333587 fdad8832507203c9875d1e55fdc679bf42cecc48	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	NPL Documents	Eastlake.pdf	1007823 7f990c13c14c9426828dd74c35dd10f320f607b2	no	45
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	NPL Documents	Gunter.pdf	330364 b806a4f735e709274fa23d1b659fcf93f2e555a2	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
15	NPL Documents	Shimizu.pdf	1284498 e3b8ee1a0847be8b7e6a6bc5791dafc815d3ae15	no	15
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
16	NPL Documents	Stallings.pdf	1451887 b32ca3a1d283b7ceeadc81e075be896ce51656dd	no	42
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
17	NPL Documents	Takata.pdf	109936 009f8475adb2a0557fdfcff79670b4a3112a0119	no	3
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
18	NPL Documents	Wells.pdf	63145 095ce48eaedeaf4359dd456e88732c1e895de5e3	no	1
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
19	Fee Worksheet (PTO-875)	fee-info.pdf	30429 44729d361de6618a2b0893ab81c890a3a85c18fe	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	16280510	

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/840,560	08/17/2007	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		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), (i), 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(i))	minus 20 =	*	X $ =		OR	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	
	06/28/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 60	Minus	** 20	= 40	X $ =		OR	X $52=	2080
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	2080

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	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))							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:
/WANDA D. MITCHELL/

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
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

23630 e 07/15/2010

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

Paper No.

Application No.:	**11/840,560**	**Date Mailed:**	**07/15/2010**
First Named Inventor:	Larson, Victor,	Examiner:	LIM, KRISNA
Attorney Docket No.:	077580-0063 (VRNK-1CP3CN2	Art Unit:	2453
Confirmation No.:	1537	Filing Date:	08/17/2007

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

Commissioner for Patents

PTO-90c (Rev.08-06)

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No. 11/840,560	Applicant(s) LARSON ET AL.	
		Art Unit 1700	

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

The amendment document filed on *28 June, 2010* is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

- ☒ 1. Amendments to the specification:
  - ☒ A. Amended paragraph(s) do not include markings.
  - ☐ B. New paragraph(s) should not be underlined.
  - ☐ C. Other _____.
- ☐ 2. Abstract:
  - ☐ A. Not presented on a separate sheet. 37 CFR 1.72.
  - ☐ B. Other _____.
- ☐ 3. Amendments to the drawings:
  - ☐ A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
  - ☐ B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
  - ☐ C. Other _____.
- ☐ 4. Amendments to the claims:
  - ☐ A. A complete listing of all of the claims is not present.
  - ☐ B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
  - ☐ C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
  - ☐ D. The claims of this amendment paper have not been presented in ascending numerical order.
  - ☐ E. Other: _____.
- ☐ 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4): For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance, or a drawing submission (only) If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.

2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a Quayle action. If any of above boxes 1 to 4 are checked, the correction required is only the corrected section of the non-compliant amendment in compliance with 37 CFR 1.121.

   Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.
   Failure to timely respond to this notice will result in:
   Abandonment of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or
   Non-entry of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable /WANDA D. MITCHELL/ Telephone No: (571)272-1032

Docket No.: 077580-0063 (VRNK-1CP3CN2) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Victor Larson et al.	:	Customer Number: 23630
	:	
	:	Confirmation Number: 1537
	:	
Application No.: 11/840,560	:	Group Art Unit: 2453
	:	
Filed: August 17, 2007	:	Examiner: Lim, Krisna
	:	

For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

AMENDMENT "A"

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

Sir:

In response to the Office action dated March 19, 2010, please amend the above-identified application and consider the accompanying remarks as follows:

Amendments to the specification begin on page 2 of this paper.

Amendments to the claims begin on page 3 of this paper

Remarks begin on page 10 of this paper.

Amendments to the specification:

Please delete paragraph [0001] in its entirety, and substitute therefor:

[0001] This application claims priority from and is a continuation of a co-pending U.S. application serial number 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504; which is a continuation of U.S. application serial number 09/558,210, filed April 26, 2000, now abandoned, which in turn is a continuation-in-part of previously-filed U.S. application serial number 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002, which in turn claims priority from and is a continuation-in-part patent application of previously-filed U.S. application serial number 09/429,643, filed on October 29, 1999, now U.S. Patent No. 7,010,604, issued March 07, 2006. The subject matter of U.S. application serial number 09/429,643, now U.S. Patent No. 7,010,604 which is bodily incorporated herein, derives from provisional U.S. application numbers 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999), both now abandoned. The present application is also related to U.S. application serial number 09/558,209, filed April 26, 2000, now abandoned, and which is incorporated by reference herein.

Amendments to the claims:

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

1.-3. (Cancelled)

4. (New) A system for providing a domain name service for establishing a secure communication link, the system comprising:

a domain name service system configured and arranged to be connected to a communication network, store a plurality of domain names and corresponding network addresses, receive a query for a network address, and indicate in response to the query whether the domain name service system supports establishing a secure communication link.

5. (New) The system of claim 4, wherein at least one of the plurality of domain names comprises a top-level domain name.

6. (New) The system of claim 5, wherein the top-level domain name is a non-standard top-level domain name.

7. (New) The system of claim 6, wherein the non-standard top-level domain name is one of .scom, .sorg, .snet, .sgov, .sedu, .smil and .sint.

8. (New) The system of claim 5, wherein the domain name service system is configured to authenticate the query using a cryptographic technique.

9. (New) The system of claim 4, wherein the communication network includes the Internet.

10. (New) The system of claim 4, wherein the domain name service system comprises an edge router.

11. (New) The system of claim 4, wherein the domain name service system is connectable to a virtual private network through the communication network.

12. (New) The system of claim 11, wherein the virtual private network is one of a plurality of secure communication links in a hierarchy of secure communication links.

13. (New) The system of claim 11, wherein the virtual private network is based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence.

14. (New) The system of claim 11, wherein the virtual private network is based on a network address hopping regime that is used to pseudorandomly change network addresses in packets transmitted between a first device and a second device.

15. (New) The system of claim 11, wherein the virtual private network is based on comparing a value in each data packet transmitted between a first device and a second device to a moving window of valid values.

16. (New) The system of claim 11, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device.

17. (New) The system of claim 4, wherein the domain name service system is configured to respond to the query for the network address.

18. (New) The system of claim 4, wherein the domain name service system is configured to provide, in response to the query, the network address corresponding to a domain name from the plurality of domain names and the corresponding network addresses.

19. (New) The system of claim 4, wherein the domain name service system is configured to receive the query initiated from a first location, the query requesting the network address associated with a domain name, wherein the domain name service system is configured to provide the network address associated with a second location, and wherein the domain name service system is configured to support establishing a secure communication link between the first location and the second location.

20. (New) The system of claim 4, wherein the domain name service system is

connected to a communication network, stores a plurality of domain names and corresponding network addresses, and comprises an indication that the domain name service system supports establishing a secure communication link.

21. (New) The system of claim 4, wherein at least one of the plurality of domain names is reserved for secure communication links.

22. (New) The system of claim 4, wherein the domain name service system comprises a server.

23. (New) The system of claim 22, wherein the domain name service system further comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses.

24. (New) The system of claim 4, wherein the domain name service system comprises a server, wherein the server comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses.

25. (New) The system of claim 4, wherein the domain name service system is configured to store the corresponding network addresses for use in establishing secure communication links.

26. (New) The system of claim 4, wherein the domain name service system is configured to authenticate the query for the network address.

27. (New) The system of claim 4, wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.

28. (New) The system of claim 4, wherein at least one of the plurality of domain names comprises a secure name.

29. (New) The system of claim 4, wherein at least one of the plurality of domain names enables establishment of a secure communication link.

30. (New) The system of claim 4, wherein the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location.

31. (New) The system of claim 4, wherein the secure communication link uses encryption.

32. (New) The system of claim 4, wherein the secure communication link is capable of supporting a plurality of services.

33. (New) The system of claim 32, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

34. (New) The system of claim 33, wherein the plurality of application programs comprises items selected from a group consisting of the following: video conferencing, e-mail, a word processing program, and telephony.

35. (New) The system of claim 32, wherein the plurality of services comprises audio, video, or a combination thereof.

36. (New) The system of claim 4, wherein the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location.

37. (New) The system of claim 36, wherein the query is initiated from the first location, wherein the second location comprises a computer, and wherein the network address is an address associated with the computer.

38. (New) The system of claim 4, wherein the domain name service system comprises a domain name database connected to a communication network and storing a plurality of domain names and corresponding network addresses for communication, wherein the domain name database is configured so as to provide a network address corresponding to a domain name in response to a query in order to establish a secure communication link.

39. (New) A machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for: connecting the domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and indicating in response to the query whether the domain name service system supports establishing a secure communication link.

40. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for storing the plurality of domain names and corresponding network addresses including at least one top-level domain name.

41. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for responding to the query for the network address.

42. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for providing, in response to the query, the network address corresponding to a domain name from the plurality of domain names and the corresponding network addresses.

43. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for receiving the query for a network address associated with a domain name and initiated from a first location, and providing a network address associated with a second location, and establishing a secure communication link between the first location and the second location.

44. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for indicating that the domain name service system supports the establishment of a secure communication link.

45. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for reserving at least one of the plurality of domain names for secure communication links.

46. (New) The machine-readable medium of claim 39, wherein the code resides on a server.

47. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for storing a plurality of domain names and corresponding network addresses so as to define a domain name database.

48. (New) The machine-readable medium of claim 39, wherein the code resides on a server, and the instructions comprise code for creating a domain name database configured to store the plurality of domain names and the corresponding network addresses.

49. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for storing the corresponding network addresses for use in establishing secure communication links.

50. (New) The machine-readable medium of claim 39, wherein the instructions comprise code for authenticating the query for the network address.

51. (New) The machine-readable medium of claim 39, wherein at least one of the plurality of domain names includes an indication that the domain name service system supports the establishment of a secure communication link.

52. (New) The machine-readable medium of claim 39, wherein at least one of the plurality of domain names includes a secure name.

53. (New) The machine-readable medium of claim 39, wherein at least one of the plurality of domain names is configured so as to enable establishment of a secure communication link.

54. (New) The machine-readable medium of claim 39, wherein the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location.

55. (New) The machine-readable medium of claim 39, wherein the secure communication link uses encryption.

56. (New) The machine-readable medium of claim 39, wherein the secure communication link is capable of supporting a plurality of services.

57. (New) The machine-readable medium of claim 56, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

58. (New) The machine-readable medium of claim 57, wherein the plurality of application programs comprises items selected from a group consisting of the following: video conferencing, e-mail, a word processing program, and telephony.

59. (New) The machine-readable medium of claim 56, wherein the plurality of services comprises audio, video, or a combination thereof.

60. (New) The machine-readable medium of claim 39, wherein the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location.

61. (New) The machine-readable medium of claim 60, wherein the instructions include code for receiving a query initiated from the first location, wherein the second location comprises a computer, and wherein the network address is an address associated with the computer.

62. (New) The machine-readable medium of claim 39, wherein the domain name service system comprises a domain name database connected to a communication network and storing a plurality of domain names and corresponding network addresses for communication, wherein the domain name database is configured so as to provide a network address corresponding to a domain name is response to the query in order to establish a secure communication link.

63. (New) A method of providing a domain name service for establishing a secure communication link, the method comprising: connecting a domain name service system to a communication network, ; storing a plurality of domain names and corresponding network addresses; and upon receiving a query for a network address for communication, indicating whether the domain name service system supports establishing a secure communication link.

REMARKS

Claims 4-63 remain in the application. Claims 1-3 have been cancelled, subject to refilling those claims in a continuation application of the present application. Claims 4-63 have been added by this amendment. The Examiner's attention is directed to the parent application, Applicant's patent, U.S. Patent No. 7,418,504 (the "'504 Patent"). Pending claims 4-63 are similar to claims 1-59 of the '504 Patent, except that they have been modified to add the limitation in independent claim 4 (and similar limitations to claims 39 and 63) that there is an indication in response to a query whether the domain name service system supports establishing a secure communication link. New claim 19 (corresponding to claim 16 of the '504 Patent) has also been amended with minor changes.

In the Official action of March 19, 2010, the Examiner has objected to the disclosure because the first paragraph of the specification needs to be updated. The Examiner has also indicated that the information disclosure statement filed May 19, 2009 fails to comply with 37 C.F.R. § 1.98(a)(3) because it does not include a concise explanation of the relevance of each of the cited references. Claims 1 has been rejected under 35 U.S.C. §112, second paragraph, as indefinite, while claims 2-3 have been rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps. Claim 2 has also been rejected under 35 U.S.C. §112, first paragraph, because one skilled in the art clearly would not know how to use the claimed invention. Claims 1-3 have been rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,418,504 (from which the current applications claims priority). Finally claims 1-3 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Shrader (US Patent No 5,864,666). The objections and rejections are traversed and reconsideration is respectfully requested in view of the foregoing amendments and following remarks.

Regarding the Examiner's objection to the specification, the Examiner has requested that applicants indicate the current status of the applications identified in paragraph [0001]. Applicants accordingly have amended paragraph [0001] to comply with the Examiner's request. Accordingly, the objection should be withdrawn.

The Examiner has indicated that the information disclosure statement filed May 19, 2009

fails to comply with 37 C.F.R. § 1.98(a)(3) because it does not include a concise explanation of the relevance. As stated in applicants' document:

> All of the documents herein submitted have been produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas. Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application.

While applicants' regret the large number of documents cited in the litigation by the opposing party, the inability to review the documents, and therefore the inability to assess the materiality of the references, nevertheless applicants felt compelled to cite the references in the file history of the present application, because the two patents in the cited litigation (US Patent Nos. 6,502,135 B1 and 7,188,180 B2) and that of the present application all relate to secure communications. The present application claims priority from a chain of applications, including the one that issued as U.S. Patent No. 6,502,135. U.S. Patent No. 7,188,180 claims priority from a chain of applications, including the same one that issued as U.S. Patent No. 6,502, 135. Accordingly, the applicants request that the Examiner reconsider his position, and review and enter the information disclosure statement of May 19, 2010.

Regarding the rejection of Claims 1 has been rejected under 35 U.S.C. §112, second paragraph, as indefinite, the Examiner states that "it is unclear from where a query is sent", "it is unclear from where the query message is requesting a secure computer network address," "it is unclear how a portal authenticates a query," and finally "the interrelationship or interfunction between a portal and a domain name database is unclear." It is submitted that these cited limitations do not make the claims indefinite. The source of the query message can be from any source in communication with the system for providing a domain name service. As recited in new claim 4, the domain name service system is configured and arranged to be (1) connected to a communication network, (2) store a plurality of domain names and corresponding network addresses, (3) receive a query for a network address, and (4) indicate in response to the query whether the domain name service system supports establishing a secure communication link. All four limitations are required by the claim.

The Examiner also finds fault since there is no express recitation of the interrelationship between the portal and domain database. While the applicants disagree with this rejection, none of the currently presented claims include the limitation of "the portal." Accordingly, this objection is believed to be overcome.

The Examiner also believed that original claims 2-3 were incomplete for "omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections." Claims 4-63 recite adequate limitations to satisfy the statutory requirements of 35 U.S.C. §112.

Claim 4 recites the restrictive limitations of a domain name service system required to be "configured and arranged to be connected to a communication network, store a plurality of domain names and corresponding network addresses, receive a query for a network address, and indicate in response to the query whether the domain name service system supports establishing a secure communication link."

Claim 39 recites "a machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for: connecting the domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and indicating in response to the query whether the domain name service system supports establishing a secure communication link." This clearly provides limitations acceptable under 35 U.S.C. §112.

Finally, claim 63 recites "a method of providing a domain name service for establishing a secure communication link, the method comprising: connecting a domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; and upon receiving a query for a network address for communication, indicating whether the domain name service system supports establishing a secure communication link." Claim 63 recites method steps that clearly recite method limitations within the requirements of 35 U.S.C. §112.

Finally, original claim 2 was also rejected under 35 U.S.C. §112, first paragraph, is not supported by an "undue breadth … asserted utility or a well established utility." Applicants

disagree. New claim 4 recites that the system provides "a domain name service for establishing a secure communication link." New claim 39 recites a "machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for connecting the domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and indicating in response to the query whether the domain name service system supports establishing a secure communication link."

Claims 1-3 have been rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,418,504 (from which the current applications claims priority). Applicants agree to submit a terminal disclaimer should the Examiner maintain this rejection against new claims 4-63.

Finally claims 1-3 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Shrader (US Patent No 5,864,666). The latter patent describes a system for administering tunneling on a firewall computer between a secure computer network and a nonsecure computer network (col. 1, lines 40 and 41). The system includes a user interface. The user interface is presented having a first pane in which a tunnel definition can be entered. A query is run on an entered tunnel definition to determine whether any existing tunnel definitions match the entered tunnel definition. The results of the query are then displayed on a scatter bar in another pane in the user interface. Locations of matching tunnel definitions are then indicated by lines through the scatter bar. A small bar is displayed proximate to the scatter bar. The small bar indicates the position of the displayed list of tunnel definitions relative to a complete list of tunnel definitions represented by the scatter bar. At this point, an action may be performed on a selected definition. (col. 1., lines 53-65).

The patent reference also describes the use of an Internet firewall product that allows administrators to create a physical firewall between a secure network and an unsecured network. The firewall product is described as providing a number of functions including "specialized domain name services." (col. 2, lines 11-18). However "IP tunneling is a feature provided by internet firewalls which is the primary subject of the present invention."

The "IP Tunnel Query Page" is shown in detail in Figs. 6 and 7, and is described in

detail in col. 7, line 34-col. 10, line 46. Clearly the page is used by a human administrator to determine tunnel definitions.

The reference thus describes a system to allow a human network administrator to administer tunneling on a firewall computer between a secure computer network and a nonsecure computer network. The system includes an interface that provides graphical depictions of tunnels between addresses in the networks as lines connecting icons representing network addresses. The system allows the user to display a selected tunnel definition in response to the user input. The only apparent query that the system responds to is a "query on an entered tunnel definition to determine whether any existing tunnel definitions match the entered tunnel definition." Clearly the system of Shrader does not provide a domain name service system "configured and arranged to be connected to a communication network, store a plurality of domain names and corresponding network addresses, receive a query for a network address, and indicate in response to the query whether the domain name service system supports establishing a secure communication link", as recited in applicants' claim 4, nor a "machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for: connecting the domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and indicating in response to the query whether the domain name service system supports establishing a secure communication link," as recited in applicants claim 39, nor a "method of providing a domain name service for establishing a secure communication link, the method comprising: connecting a domain name service system to a communication network, ; storing a plurality of domain names and corresponding network addresses; and upon receiving a query for a network address for communication, indicating whether the domain name service system supports establishing a secure communication link," as recited in applicants' claim 63.

In summary therefore, the remaining claims 4-63, the remaining claims in the application, are believed to be in condition for allowance. An early and favorable action thereon is therefore earnestly solicited.

The Examiner is invited to call the undersigned agent if there are any questions.

To the extent necessary, a petition for a one month extension of time under 37 C.F.R.

1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer
Registration No. 26,418

28 State Street
Boston, MA 02109
Phone: 617.535.4065
Facsimile: 617.535.3800
E-mail address: tkusmer@mwe.com

Please recognize our Customer No. 23,630 as our correspondence address.

Date: June 28, 2010

Electronic Patent Application Fee Transmittal

Application Number:	11840560
Filing Date:	17-Aug-2007
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	43	52	2236
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	1251	1	130	130
Miscellaneous:				
		Total in USD ($)		**2366**

Electronic Acknowledgement Receipt	
EFS ID:	7907919
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	28-JUN-2010
Filing Date:	17-AUG-2007
Time Stamp:	17:02:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2366
RAM confirmation Number	3951
Deposit Account	501133
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees) Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AmendA.pdf	62014 d13a86bf188224a7964be0a28e8cbec6ee25774f	yes	15

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	9
Applicant Arguments/Remarks Made in an Amendment	10	15

Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	32493 3c32ce143ac314ff8062b7696dd724072838eb7c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	94507		

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.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	11/840,560
				Filing Date	08-17-2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0063

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed before the receipt of a first office action.

[ ] Items contained in this Information Disclosure Statement were first cited in any communication from a foreign patent office in a counterpart foreign application.

[ ] No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, 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 this Information Disclosure Statement

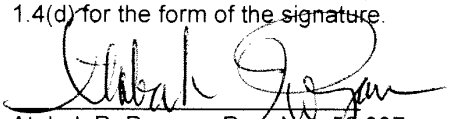
[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] 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.



Date: 04/01/2010

Atabak R, Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02108
Tel. (617) 535-4000
Fax (617) 535-3800

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	11/840,560
	Filing Date	08-17-2007
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	077580-0063

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B8	US2007/0266141	11/2007	Norton, Michael Anthony	
	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	

EXAMINER	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.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	11/840,560
	Filing Date	08-17-2007
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	077580-0063

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley T.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	

English Abstract
of Cited Document 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **62-214744**

(43)Date of publication of application : **21.09.1987**

(51)Int.Cl. **H04L 9/00**
H04L 11/20
H04L 11/26

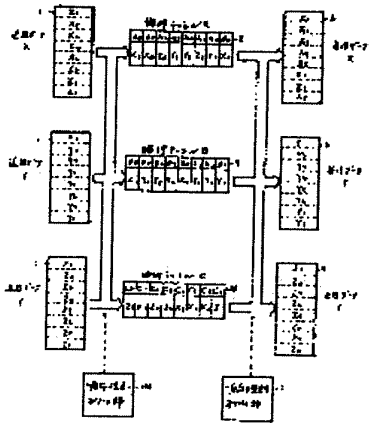
(21)Application number : **61-056812**

(22)Date of filing : **17.03.1986**

(71)Applicant : **HITACHI LTD**

(72)Inventor : **OOYA KAZUAKI**
HIRAGA KATSUHISA

(54) PACKET TRANSMISSION SYSTEM



(57)Abstract:

PURPOSE: To prevent the leakage of data by providing a means controlling the order of packet by a prescribed definition to the reception and transmission side, deciding the logical channel of each packet in the order of sending at the transmission side and restoring the data string of the packet received from each logical channel at the reception side.

CONSTITUTION: Data X, Y, Z to be sent of data 1, 4, 7 are split at each packet, a transmisson order rule control section 10 is used to share the packets into logical channels A, B, C of data 2, 5, 8. In this case, the sent order is changed according to the sequence restriction of the control section 10. Thus, the packet data are sent in the entirely difference order from that of the packet data constituting the original data 1, 4, 7 to be sent. At the reception side, the packet data received from each logical channel (2, 5, 8) is rearranged by a reception side order rule control section 11 to obtain reception data X, Y, Z of data 3, 6, 7. Thus, the leakage of the data from the transmission line and the decoding are prevented.

Cited Document 1 (JP-A (Kokai) S62-214744)

The order of packet data in each logical channel of the present invention is different from those in logical channels 2, 5, and 8 of the conventional packet transmission system as shown in Fig. 5 in that correct information cannot be obtained at the receiver even if the data in one logical channel are aligned sequentially, as indicated by 2, 5, and 8 in Fig. 1. Therefore, at the receiver, it is necessary to realign the data received from each logical channel with reference to the same order rule as that used at the transmitter.

Fig. 2 shows an example of the order rule. When arranged in a table indicated by 12, this order rule forms a matrix in which 24 types of numerals from A1 to C8, configured by the combination of the logical channel numbers of A, B, and C, and the sequence numbers from 1 to 8, correspond to the packet data from X1 to Z8 obtained by dividing the corresponding transmission data X, Y, and Z.

Fig. 3 shows an example of processing at the transmitter. When the data to be transmitted via the logical channel A of 2 are selected from the transmission data X, Y, and Z of 1, 4, and 7, the order rule shown in the table 12 in Fig. 3 is used to send out the packets in the order of X_1, Y_2, Z_2, Y_6, Y_7, and Z_6 to the logical channel A. The same applies to the data to be transmitted via the logical channels B and C of 5 and 8.

Fig. 4 shows an example of processing at the receiver. For example, the data X_1, Y_2, Z_2, Y_6, Y_7, and Z_6 received from the logical channel A indicated by 2 are aligned in each position of the received data X, Y, and Z indicated by 3, 6, and 9 according to the order rule of the logical channel A as shown in table 12 of Fig. 3. The same processing is executed for the other logical channels to restore the received data X, Y, and Z.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－214744

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)9月21日
H 04 L 9/00		B－7240－5K	
11/20	102	A－7117－5K	
11/26		7117－5K	審査請求　未請求　発明の数 1　（全4頁）

⑤④発明の名称　パケット伝送方式

㉑特　願　昭61－56812

㉒出　願　昭61(1986)3月17日

㉒発明者　大家　万明　秦野市堀山下1番地　株式会社日立製作所神奈川工場内

㉒発明者　平賀　勝久　秦野市堀山下1番地　株式会社日立製作所神奈川工場内

㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

パケット伝送方式

2．特許請求の範囲

(1) 送信側と受信側において複数の論理チャネルを使用しデータをパケット分割して伝送するパケット伝送方式において、送信側と受信側にパケットの送信及び受信の順序を予め定めた定義に従って制御する順序規則制御手段を持ち、この順序規則制御手段により、送信側では受信する各パケットの論理チャネル及び送出順序を決定し、受信側では各論理チャネルから受信したパケットのデータ列の復元を行うことを特徴としたパケット伝送方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明はパケット伝送方式に係り、特に伝送内容の秘密を守るため、伝送路上でデータが第3者に漏れ、これが容易に解析されることを防ぐのに好適なパケット伝送方式に関する。

〔従来の技術〕

パケット伝送方式の一つに、送信側と受信側において複数の論理チャネルを使用し、データをパケット分割して伝送する方式がある（ＣＣＩＴＴ，Ｘ．２５勧告）。

第５図に従来のこの種パケット伝送方式を示す。１，４，７は送信しようとするデータＸ，Ｙ，Ｚであり、これをそれぞれパケット分割し、２，５，８の論理チャネルＡ，Ｂ，Ｃを経由して各々のパケットデータを受信側へ送信する。受信側では、各論理チャネルごとに受信したパケットデータをシーケンス番号順に整列させ、３，６，９の受信データＸ，Ｙ，Ｚを得る。

なお、秘密データ伝送に関連する公知文献としては、例えば特開昭６０－５４５４４号公報が挙げられる。

〔発明が解決しようとする問題点〕

従来技術においては、受信側において論理チャネル番号とパケットシーケンス番号により、パケットデータの識別を行うため、データを受信した

側では容易にパケットの解読ができ、データが第3者へ漏洩するという問題があった。

本発明の目的は、伝送しようとするデータの形式を加工することなく、データを構成するパケットをそれぞれ異った仮想的通信路を通して伝送することにより、伝送しようとするデータが伝送路上から漏れ容易に解読されることを防ぐためのパケット伝送方式を提供することにある。

〔問題点を解決するための手段〕

本発明は、伝送しようとするデータを、同一の論理チャネルを通さずに、データを構成する複数のパケットをあらかじめ定めた規則により、いくつかの異った論理チャネルを使用して分割伝送する。あらかじめ定めた規則とは伝送しようとする一定順序のパケットをどの順序でどの仮想的通信路に送出するかを決めた通信路ごとの順序規則を言う。パケットを送信する側では、伝送しようとするデータを構成する一連のパケットを上記規則に従って仮想的通信路に順次送出する。パケットを受信する側では、同様に上記規則に従い、各仮想的通信路より受信したパケットを整列させ元のデータ列を復元する。

〔作　用〕

本発明は、データの漏洩を防止することを目的とし、伝送しようとするパケット列の順序及び伝送路に関してスクランブリングしようとするものである。従来のパケット伝送では、各パケットごとに持つ論理チャネル番号及びシーケンス番号を用いて、送信側と受信側のデータ側の順序制御を行っているため、受信側では受信したパケットデータ列から得られる情報のみで容易に元のデータ列を復元させることが容易である。

本発明においては、送信側と受信側にあらかじめ定義した論理チャネルとシーケンス番号から成る送信及び受信パケットの順序を変換するための順序規則を持ち、この順序情報と各パケットに持つ論理チャネル番号とパケットシーケンス番号を用いて、元のデータ列を復元させる。従って順序規則を持たないものが受信しても解読はできない。

〔実施例〕

以下、本発明の一実施例について図面により説明する。

第1図に本発明のパケット伝送方式を示す。1，4，7の送信しようとするデータX，Y，Zをそれぞれパケット分割し、10の送信側順序規則制御部を用いて、それぞれのパケットを2，5，8の各論理チャネルA，B，Cに振り分ける。この際、送出する順序も制御部10の順序規則に従って変化させる。従って、各論理チャネル2，5，8上には、図示の如く、送出しようとする元のデータ1，4，7を構成するパケットデータとはまったく異った順序で、パケットデータが伝送されることになる。受信側では、2，5，8の各論理チャネルより受信したパケットデータを、11の受信側順序規則制御部により整列し直し、3，6，7の受信データX，Y，Zを得る。

本発明における各論理チャネル上のパケットデータの順序は、第5図に示す従来のパケット伝送方式の論理チャネル2，5，8と異なり、第1図の2，5，8に示す様に1つの論理チャネル内のデータを順に整列させても受信側では正しい情報を得ることができない。従って、受信側では、送信側と同じ順序規則を参照して、各論理チャネルから受信したデータを再度整列させる必要がある。

第2図に順序規則の1例を示す。この順序規則例は、12に示すテーブル形式とした場合、A，B，Cの論理チャネル番号と1から8のシーケンス番号との組み合せによって構成されるA1からC8までの24種類の番号と、これに対応する送信データX，Y，Zを分割したX1からZ8のパケットデータを対応させたマトリックスとなる。

第3図に送信側の処理例を示す。1，4，7の送信データX，Y，Zより、2の論理チャネルA経由で送信するデータを選択する場合、第3図のテーブル12に示した順序規則を用いて、論理チャネルAに対して、X_1，Y_2，Z_3，Y_6，Y_7，Z_8の順序でパケットを送出する。5と8の論理チャネルB、C経由で送信するデータも同様である。

第4図に受信側の処理例を示す。例えば、2に

示す論理チャネルAより受信したデータ、X_1，Y_2，Z_2，Y_6，Y_7，Z_6は、第3図のテーブル12で示した論理チャネルAの順序規則に従い、3，6，9に示される受信データX，Y，Zのそれぞれの位置に整列される。他の論理チャネルについても同様の処理を行い、受信データX，Y，Zを復元させる。

なお、順序規則は、テーブル形式で定義する方式のほかに、計算式で定義する方式が考えられる。

〔発明の効果〕

本発明によれば、あらかじめ定められた順序規則を知っている場合のみ、パケットデータの正しい送受信が行える。従って、順序規則を知らされていない第三者は正しい受信を行うことが出来ず、データの機密を守る上で効果がある。また、本発明においては、複数の論理チャネルを使用するため、各論理チャネルを物理的に別々の回線に分割して配置することが出来、この時には物理的に別々の回線を同時に接続して受信する必要があるため、データの漏洩防止にさらに効果がある。

4．図面の簡単な説明

第1図は本発明のパケット伝送方式を説明する図、第2図は本発明で用いる順序規則の一例を示す図、第3図は本発明による送信側の処理例を示す図、第4図は本発明による受信側の処理例を示す図、第5図は従来のパケット伝送方式を説明する図である。

1，4，7…送信データ、

3，6，9…受信データ、

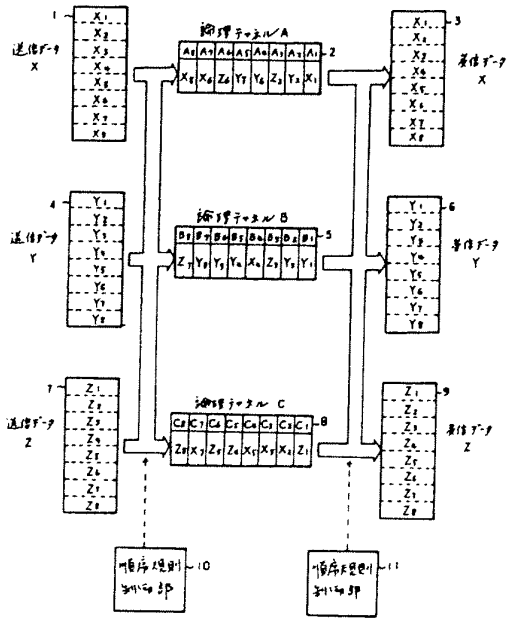
2，5，8…論理チャネル、

10…送信側順序規則制御部、

11…受信側順序規則制御部。

代理人弁理士　小川勝男

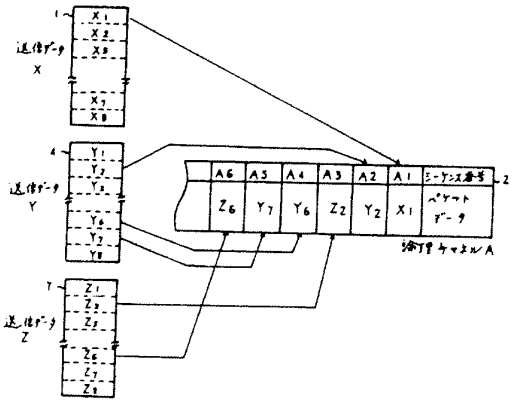
第1図



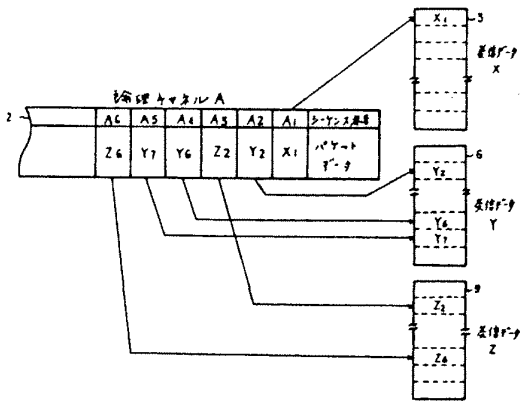
第2図

シーケンス番号 / 論理チャネル	1	2	3	4	5	6	7	8
A	X_1	Y_2	Z_2	Y_6	Y_7	Z_6	X_6	X_8
B	Y_1	Y_3	Z_3	X_4	Y_4	Y_5	Y_8	Z_7
C	Z_1	X_2	X_3	X_5	Z_4	Z_5	X_7	Z_8

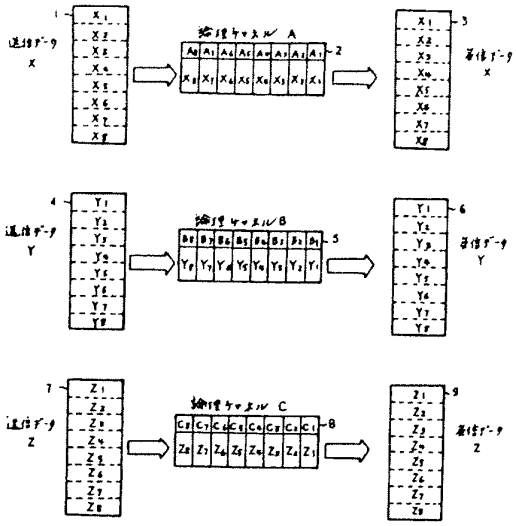
第3図



第 4 図



第 5 図



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-070531**

(43)Date of publication of application : **10.03.1998**

(51)Int.Cl. **H04L 12/22**
G06F 13/00
H04K 1/00

(21)Application number : **08-223898**

(22)Date of filing : **26.08.1996**

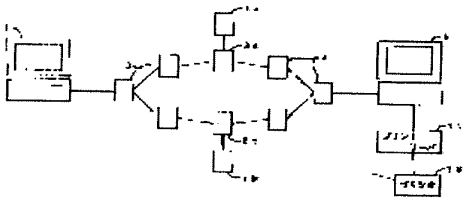
(71)Applicant : **BROTHER IND LTD**

(72)Inventor : **SUZUKI MASASHI**
MATSUDA KAZUHIKO
SAGOU AKIRA
KONDO HIROMOTO
YASUI TSUNEO

(54) DATA COMMUNICATION SYSTEM AND RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data communication system capable of satisfactorily preventing the leakage of data to be communicated.



SOLUTION: A personal computer 1 bi-sects data to be transmitted, adds transmission source data and transmission time data to the respective bisected data and transmits respective data to different servers 7a and 7b through different communication routes. Then the respective servers 7a and 7b transmit each received data to a server 5 through the communication route. The server 5 judges whether or not the transmission source data and transmission time data of the received data is matched with those of the already received data, and at the time they are matched, the received data is combined with the already received to obtain data before bisecting.

CLAIMS

[Claim(s)]

[Claim 1]A data communication system provided with a sending set characterized by comprising the following which transmits data, and a receiving set which receives the above-mentioned data transmitted from this sending set.

A data dividing means into which it has two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and the above-mentioned sending set divides the above-mentioned data at plurality.

An identification data grant means to give identification data which matches the data with each data divided in this data dividing means mutually.

A data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation.

A data-coupling means to combine the data which have and have identification data in which the above-mentioned receiving set corresponds mutually among each data received in a data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[Claim 2]The data communication system according to claim 1, wherein the above-mentioned identification data contains transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[Claim 3]The data communication system according to claim 1 or 2, wherein the above-mentioned identification data contains a serial number which has numerals common to at least a part.

[Claim 4]A receiving set comprising:

A data receiving means which receives data separately via mutually different repeating

installation.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received from each data received in this data receiving means in an identification data extraction means to extract predetermined identification data, and the above-mentioned data receiving means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the data communication system provided with the sending set which transmits data, and the receiving set which receives the data transmitted from the sending set, and a receiving set applicable to the data communication system.

[0002]

[Description of the Prior Art]Conventionally, in this kind of data communication system, receiving the data which transmitted data from the sending set via the telephone line and the cable, and was transmitted from that sending set with a receiving set is performed. Performing such data communications through the Internet is also considered in recent years.

[0003]

[Problem(s) to be Solved by the Invention]However, in this kind of data communication system, since the whole data was transmitted and received via a telephone line, a cable, etc., the data which spreads a telephone line, a cable, etc. may have been monitored by the 3rd person. For this reason, it was difficult to prevent disclosure of the data which communicates. Especially the Internet was easy to access and it was much more difficult to prevent disclosure of data.

[0004]Then, the invention according to claim 3 was made [that especially the invention according to claim 2 simplifies composition further for the purpose of the invention according to claim 1 to 3 providing the data communication system which can prevent disclosure of the data which communicates good, and] for the purpose of performing the reconstitution of data much more correctly. The invention according to claim 4 was made for the purpose of providing a receiving set applicable to the data communication system.

[0005]

[The means for solving a technical problem and an effect of the invention] The invention according to claim 1 made since the above-mentioned purpose was attained, In the data communication system provided with the sending set which transmits data, and the receiving set which receives the above-mentioned data transmitted from this sending set, Have two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and. The data dividing means to which the above-mentioned sending set divides the above-mentioned data into plurality, and an identification data grant means to give the identification data in which the data is mutually matched with each data in which it was divided in this data dividing means, The data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation, It **** and is characterized by having a data-coupling means to combine the data which have identification data in which the above-mentioned receiving set corresponds mutually among each data received in the data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[0006]In this invention constituted in this way, a sending set divides data into plurality by a data dividing means, and gives the identification data which matches data with the data of each which was divided mutually by an identification data grant means. A sending set transmits each data in which the above-mentioned identification data was given to mutually different repeating installation by a data sending means. Then, each repeating installation relays each data separately via a mutually different communication path, and a receiving set receives each above-mentioned data separately from each repeating installation by a data receiving means. Then, a receiving set combines the data which have identification data mutually corresponding among each received data by a data-coupling means.

[0007]For this reason, data combined by a data-coupling means of a receiving set is in agreement with data before division by a data dividing means of a sending set. That is, it means that data before division was transmitted even to a receiving set. Data by which each above-mentioned communication path is spread via repeating installation is data after division by ******** and a data dividing means. For this reason, even if data by which a communication path is spread is monitored, that data will not be in agreement with data before division.

[0008]Therefore, in this invention, disclosure of data which communicates can be prevented good. As a communication path, a telephone line, the Internet besides a cable,

etc. are applicable, and also when it is any, disclosure of data can be prevented good. In addition to the composition according to claim 1, the invention according to claim 2 is characterized by the above-mentioned identification data containing transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[0009]That is, data after the above-mentioned division is usually transmitted to the almost same time (a difference is less than 1 minute) from the same sending set. So, in this invention, transmission source data which expresses common transmitting origin to the above-mentioned identification data, and transmission time data showing having been mostly transmitted to identical time are included. For this reason, in a receiving set, data can be combined easily and it can restore. A common sending set is also equipped with a function which gives transmission source data and transmission time data in many cases. Therefore, when this invention is applied to such a sending set, even if it does not provide composition special as an identification data grant means, the above-mentioned sending set can be realized.

[0010]Therefore, in addition to the effect according to claim 1, in this invention, an effect that it can simplify further produces composition of a sending set. The invention according to claim 3 is characterized by the above-mentioned identification data containing a serial number which has numerals common to at least a part in addition to the composition according to claim 1 or 2.

[0011]In this invention constituted in this way, data after division is matched using a serial number which has common numerals at least in part. For this reason, the data after division can be matched very correctly. For example, when each data after division is long and transmission time of each data shifts substantially, each data can be matched good.

[0012]Therefore, in addition to the effect of the invention according to claim 1 or 2, in this invention, an effect that it can restore much more correctly produces data after division. The receiving set according to claim 4 is provided with the following.

A data receiving means which receives data separately via mutually different repeating installation.

An identification data extraction means to extract predetermined identification data from each data received in this data receiving means.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received in the above-mentioned data receiving means.

[0013]With this invention constituted in this way, a data receiving means receives data separately via mutually different repeating installation, and an identification data extraction means extracts predetermined identification data from each received data. Then, a data-coupling means combines the data which have identification data mutually corresponding among data received in a data receiving means.
[0014]For this reason, this invention is applicable good as a receiving set in the data communication system according to any one of claims 1 to 3. the above-mentioned identification data may contain transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time, may contain a serial number which boils a part at least and has common numerals, and may be a thing of other gestalten.
[0015]
[Embodiment of the Invention]Next, an embodiment of the invention is described with a drawing. Drawing 1 is an outline lineblock diagram showing the data communication system which applied this invention. This embodiment applies this invention to the network print system using the Internet.
[0016]As shown in drawing 1, the personal computer (henceforth a personal computer) 1 of the users as a sending set is connected to the server 5 as a receiving set by the side of a print service station via the Internet which connects many providers 3. For this reason, if data is transmitted towards the server 5 from the personal computer 1, that data will be spread via [the adjoining provider 3] one by one. The data which communicates the Internet top is once memorized to the two providers 3a and 3b who exist on a different communication path, and the servers 7a and 7b as repeating installation which changes an address (address of a transmission destination) and transmits are connected to them.
[0017]The personal computer 1 and the servers 5, 7a, and 7b are all the computers of the common knowledge provided with the external memory or the modem for communication besides CPU, ROM, and RAM, and the printer 13 is further connected to the server 5 via the print server 11. This system is for transmitting image data etc. to the server 5 of a print service station (printer) from users' (customer) personal computer 1, and performing image formation with the printer 13. The servers 5, 7a, and 7b may be FTP (file transfer protocol) servers, or may be mail servers.
[0018]Next, processing of the personal computer 1 in this system and the servers 5, 7a, and 7b is explained using drawing 2 - the flow chart of four. Users' personal computer 1 will perform processing of drawing 2, if transmission of data is directed via the keyboard etc. which are not illustrated. If processing is started as shown in drawing 2,

the data first transmitted in S1 will be read, and the data will be divided into two by S3 continuing. The 1st data after division is transmitted to the 1st address corresponding to the server 7a, by S7, the 2nd data after division is transmitted to the 2nd address corresponding to the server 7b, and processing is ended S5 continuing. In transmission of the data in S5 and S7, the transmission source data showing the address of the personal computer 1 which is a transmitting agency, and the transmission time data showing the transmission time are given to the data to transmit. Since this processing is common knowledge, it is not explained in full detail here. It is good also considering which of the data after division as the 1st at S5 and S7.

[0019]On the other hand, the server 7a carries out repeat execution of the processing shown in drawing 3. The server 7b also carries out repeat execution of the same processing. As shown in drawing 3, when processing was started, and it judges whether data was received or not and receives in S11 (S11:YES), it shifts to S13. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S13, the received data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), it stands by in S11 as it is.

[0020]For this reason, if the data after the personal computer 1 dividing is transmitted to the servers 7a and 7b by processing of drawing 2 (S5, S7), by processing of drawing 3, the servers 7a and 7b will receive each data after division separately (S11;YES), and will transmit that data to the server 5 (S13). That is, the data after division is transmitted to the server 5 via a different communication path.

[0021]Next, drawing 4 is a flow chart showing the processing in which the server 5 carries out repeat execution. If processing is started, when it judges whether data was received or not and receives in S21 (S21:YES), it will shift to S23. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S23, the transmission source data given to the data judges whether a match has a match, i.e., the address of a transmitting agency, in the data which already receives and is stored in the memory. The data whose transmission time which shifts to S25 and transmission time data expresses in the already received data if there are data received in S21 and data whose address of a transmitting agency corresponds (S23:YES) corresponds mostly judges whether it is in it.

[0022]When an affirmative judgment is carried out by S25, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 2, and S7. Then, the data after combination is sent to the print server 11 in S29 which combines two data in S27 and

continues in this case (S25:YES), and it returns to S21. Then, image formation with the printer 13 is performed based on the data after combination, i.e., the data read in S1 of drawing 2. On the other hand, when a negative judgment is carried out by SS21, S23, or 25, nothing is done but it returns to S21 as it is.

[0023]Thus, in this system, it can restore by the server 5 and image formation of the data transmitted via a communication path which divides with the personal computer 1 and is different can be carried out with the printer 13. The data spread via each provider 3 is data after division, respectively. For this reason, even if the data spread via each provider 3 is monitored, that data will not be in agreement with the data before division. Therefore, in this system, disclosure of the data which communicates can be prevented good. In this system, the data which should be combined in S27 is identified with transmission source data and transmission time data. The common personal computer is also equipped with the function which gives transmission source data and transmission time data in many cases. In this system, since such a general function is used, processing can be simplified further.

[0024]Next, other embodiments of this invention are described using drawing 5 - the flow chart of seven. In this embodiment, since only processing of each part differs from the above-mentioned embodiment, the numerals used by drawing 2 are used as it is. In drawing 5 -7, the same numerals are given to drawing 2 - the same processing as four, and detailed explanation of processing is omitted to them.

[0025]Drawing 5 is a flow chart showing the processing which the personal computer 1 performs, when transmission of data is directed. After reading the data to transmit (S1) and dividing the data into two if processing is started as shown in drawing 5 (S3), it shifts to S31. In S31, a serial number is generated using a random number etc. from current time. As a serial number, the thing containing numerals other than numbers, such as the alphabet, may be adopted. In S33 continuing, "1" of the serial number and a number is given to the 1st data, and "2" of the above-mentioned serial number and a number is given to the 2nd data in S35. Then, each data after the division to which the serial number etc. were given is transmitted to the 1st and 2nd addresses (it corresponds to the servers 7a and 7b), and processing is ended (S5, S7).

[0026]Drawing 6 is a flow chart showing the processing in which the servers 7a and 7b carry out repeat execution. If data is received (S11:YES), it will shift to S41, and it is judged whether the serial number is given to the data. When given (S41:YES), it shifts to S13, and data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), and when the serial number is not given (S41:NO), it shifts to S11 as it is. That is, since it is not the data transmitted

by S5 of drawing 5, and S7 when the serial number is not given, other routines which are not illustrated perform the usual processing as the servers 7a and 7b.

[0027]Drawing 7 is a flow chart showing the processing in which the server 5 carries out repeat execution. In this processing, if data is received (S21:YES), it will shift to S51, and it is judged whether the serial number is given to that data. It is judged whether there are what was given to the data, and a thing which has the same serial number in the data which shifts to S53 when given (S51:YES), already receives, and is stored in the memory.

[0028]When an affirmative judgment is carried out by S53, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 5, and S7. Then, two data is combined in this case (S27), and it sends to the print server 11 (S29). Then, image formation with the printer 13 is performed based on the data after combination. On the other hand, when a negative judgment is carried out by SS21, S51, or 53, nothing is done but it returns to S21 as it is.

[0029]When this embodiment also divides data and makes a different communication path spread like the above-mentioned embodiment, disclosure of data can be prevented good. In this system, the data after division is matched using the serial number. For this reason, data can be restored much more correctly. For example, when each data after division is long and the transmission time of each data shifts substantially (i.e., when S5 of drawing 5 and the interval of S7 become large etc.), each data is matched good. When there is no serial number in data (S41:NO), the servers 7a and 7b perform the usual processing. For this reason, it is not necessary to extend the servers 7a and 7b for the above-mentioned processing.

[0030]The processing which gives the transmission source data and transmission time data in S5 and S7 in each above-mentioned embodiment, And in processing of S33 and S35, processing of S3 for an identification data grant means to a data dividing means. In transmitting processing of the data in S5 and S7, processing of S21 to a data sending means to a data receiving means. The processing which extracts transmission source data [in / to a data-coupling means / in processing of S27 / S23, S25, S51, and S53], transmission time data, or a serial number is equivalent to an identification data extraction means, respectively.

[0031]This invention is not limited to the above-mentioned embodiment at all, and can be carried out with various gestalten in the range which does not deviate from the gist of this invention. For example, this invention is applicable to the data communication system using various communication paths, such as a telephone line, a cable, radio

besides using the Internet a data communication system. However, the Internet is very easy to access. Therefore, when it applies to the data communication system using the Internet like the above-mentioned embodiment, the effect of the leakage control of the data based on this invention becomes much more remarkable.

[0032]Although this invention is applied to the server 5 of a receiver in the above-mentioned embodiment to the network print system which connected the printer 13, in addition to this, this invention is applicable to various data communication systems. For example, it is applicable also to the system which only transmits and receives data. In this case, what is necessary is just to omit processing (drawing 4, drawing 7) of the five serverS29.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is an outline lineblock diagram showing the data communication system which applied this invention.

[Drawing 2]It is a flow chart showing processing of the transmitting side personal computer of the system.

[Drawing 3]It is a flow chart showing processing of the server for relay of the system.

[Drawing 4]It is a flow chart showing processing of the receiver server of the system.

[Drawing 5]It is a flow chart showing other gestalten of processing of the above-mentioned transmitting side personal computer.

[Drawing 6]It is a flow chart showing other gestalten of processing of the above-mentioned server for relay.

[Drawing 7]It is a flow chart showing other gestalten of processing of the above-mentioned receiver server.

[Description of Notations]

1 -- Personal computer 3 -- Provider 5, 7a, 7b -- Server

11 -- Print server 13 -- Printer

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－70531

(43)公開日　平成10年(1998) 3月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/22		9744－5Ｋ	Ｈ０４Ｌ	11/26	
Ｇ０６Ｆ　13/00	３５１		Ｇ０６Ｆ	13/00	３５１Ａ
Ｈ０４Ｋ　1/00			Ｈ０４Ｋ	1/00	Ｚ

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平8－223898

(22)出願日　平成８年(1996) ８月26日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

(72)発明者　鈴木　正史
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　松田　和彦
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　佐郷　朗
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(74)代理人　弁理士　足立　勉

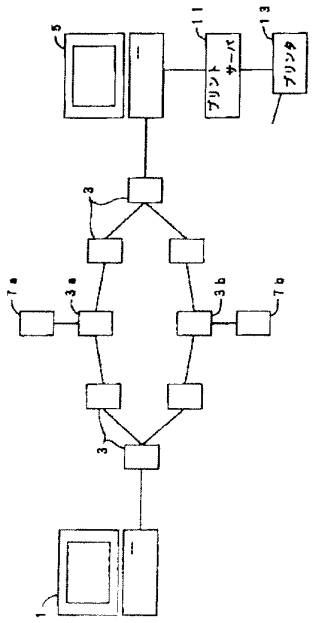
最終頁に続く

(54)【発明の名称】　データ通信システムおよび受信装置

(57)【要約】

【課題】　通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することである。

【解決手段】　パソコン１によって、送信するデータを二つに分割し、その分割した各データにそれぞれ送信元データや送信時刻データを付して、その各データを異なる通信経路を介して別々のサーバ７ａ，７ｂに送信する。そして、各サーバ７ａ，７ｂは、受信した各データを異なる通信経路を介してサーバ５に送信する。サーバ５は、受信したデータと、既に受信しているデータとについて、前記送信元データや送信時刻データが一致するか否かを判断し、一致した場合は前記受信したデータと既に受信しているデータとを結合して分割前のデータにさせる。



1

【特許請求の範囲】
【請求項１】　データを送信する送信装置と、
該送信装置から送信された上記データを受信する受信装置と、
を備えたデータ通信システムにおいて、
上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、
上記送信装置が、
上記データを複数に分割するデータ分割手段と、
該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、
上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、
を有し、
上記受信装置が、
上記各中継装置から個々にデータを受信するデータ受信手段と、
該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、
を有することを特徴とするデータ通信システム。
【請求項２】　上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴とする請求項１記載のデータ通信システム。
【請求項３】　上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴とする請求項１または２記載のデータ通信システム。
【請求項４】　互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、
該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、
上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、
を備えたことを特徴とする受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを送信する送信装置と、その送信装置から送信されたデータを受信する受信装置とを備えたデータ通信システム、およびそのデータ通信システムに適用可能な受信装置に関する。
【０００２】
【従来の技術】従来、この種のデータ通信システムでは、電話回線やケーブルを介して送信装置からデータを送信し、その送信装置から送信されたデータを受信装置にて受信することが行われている。また、近年、インターネットを通じてこのようなデータ通信を行うことも考

2

えられている。
【０００３】
【発明が解決しようとする課題】ところが、この種のデータ通信システムでは、電話回線やケーブル等を介してデータ全体が送受信されるので、電話回線やケーブル等を伝搬するデータが第３者によって傍受される可能性があった。このため、通信されるデータの漏洩を防止するのが困難であった。特に、インターネットはアクセスが容易であり、データの漏洩を防止することが一層困難であった。
【０００４】そこで、請求項１～３記載の発明は、通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することを目的とし、特に、請求項２記載の発明は構成を一層簡略化することを、請求項３記載の発明はデータの復元を一層正確に行うことを目的としてなされた。また、請求項４記載の発明は、そのデータ通信システムに適用可能な受信装置を提供することを目的としてなされた。
【０００５】
【課題を解決するための手段および発明の効果】上記目的を達するためになされた請求項１記載の発明は、データを送信する送信装置と、該送信装置から送信された上記データを受信する受信装置と、を備えたデータ通信システムにおいて、上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、上記送信装置が、上記データを複数に分割するデータ分割手段と、該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、を有し、上記受信装置が、上記各中継装置から個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、を有することを特徴としている。
【０００６】このように構成された本発明では、送信装置は、データ分割手段によりデータを複数に分割し、その分割された個々のデータに、データ同士を互いに対応付ける識別データを、識別データ付与手段によって付与する。更に、送信装置は、データ送信手段により、上記識別データが付与された各データを互いに異なる中継装置に送信する。すると、各中継装置は、各データを互いに異なる通信経路を介して個々に中継し、受信装置は、データ受信手段により、上記各データを各中継装置から個々に受信する。続いて、受信装置は、データ結合手段により、受信した各データの内、互いに対応する識別データを有するデータ同士を結合する。
【０００７】このため、受信装置のデータ結合手段により結合されたデータは、送信装置のデータ分割手段によ

る分割前のデータと一致する。すなわち、分割前のデータが受信装置まで送信されたことになる。また、中継装置を介して上記各通信経路を伝搬されるデータは、ぞれぞれ、データ分割手段による分割後のデータである。このため、通信経路を伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。

【０００８】従って、本発明では、通信されるデータの漏洩を良好に防止することができる。なお、通信経路としては、電話回線やケーブルの他、インターネット等も適用することができ、いずれの場合もデータの漏洩を良好に防止することができる。請求項２記載の発明は、請求項１記載の構成に加え、上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴としている。

【０００９】すなわち、上記分割後のデータは、通常、同じ送信装置からほぼ同じ時刻（例えば差が１分未満）に送信される。そこで、本発明では、上記識別データに、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含めている。このため、受信装置では、データを容易に結合して復元することができる。また、送信元データおよび送信時刻データを付与する機能は、一般の送信装置にも備えられている場合が多い。よって、このような送信装置に本発明を適用した場合、識別データ付与手段として特別な構成を設けなくても上記送信装置を実現することができる。

【００１０】従って、本発明では、請求項１記載の効果に加えて、送信装置の構成を一層簡略化することができるといった効果が生じる。請求項３記載の発明は、請求項１または２記載の構成に加え、上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴としている。

【００１１】このように構成された本発明では、分割後のデータを少なくとも一部に共通の符号を有するシリアルナンバーを用いて対応付けている。このため、分割後のデータ同士をきわめて正確に対応付けることができる。例えば、分割後の各データが長くて各データの送信時刻が大幅にずれたときなどにも、各データを良好に対応付けることができる。

【００１２】従って、本発明では、請求項１または２記載の発明の効果に加えて、分割後のデータを一層正確に復元することができるといった効果が生じる。請求項４記載の受信装置は、互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、を備えたことを特徴としている。

【００１３】このように構成された本発明では、データ受信手段は互いに異なる中継装置を介して個々にデータを受信し、識別データ抽出手段は、受信した各データから所定の識別データを抽出する。すると、データ結合手段は、データ受信手段にて受信したデータの内、互いに対応する識別データを有するデータ同士を結合する。

【００１４】このため、本発明は、請求項１～３のいずれかに記載のデータ通信システムにおける受信装置として、良好に適用することができる。なお、上記識別データは、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むものであってもよく、少なくとも一部分に共通の符号を有するシリアルナンバーを含むものであってもよく、その他の形態のものであってもよい。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態を図面と共に説明する。図１は本発明を適用したデータ通信システムを表す概略構成図である。なお、本実施の形態は、インターネットを利用したネットワークプリントシステムに本発明を適用したものである。

【００１６】図１に示すように、送信装置としてのユーザー側のパーソナルコンピュータ（以下パソコンという）１は、多数のプロバイダ３を接続してなるインターネットを介してプリントサービスステーション側の受信装置としてのサーバ５に接続されている。このため、パソコン１からサーバ５に向けてデータを送信すると、そのデータは隣接するプロバイダ３を順次経由して伝搬される。また、異なる通信経路上に存在する二つのプロバイダ３ａ，３ｂには、インターネット上を通信されるデータを一旦記憶し、宛名（送信先のアドレス）を変えて送信する中継装置としてのサーバ７ａ，７ｂが接続されている。

【００１７】なお、パソコン１およびサーバ５，７ａ，７ｂは、いずれも、ＣＰＵ，ＲＯＭ，ＲＡＭの他、外付けのメモリや通信用のモデムを備えた周知のコンピュータで、サーバ５には、更に、プリントサーバ１１を介してプリンタ１３が接続されている。本システムは、ユーザー（顧客）側のパソコン１からプリントサービスステーション（印刷業者）のサーバ５へ画像データ等を送信して、プリンタ１３による画像形成を行うためのものである。また、サーバ５，７ａ，７ｂは、ＦＴＰ（ファイル・トランスファー・プロトコル）サーバであっても、メールサーバであってもよい。

【００１８】次に、本システムにおけるパソコン１およびサーバ５，７ａ，７ｂの処理を、図２～４のフローチャートを用いて説明する。ユーザー側のパソコン１は、図示しないキーボード等を介してデータの送信が指示されると、図２の処理を実行する。図２に示すように、処理を開始すると、先ずＳ１にて送信するデータを読み込み、続くＳ３でそのデータを二つに分割する。続くＳ５

では、分割後の１つ目のデータをサーバ７ａに対応する第１アドレスへ送信し、Ｓ７では、分割後の２つ目のデータをサーバ７ｂに対応する第２アドレスへ送信して処理を終了する。なお、Ｓ５，Ｓ７におけるデータの送信に当たっては、送信元であるパソコン１のアドレスを表す送信元データと、その送信時刻を表す送信時刻データとが、送信するデータに付与される。この処理は周知であるのでここでは詳述しない。また、Ｓ５，Ｓ７では分割後のデータのどちらを１つ目としてもよい。

【００１９】一方、サーバ７ａは図３に示す処理を繰り返し実行する。なお、サーバ７ｂも同様の処理を繰り返し実行する。図３に示すように、処理を開始すると、Ｓ１１にてデータを受信したか否かを判断し、受信した場合（Ｓ１１：ＹＥＳ）はＳ１３へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。Ｓ１３では、受信したデータをサーバ５に対応する所定アドレスへ送信してＳ１１へ移行する。また、データを受信していない場合（Ｓ１１：ＮＯ）は、そのままＳ１１にて待機する。

【００２０】このため、図２の処理により、パソコン１が分割後のデータをサーバ７ａ，７ｂに送信すると（Ｓ５，Ｓ７）、図３の処理により、サーバ７ａ，７ｂは分割後の各データを個々に受信し（Ｓ１１；ＹＥＳ）、そのデータをサーバ５に送信する（Ｓ１３）。すなわち、分割後のデータが異なる通信経路を介してサーバ５に送信される。

【００２１】次に、図４はサーバ５が繰り返し実行する処理を表すフローチャートである。処理を開始すると、Ｓ２１にてデータを受信したか否かを判断し、受信した場合（Ｓ２１：ＹＥＳ）はＳ２３へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。Ｓ２３では、既に受信してメモリに格納されているデータの中で、そのデータに付与された送信元データが一致するもの、すなわち、送信元のアドレスが一致するものがあるか否かを判断する。既に受信したデータの中で、Ｓ２１にて受信したデータと送信元のアドレスが一致するデータがあれば（Ｓ２３：ＹＥＳ）、Ｓ２５へ移行し、送信時刻データが表す送信時刻がほぼ一致するデータが、その中にあるか否かを判断する。

【００２２】Ｓ２５で肯定判断した場合、Ｓ２１にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図２のＳ５，Ｓ７で連続して送信されたデータである。そこで、この場合（Ｓ２５：ＹＥＳ）、Ｓ２７にて二つのデータを結合し、続くＳ２９にて結合後のデータをプリントサーバ１１へ送付してＳ２１へ戻る。すると、結合後のデータ、すなわち、図２のＳ１にて読み込まれたデータに基づき、プリンタ１３による画像形成が実行される。一方、Ｓ２１，Ｓ２３，Ｓ２５のいずれかで否定判断した場合は、何もせずそのままＳ２１へ戻る。

【００２３】このように、本システムでは、パソコン１により分割して異なる通信経路を介して送信されたデータを、サーバ５にて復元し、プリンタ１３にて画像形成することができる。また、各プロバイダ３を介して伝搬されるデータは、それぞれ分割後のデータである。このため、各プロバイダ３を介して伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。従って、本システムでは、通信されるデータの漏洩を良好に防止することができる。更に、本システムでは、Ｓ２７にて結合すべきデータを、送信元データおよび送信時刻データによって識別している。送信元データおよび送信時刻データを付与する機能は、一般のパソコンにも備えられている場合が多い。本システムでは、このような一般的な機能を利用しているので、処理を一層簡略化することができる。

【００２４】次に、本発明の他の実施の形態を図５～７のフローチャートを用いて説明する。なお、本実施の形態では、前述の実施の形態とは各部の処理のみが異なるので、図２で使用した符号等はそのまま使用する。また、図５～７では、図２～４と同様の処理には同一の符号を付して、処理の詳細な説明を省略する。

【００２５】図５は、データの送信が指示されたときパソコン１が実行する処理を表すフローチャートである。図５に示すように、処理を開始すると、送信するデータを読み込み（Ｓ１）、そのデータを二つに分割した（Ｓ３）後、Ｓ３１へ移行する。Ｓ３１では、現在時刻から乱数等を用いてシリアルナンバーを発生する。なお、シリアルナンバーとしては、アルファベット等の数字以外の符号を含むものを採用してもよい。続くＳ３３では、１つ目のデータにそのシリアルナンバーおよび数字の「１」を付与し、Ｓ３５では、２つ目のデータに上記シリアルナンバーおよび数字の「２」を付与する。続いて、シリアルナンバー等が付与された分割後の各データを、第１および第２のアドレス（サーバ７ａおよび７ｂに対応）に送信して処理を終了する（Ｓ５，Ｓ７）。

【００２６】図６はサーバ７ａ，７ｂが繰り返し実行する処理を表すフローチャートである。データを受信すると（Ｓ１１：ＹＥＳ）Ｓ４１へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合（Ｓ４１：ＹＥＳ）はＳ１３へ移行し、データをサーバ５に対応する所定アドレスへ送信してＳ１１へ移行する。また、データを受信していない場合（Ｓ１１：ＮＯ）、およびシリアルナンバーが付与されていない場合（Ｓ４１：ＮＯ）は、そのままＳ１１へ移行する。すなわち、シリアルナンバーが付与されていない場合は、図５のＳ５，Ｓ７によって送信されたデータではないので、図示しない他のルーチンにより、サーバ７ａ，７ｂとしての通常の処理を行うのである。

【００２７】図７は、サーバ５が繰り返し実行する処理

を表すフローチャートである。この処理では、データを受信すると（Ｓ２１：ＹＥＳ）Ｓ５１へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合（Ｓ５１：ＹＥＳ）Ｓ５３へ移行し、既に受信してメモリに格納されているデータの中で、そのデータに付与されたものと同一のシリアルナンバーを有するものがあるか否かを判断する。

【００２８】Ｓ５３で肯定判断した場合、Ｓ２１にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図５のＳ５，Ｓ７で連続して送信されたデータである。そこで、この場合、二つのデータを結合し（Ｓ２７）、プリントサーバ１１へ送付する（Ｓ２９）。すると、結合後のデータに基づき、プリンタ１３による画像形成が実行される。一方、Ｓ２１，Ｓ５１，Ｓ５３のいずれかで否定判断した場合は、何もせずそのままＳ２１へ戻る。

【００２９】本実施の形態でも、前述の実施の形態と同様、データを分割し、異なる通信経路を伝搬させることにより、データの漏洩を良好に防止することができる。また、本システムでは、分割後のデータをシリアルナンバーを用いて対応付けている。このため、データを一層正確に復元することができる。例えば、分割後の各データが長くて各データの送信時刻が大幅にずれたとき、すなわち、図５のＳ５，Ｓ７の間隔が大きくなったときなどにも、各データが良好に対応付けられる。更に、データにシリアルナンバーがない場合（Ｓ４１：ＮＯ）、サーバ７ａ，７ｂは通常の処理を行う。このため、上記処理のためにサーバ７ａ，７ｂを増設する必要もない。

【００３０】なお、上記各実施の形態において、Ｓ５，Ｓ７における送信元データおよび送信時刻データを付与する処理、並びに、Ｓ３３，Ｓ３５の処理が識別データ付与手段に、Ｓ３の処理がデータ分割手段に、Ｓ５，Ｓ７におけるデータの送信処理がデータ送信手段に、Ｓ２１の処理がデータ受信手段に、Ｓ２７の処理がデータ結合手段に、Ｓ２３，Ｓ２５，Ｓ５１，Ｓ５３における送信元データ，送信時刻データ，またはシリアルナンバーを抽出する処理が識別データ抽出手段に、それぞれ相当する。

【００３１】また、本発明は、上記実施の形態になんら限定されるものではなく、本発明の要旨を逸脱しない範囲で種々の形態で実施することができる。例えば、本発明は、インターネットを利用したデータ通信システムの他、電話回線やケーブル，無線等、種々の通信経路を利用したデータ通信システムに適用することができる。但し、インターネットはきわめてアクセスが容易である。従って、上記実施の形態のように、インターネットを利用したデータ通信システムに適用した場合、本発明によるデータの漏洩防止の効果が一層顕著になる。

【００３２】更に、上記実施の形態では、受信側のサーバ５にプリンタ１３を接続したネットワークプリントシステムに対して本発明を適用しているが、本発明は、この他種々のデータ通信システムに適用することができる。例えば、単にデータを送受信するだけのシステムにも適用することができる。この場合、サーバ５のＳ２９の処理（図４，図７）を省略すればよい。

【図面の簡単な説明】

【図１】本発明を適用したデータ通信システムを表す概略構成図である。

【図２】そのシステムの送信側パソコンの処理を表すフローチャートである。

【図３】そのシステムの中継用サーバの処理を表すフローチャートである。

【図４】そのシステムの受信側サーバの処理を表すフローチャートである。

【図５】上記送信側パソコンの処理の他の形態を表すフローチャートである。

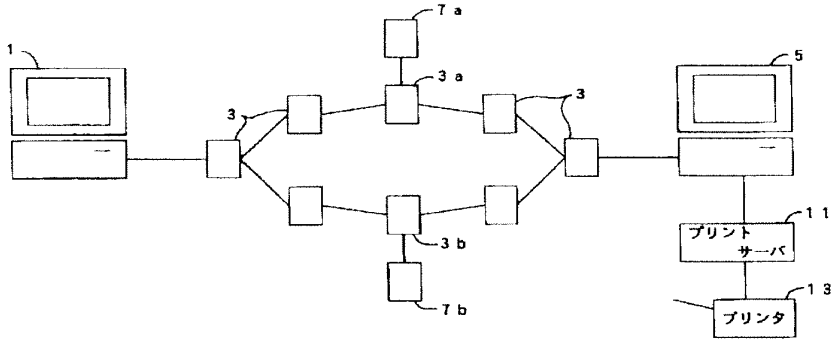
【図６】上記中継用サーバの処理の他の形態を表すフローチャートである。

【図７】上記受信側サーバの処理の他の形態を表すフローチャートである。

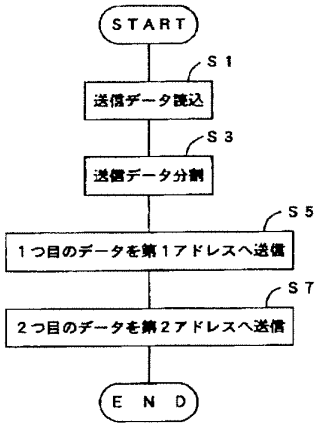
【符号の説明】

１…パソコン　　３…プロバイダ
５，７ａ，７ｂ…サーバ
１１…プリントサーバ　　１３…プリンタ

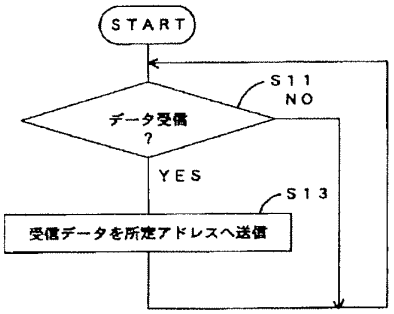
【図１】


1
7a
3a
3
3
5
3b
7b
プリント
サーバ
11
プリンタ
13

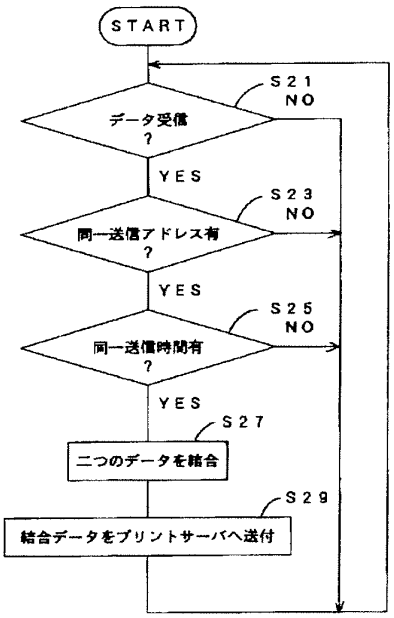
【図２】


START
S1
送信データ読込
S3
送信データ分割
S5
1つ目のデータを第1アドレスへ送信
S7
2つ目のデータを第2アドレスへ送信
E N D

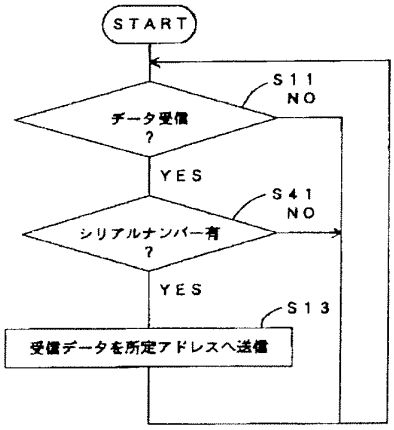
【図３】


START
S11
NO
データ受信
?
YES
S13
受信データを所定アドレスへ送信

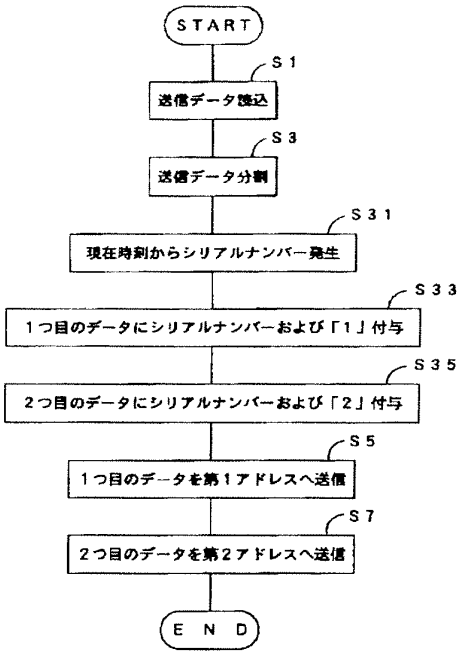
【図４】


START
S21
NO
データ受信
?
YES
S23
NO
同一送信アドレス有
?
YES
S25
NO
同一送信時間有
?
YES
S27
二つのデータを結合
S29
結合データをプリントサーバへ送付

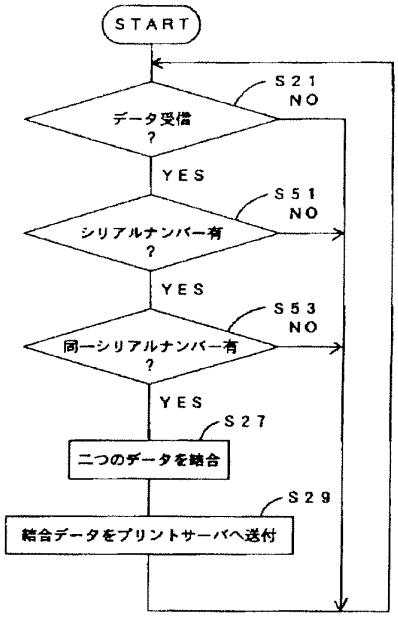
【図６】


START
S11
NO
データ受信
?
YES
S41
NO
シリアルナンバー有
?
YES
S13
受信データを所定アドレスへ送信

【図５】



【図７】



フロントページの続き

(72)発明者　近藤　博大
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　安井　恒夫
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

English Abstract
of Cited Document 3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-363941**

(43)Date of publication of application : **16.12.1992**

(51)Int.Cl. **H04L 12/48**
H04L 9/00
H04L 9/10
H04L 9/12

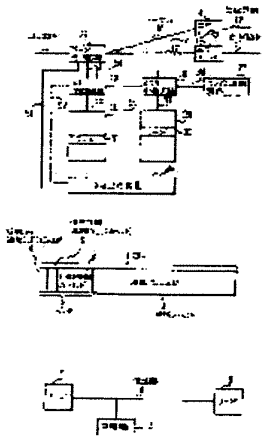
(21)Application number : **03-044062**

(22)Date of filing : **18.02.1991**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **NAKAJIMA SEIICHI**
HARADA YONOSUKE

(54) INTERCEPT PREVENTION METHOD IN ASYNCHRONOUS TRANSFER MODE COMMUNICATION



(57)Abstract:

PURPOSE: To prevent intercept without losing high speed performance of the asynchronous transfer mode(ATM) by using optional one of plural virtual bus identifiers (VPI) and virtual line identifiers (VCI) allocated to one call channel at random so as to transfer a cell.

CONSTITUTION: Plural VPI, VCI are assigned to one call channel and one of the plural VCI, VPI allocated is used at random optionally to transfer a cell. Since the VPI, VCI relating to the same call channel are always changed in the unit of cells through a transmission line 9 between a transmission node and a reception node, even when a cell having the specific VPI, VCI is extracted, it is impossible to collect the communication content of the specific call. Even when all cells on the transmission line 9 are collected, it is difficult to extract a cell of the specific call and the intercept is prevented. Furthermore, since only the VPI and VCI are revised in the unit of cells, the processing of the header 2 is easy and intercept is prevented without losing the high speed performance of the ATM.

Cited Document 3 (JP-A (Kokai) H04-363941)

<1>

[0019]

[Effects of the Invention]

As explained above, in the method of preventing intercept in ATM communication of the present invention, a plurality of VPIs and VCIs which identify a channel multiplexed by cells are allocated, and are differentiated in each cell. Thus, it is impossible to collect a communication content of a specific call, even when specific VPIs and VCIs are extracted. Accordingly, the method enables prevention of intercept. Furthermore, since only VPIs and VCIs are converted in this method, header processing does not become complicated and a circuit configuration becomes simple. Accordingly, the present method enables prevention of intercept without losing high speed performance of ATM.

<2>

[Explanations of Letters or Numerals]

1, cell; 2, header; 3, information field; 4, virtual path identifier (VPI) field; 5, virtual channel identifier (VCI) field; 6, information field; 7 and 8, nodes; 9, transmission line; 10, eavesdropping device; 11, input transmission line; 12 and 13, output transmission lines; 14 and 15, output buffers; 16 and 17, highways; 21, header processing circuit; 22 and 23, memory control circuits; 24 and 25, memories; 26, central processing device; 27, random selection circuit; 31 and 32, words; 41, 42, 43, 44, and 45, fields; 51, 52, 53, 54, 55, 56, 57, and 58, control lines.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平4－363941

(43)公開日　平成４年(1992)12月16日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/48					
9/00					
9/10					
		8529－5K	Ｈ０４Ｌ　11／20	Ｚ	
		7117－5K	9／00	Ｚ	

審査請求　未請求　請求項の数１(全　5　頁)　最終頁に続く

(21)出願番号　特願平3－44062

(22)出願日　平成３年(1991)２月18日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　中島　誠一
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　原田　要之助
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

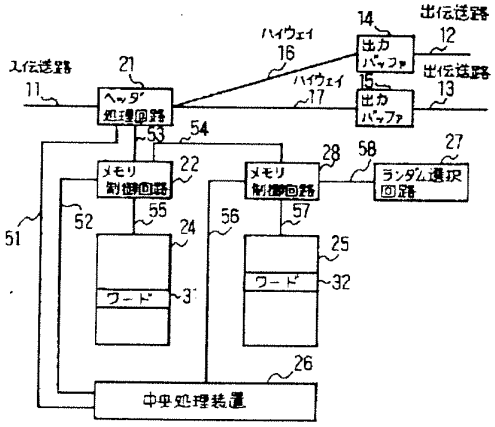
(74)代理人　弁理士　並木　昭夫

(54)【発明の名称】　非同期転送モード通信における盗聴防止方法

(57)【要約】

【目的】　ＡＴＭ（非同期転送モード）通信の高速性を損なわずに盗聴防止を可能にする。

【構成】　１つの呼のチャネル（セル多重化されたチャネル）に対して該チャネルを識別する複数のＶＰＩ、ＶＣＩを割り当て、割り当てられた複数のＶＰＩ、ＶＣＩの中から任意の一つをランダム選択回路２７によりランダムに選択、使用してセルを転送するようにする。



1

【特許請求の範囲】

【請求項1】　非同期転送モード通信において、1つの呼のチャネルに対して複数の仮想パス識別の割り当て、或いは複数の仮想回線識別の割り当て、の少なくとも一方を実施し、該呼の情報を転送するに際し、セル単位に割り当てられた複数の仮想パス識別の中の任意の一つのランダム使用、或いはセル単位に割り当てられた複数の仮想回線識別の中の任意の一つのランダム使用、の少なくとも一方を実施してセルを転送することを特徴とする非同期転送モード通信における盗聴防止方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、非同期転送モード通信において、セル多重化された回線での情報の盗聴防止方法に関するものである。

【0002】

【従来の技術】高度情報化社会において情報の盗聴防止が重要であることは述べるまでもない。本発明は、かかる意味での非同期転送モード通信における盗聴防止方法に関するものであるが、先ず非同期転送モード通信についての簡単な説明から始める。さて、時分割多重方式には、時間軸上の位置の識別によって多重する方式とラベルの識別によって多重する方式とがある。従来、ラベル多重方式として情報フィールドの長さを可変として多重するパケット方式があるが、最近、固定長のパケット（セル）を用いて多重する方式（被同期転送モード　Asynchronous Transfer Mode　以降ＡＴＭと略記する）が提案されている。ＡＴＭでは、情報転送の要求時のみセルが送出されるので、その頻度に応じて間欠的／連続的通信が可能になり、低速から高速までの任意の転送速度に対応することができ、かつ、情報がない場合には空きセルが挿入されるため、決まったタイミングでセルが出現し、セルの先頭の識別と交換とを高速に行うことができる特徴があり、今後の広帯域ＩＳＤＮの転送モードとして有望な方式である。なお、ＡＴＭについて記載した文献としては、川原崎他，「ＡＴＭ通信技術の動向－－高速広帯域系への展開に向けて－－」、電子情報通信学会誌、71,8, pp.809-814（昭63-08）を挙げることができる。

【0003】図3は国際標準のＡＴＭセル構造を示す説明図である。同図において、1はセル、2はヘッダ、3は情報フィールド、4は仮想パス識別（ＶＰＩ）フィールド、5は仮想回線識別（ＶＣＩ）フィールド、6はその他の制御情報フィールドであり、セル1は53バイト、ヘッダ2は5バイト、情報フィールド3は48バイト、ＶＰＩフィールド4は網内では12ビット、ユーザ・網間では8ビット、ＶＣＩフィールド5は16ビットで構成される。ヘッダ2には多重、セル交換、トラヒック制御等に必要な制御情報が含まれている。

【0004】ノードにおいて、通常、ハードウェアによ

2

りヘッダ2が分析されて多重、セル交換、トラヒック制御が高速に行われる。多重化された伝送路上の1つの特定のチャネルは（ＶＰＩ＋ＶＣＩ）で識別され、交換ノードでＶＰＩ，ＶＣＩは新たな値に付け替えられる。図4はノード間における盗聴の例を示すブロック図で、7，8はノード、9は伝送路、10は盗聴機であり、伝送路9にはセル1が転送される。特定のチャネルを盗聴するには、盗聴機10で特定のＶＰＩ，ＶＣＩのセルを選択すればよく、容易に盗聴される恐れがある。盗聴を防止する方法には、従来の技術としてはセル1に暗号をかける方式が考えられる。

【0005】しかし、ＡＴＭでは伝送速度として数Ｇｂｉｔ／ｓ以上の速度までを想定しているため、交換ノードでセルを復号化し、ヘッダ2を分析することは実現不可能である。また、ＶＰＩ，ＶＣＩのみを暗号化しても、暗号化されたＶＰＩ，ＶＣＩは、交換機における交換時の行先を示す情報であり、常に通信中同じ値をとるので、その値でセルを抽出すれば容易に盗聴されることになる。

【0006】

【発明が解決しようとする課題】本発明は、上記事情に鑑みてなされたもので、その目的とするところはＡＴＭの高速性を損なわずに盗聴を防止することのできる非同期転送モード通信における盗聴防止方法を提供することにある。

【0007】

【課題を解決するための手段】本発明は、上記の課題を解決するため、1つの呼のチャネルに対して複数のＶＰＩ，ＶＣＩを割り当て、割り当てられたＶＰＩ，ＶＣＩの中から任意の一つをランダムに使用してセルを転送するようにしたものである。

【0008】

【作用】本発明は、1つの呼のチャネルに対して複数のＶＰＩ，ＶＣＩを割り当て、割り当てられた複数のＶＰＩ，ＶＣＩの中から任意の一つをランダムに使用してセルを転送することを最も特徴とするものである。したがって、送信ノードと受信ノードと間の伝送路において、同一の呼のチャネルに関するＶＰＩ，ＶＣＩはセル単位で常に変化するため、特定のＶＰＩ，ＶＣＩのセルを抽出しても特定の呼の通信内容を収集することは不可能になる。また、伝送路上のすべてのセルを収集したとしても、特定の呼のセルを抽出することは困難であり、盗聴の防止が可能になる。本発明では、ＶＰＩ，ＶＣＩのみをセル単位で変更するため、送信ノード、受信ノードのヘッダ2の処理は容易であり、ＡＴＭの高速性を損なうことなく盗聴の防止が可能となる。

【0009】

【実施例】本発明の実施例を図面に基づいて詳細に説明する。説明を簡単にするため、ＶＣＩにのみ本発明を適用した場合を例にとって説明する。図1は本発明の盗聴

3

防止方法を実現する交換ノードの実施例であって、１１は入り伝送路、１２，１３は出伝送路、１４，１５は出力バッファ、１６，１７は交換ノード内のハイウェイ、２１はヘッダ処理回路、２２，２３はメモリ制御回路、２４，２５はメモリ、２６は中央処理装置、２７はランダム選択回路、３１，３２はメモリ２４，２５のワード、４１，４２，４３，４４，４５はワード３２のフィールド、５１，５２，５３，５４，５５，５６，５７，５８は制御線である。

【００１０】メモリ２４は、入り伝送路１１から到着するセルの「入りＶＣＩ」と「変換ＶＣＩ」との対応をとるメモリであり、入りＶＣＩをアドレスとして変換ＶＣＩを得ることができる。メモリ２５は「変換ＶＣＩ」と、「出ＶＣＩ」との対応をとるメモリであり、変換ＶＣＩをアドレスとして出ＶＣＩを得ることができる。入り伝送路１１からセルが到着すると、ヘッダ処理回路２１は入りＶＣＩを制御線５３を介してメモリ制御回路２２に入力する。

【００１１】メモリ制御回路２２は、制御線５５を介して入りＶＣＩをアドレスとして入力し、メモリ２４のワード３１から変換ＶＣＩを読み出し、変換ＶＣＩを制御線５４を介してメモリ制御回路２３に入力する。メモリ制御回路２３は、制御線５７を介して変換ＶＣＩをアドレスとしてメモリ２５に入力し、出ＶＣＩ（複数）をワード３２から読み出し、制御線５８を介してランダム選択回路２７により、複数の出ＶＣＩの中から１つの出ＶＣＩを決定し、制御線５４、メモリ制御回路２２、制御線５３を介してヘッダ処理回路２１に出ＶＣＩを返送し、ヘッダ処理回路２１は、該セルの入りＶＣＩをその出ＶＣＩに置き換えて、例えばハイウェイ１７を介して出力バッファ１５に入力する。該セルは出力バッファ１５から出伝送路１３に送出される。

【００１２】１つの呼に関するセルのＶＣＩは複数割り当てられるが、この割り当ては呼の設定時に送信側の交換ノードから呼設定制御セルを用いて、例えば、入りＶＣＩとして＃３，＃３８，＃７４を使用することを通知してくる。ヘッダ処理回路２１がヘッダを分析して呼設定制御セルを検出すると制御線５１を介して中央処理装置２６に該セルを転送する。中央処理装置２６は、出方路の選択制御等に加えて、変換ＶＣＩ、出ＶＣＩを決定する。まず、空きの変換ＶＣＩを決定すると、変換ＶＣＩをメモリ２４の入りＶＣＩに対応するアドレスに書くため、送信側交換ノードから指定された複数のＶＣＩと中央処理装置２６が決定した変換ＶＣＩを制御線５２を介してメモリ制御回路２２に転送する。

【００１３】メモリ制御回路２２は、その指示に従って変換ＶＣＩを指定のアドレスに書き込む。例えば、変換ＶＣＩを＃２１とすれば、上記の例ではメモリ２４のアドレス＃３，＃３８，＃７４に変換ＶＣＩの＃２１が書かれる。したがって、該呼のセルの入りＶＣＩが＃３，

4

＃３８，＃７４の何れかであれば、変換ＶＣＩは＃２１に変換されることになる。中央処理装置２６は同時に、空いた複数の出ＶＣＩ（例えば＃５５，＃８９，＃９３）を決定し、制御線５６を介してメモリ２５の変換ＶＣＩに対応するアドレスに、複数の出ＶＣＩを書き込むため、変換ＶＣＩと出ＶＣＩをメモリ制御回路２３に転送する。

【００１４】メモリ制御回路２３は、変換ＶＣＩに対応するアドレスに出ＶＣＩ（この例では＃５５，＃８９，＃９３）を書き込む。具体的には、図２に示すワード３２のフィールド４１～４５に、１つのフィールドに１つの出ＶＣＩを、例えば＃５５とか、＃８９のように、書き込む。この例では３つの出ＶＣＩを使用しているため、フィールド４１，４２，４３に＃５５，＃８９，＃９３が各々書き込まれる。メモリ制御回路２３は、ワード３２を読み出すと、制御線５８を介してランダム選択回路２７に複数の出ＶＣＩを入力し、ランダム選択回路２７は乱数を発生して複数の出ＶＣＩから１つの出ＶＣＩを選択し、制御線５８、メモリ制御回路２３、制御線５４、メモリ制御回路２２、制御線５３を介してヘッダ処理回路２１に該出ＶＣＩを返送する。

【００１５】このため、ワード３２を読み出す毎に、上記の例では出ＶＣＩは＃５５，＃８９，＃９３の中の一つがランダムに選択されることになる。従って、入り伝送路１１から該呼のセルが到着すると、入りＶＣＩは（＃３，＃３８，＃７４のいずれかでセル単位に変わる）変換ＶＣＩの＃２１に一旦変換され、出ＶＣＩは＃５５，＃８９，＃９３ののいずれかに変換されることになる。このため、入り伝送路１１、出伝送路１３に流れる該呼チャネルのＶＣＩは固定されず常に変化しており、盗聴を防止することができる。

【００１６】上記説明では、割り当て入りＶＣＩ、出ＶＣＩの数は数個であったが、ＶＣＩは１６ビットの容量があるため、割り付けるＶＣＩの数を数百以上にすることも特に大きな制約にはならない。上記例では、入りＶＣＩ、出ＶＣＩの割り当ては呼設定時に行われるため、通信中は割り当てられた複数のＶＣＩは固定されるが、通信中にこれを変更することも可能である。これは、通信中に送信ノードで新たなＶＣＩを決定し、受信ノードでは中央処理装置２６からメモリ２４、２５の内容を書き換えれば良く、この場合にはＶＣＩのランダム性が増加するため、盗聴に対する耐力を高めることが可能となる。

【００１７】上記説明では、ＶＣＩの複数割り当てを呼設定時に行った例であるが、あらかじめ、ノード間でＶＣＩの割り当てグループを定めておき、その呼設定時にはそのグループ内の１つのＶＣＩを相手ノードに通知する方法をとってもよい。上記説明では、ＶＣＩをセル単位で変更する例であったが、さらにＶＰＩをもセル単位に変更する場合、あるいはＶＰＩのみを変更する場合に

5

も図1と同様な構成で実現できることは明らかである。

【0018】上記実施例に加えて、入り伝送路1、出伝送路13等に流れる情報に従来行われているスクランブラを掛ければ、さらに盗聴に対する耐力を高めることが可能となる。また、送信ノードから割り当てたVPI、VCIを通知する情報に対して暗号をかければ、さらに盗聴にたいする耐力を高めることが可能となる。上記説明では、特殊な呼が非常に少ない場合には複数のVCIを用いても盗聴の可能性が高いが、ダミーのチャネルを設定したり、空きセルに複数のVCIを割り当てる等により対処すればよい。

<1>

【0019】

【発明の効果】以上説明したように、本発明のATM通信における盗聴防止方法によれば、セル多重化されたチャネルを識別するVPI、VCIを複数割り当て、VPI，VCIをセル単位に変更するため、伝送路上で特定VPI，VCIを抽出しても特定呼の通信情報を得ることが不可能であり、盗聴の防止をすることが可能となる。また、本方法ではVPI、VCIのみを変更するため、ヘッダの処理が複雑にならず簡単な回路構成とすることができ、ATMの高速性を損なうことなく盗聴防止

6

が実現できる。

【図面の簡単な説明】

【図1】本発明の一実施例を示すブロック図である。

【図2】図1におけるワード32の構成例を示す説明図である。

【図3】ATMセル構造を示す説明図である。

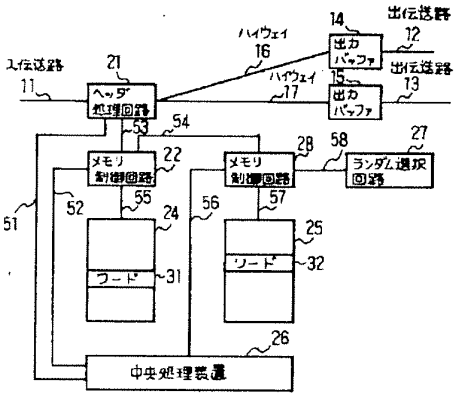
【図4】ノード間における盗聴の例を示すブロック図である。

<2>

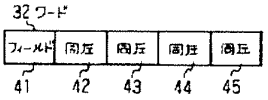
【符号の説明】

1…セル、2…ヘッダ、3…情報フィールド、4…仮想パス識別（VPI）フィールド、5…仮想回線識別（VCI）フィールド、6…情報フィールド、7，8…ノード、9…伝送路、10…盗聴機、11…入り伝送路、12，13…出伝送路、14，15…出力バッファ、16，17…ハイウェイ、21…ヘッダ処理回路、22，23…メモリ制御回路、24，25…メモリ、26…中央処理装置、27…ランダム選択回路、31，32…ワード、41，42，43，44，45…フィールド、51，52，53，54，55，56，57，58…制御線

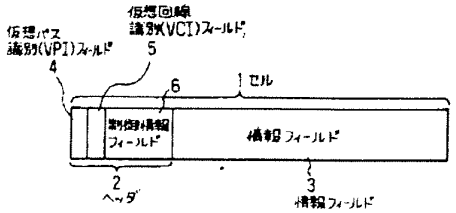
【図1】



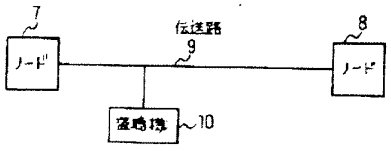
【図2】



【図3】



【図4】



【手続補正書】
【提出日】平成４年６月１８日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　非同期転送モード通信において、１つの呼のチャネルに対して複数の仮想パス識別の割り当て、或いは複数の仮想回線識別の割り当て、の少なくとも一方を実施し、該呼の情報を転送するに際し、セル単位に割り当てられた複数の仮想パス識別の中の任意の一つのランダム使用、或いはセル単位に割り当てられた複数の仮想回線識別の中の任意の一つのランダム使用、の少なくとも一方を実施してセルを転送することを特徴とする非同期転送モード通信における盗聴防止方法。

フロントページの続き

(51)Int.Cl.⁵	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/12				

Cited Document 5
translated by Computer

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-018492**

(43)Date of publication of application : **17.01.1997**

(51)Int.Cl. **H04L 12/28**
H04L 12/02
H04Q 3/00

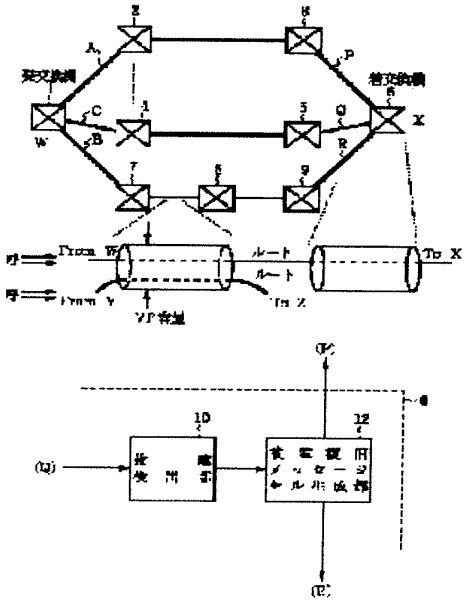
(21)Application number : **07-166048**

(22)Date of filing : **30.06.1995**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **OKI EIJI**
YAMANAKA NAOAKI

(54) ATM COMMUNICATION NETWORK AND FAILURE RESTORATION METHOD



(57)Abstract:

PURPOSE: To reduce the cost of an exchange and further to enforce a fault restoration without providing a device concentratedly restoring a fault by omitting a redundant hardware constitution for securing the high reliability of an exchange.

CONSTITUTION: An incoming exchange 6 is provided with a fault restoration message generation part 12 as a means transmitting a fault restoration message to a virtual pass. A fault restoration message cell has a destination area and a message area. On the destination area, information for reaching a transmitting exchange 1 is mounted via one or more repeating exchanges 2 to 5 and 7 to 9. The repeating exchanges 2 to 5 and 7 to 9 are

provided with a fault restoration message cell information mounting parts 14 mounting null band information on the repeating exchanges 2 to 5 and 7 to 9 in the message area of the routing fault restoration message cell. By this constitution, constitution, the cost of the exchange is reduced and further, the restoration is made possible without providing a device concentrately performing a fault restoration.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]An ATM communication network comprising:

Two or more subscriber exchange.

Two or more physical transmission lines which connect between [this] two or more subscriber exchange.

In an ATM communication network which is provided with a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange, to said subscriber exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, A means to have a destination area and a message area, and for information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party to be carried, and to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes in said transit exchange.

[Claim 2]The ATM communication network according to claim 1 provided with a means to add the number of transit exchanges carried in this hop counter field whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area was provided and a fault restoration message cell passed to said transit exchange.

[Claim 3]The ATM communication network according to claim 1 or 2 with which a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell sends out a fault restoration message cell according to an output of this means to recognize.

[Claim 4]Said subscriber exchange is equipped with a means to receive a fault restoration message cell which comes via two or more virtual paths, The ATM communication network according to any one of claims 1 to 3 provided with a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell, and transit exchanges.

[Claim 5]a virtual path set as subscriber exchange -- present -- a virtual path of business and

a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, A fault restoration method choosing two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell in subscriber exchange used as an address of this fault restoration message cell.
[Claim 6]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a fault restoration method according to claim 5 on an autonomous distribution target.
[Claim 7]a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. A standby method of fault restoration choosing beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.
[Claim 8]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a standby method of the fault restoration according to claim 7 on an autonomous distribution target.
[Claim 9]A fault restoration method, wherein it addresses subscriber exchange in one communications network to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network and it sends out a fault restoration message cell to a virtual path, respectively.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention is used for an ATM (Asynchronous Transfer Mode) communications network. It is related with the fault restoration art over failure of the communication apparatus especially inserted in the transmission line.
[0002]
[Description of the Prior Art]The virtual channel hair drier (Virtual Channel Handler,

switchboard) which switches by an ATM communication network making a unit physically a virtual channel (Virtual Channel: it is called following VC), It is connected by the transmission line and the virtual path hair drier (Virtual Path Handler:VPH or cross connect, XC) which sets up the route of information transfer by making a virtual path (Virtual Path: henceforth VP) into a unit is constituted. Theoretically, between VCH is connected by VP and the termination of VP is carried out by VCH via zero or one or more VPH(s).

[0003]The fault restoration method for failure of the conventional communication apparatus is shown in drawing 12. Drawing 12 is a figure showing the concept of the conventional fault restoration method. There is fault restoration of VP level shown in the fault restoration and drawing 12 (a) of the physical level shown in drawing 12 (b) in the conventional fault restoration method. making the physical transmission-line link double, in order to realize fault restoration of a physical level -- one side -- present -- business -- a system and another side are made into the reserve system. if -- present -- business -- if failure occurs in the communication apparatus of a system -- present -- business -- it changes from a system to a reserve system, and failure is restored. However, in the fault restoration of a physical level, a physical transmission-line link must be made double and there is always a problem that a network resource cannot be used efficiently.

[0004]Then, there is the fault restoration method of VP level which applied the concept of VP which is the feature of an ATM communication network. VP is identified by VPI (Virtual Path Identifier) in the header area given to the cell which is a functional information unit, and a course is set up in VPH by the pass connection (routing) table which described the connection destination of the path. Fault restoration of VP level is realized by switching VP cut by failure to VP which bypassed the locating fault and was newly formed using the ability of the course and capacity of VP to set up independently. It is based on the detour path information to which the central post office which is supervising the ATM communication network unitary was especially set beforehand at the time of a failure occurrence, and is each node () within the net. [VCH and] The fault restoration method with which a centralized control system and each node make an autonomous distribution target look for and restore a detour path for the method which controls to VPH and others is called self healing method. As compared with the fault restoration of a physical level, it excels in the fault restoration of VP level with the point that the network resource of a transmission line can be used efficiently, or the point that it can respond to change of a net flexibly. Therefore, the fault restoration method which combined the physical level and VP level is applied as the conventional fault restoration method.

[0005]

[Problem(s) to be Solved by the Invention]However, in the fault restoration method of only the conventional physical level and VP level, sake [premised], a high reliability switchboard is required for failure of VCH (switchboard). In the ATM communication

network with which two or more media are intermingled, although the reliability demanded for every media differed, the switchboard was designed satisfy reliability according to the reliability demanded most highly, and it was redundant not much to the media which do not require reliability. Although drawing 13 is a key map of the high-reliability-ized switchboard, in the high-reliability-ized switchboard, the switch part, the I/O part, and the CPU section have doubled like drawing 13, and these units are further combined by the crossing route. The cost of the high-reliability-ized switchboard will become high about 6 times from 4 times compared with the cost of a switchboard with simple composition by such double-ization.

[0006]This invention is carried out to such a background and is a thing.

It is providing the ATM communication network and the fault restoration method of performing the measure against fault restoration on condition of the purpose.

An object of this invention is to provide the ATM communication network and the fault restoration method the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. An object of this invention is to provide the ATM communication network and the fault restoration method of reducing the cost of a switchboard. An object of this invention is to provide the ATM communication network and the fault restoration method of performing fault restoration, without forming the device which performs fault restoration intensively.

[0007]

[Means for Solving the Problem]When applying a switchboard with simple composition as a communication apparatus, it is necessary to restore quickly VC route obstacle at the time of failure of a switchboard. Then, this invention provides a method of restoring VC route obstacle quickly at the time of failure of a switchboard. As the method, at the time of failure of a switchboard, in order to restore a working route obstacle between arrival-and-departure switchboards, a fault restoration message cell is sent out from an incoming exchange, A switchboard exchanges information with an autonomous distribution target, and notifies reticulated voice to ********, a route is changed, and a route obstacle by switchboard failure is restored by VC route level. This is called self healing of VC route level.

[0008]In conventional technology, although self healing of VP level was performed, there is a place by which it is characterized [of this invention] in the ability to restore VC route obstacle at the time of switchboard failure by self healing of VC route level.

[0009]That is, the first viewpoint of this invention is an ATM communication network which is provided with two or more physical transmission lines which connect between [this] two or more subscriber exchange with two or more subscriber exchange, and a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange.

[0010]Here a place by which it is characterized [of this invention] to said subscriber

exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have a destination area and a message area, it is carried by information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party, and to said transit exchange. It is in a place provided with a means to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes.

[0011]Whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area is provided and a fault restoration message cell passes to said transit exchange, it is desirable to have a means to add the number of transit exchanges carried in this hop counter field.

[0012]As for a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell, it is desirable to send out a fault restoration message cell according to an output of this means to recognize.

[0013]It is desirable to equip said subscriber exchange with a means to receive a fault restoration message cell which comes via two or more virtual paths, and to have a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell and transit exchanges.

[0014]A place by which the second viewpoint of this invention is the fault restoration method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell, it is in a place which chooses two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0015]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration method, and each subscriber exchange performs this fault restoration method on an autonomous distribution target.

[0016]A place by which the third viewpoint of this invention is a fault restoration standby method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which

can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. It is in a place which chooses beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0017]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration standby method, and each subscriber exchange performs this fault restoration standby method on an autonomous distribution target.

[0018]A place by which the fourth viewpoint of this invention is the fault restoration method, and it is characterized [the], Subscriber exchange in one communications network is in a place which addresses to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network, and sends out a fault restoration message cell to a virtual path, respectively.

[0019]Although that expression [like] which is a communication apparatus which is different in subscriber exchange and a transit exchange is used in this specification, this is for explaining plainly and a communication apparatus of the same hardware constitutions can realize it.

[0020]

[Function]In the method of this invention, by self healing of VC route level. Since a fault restoration message cell is sent out from an incoming exchange, a switchboard can exchange information with an autonomous distribution target, and can notify reticulated voice to ********, a route can be changed and VC route obstacle at the time of switchboard failure can be restored, The necessity which uses a high reliability switchboard is lost and cost reduction is planned by using a switchboard with simple composition.

[0021]The fault restoration message cell which an incoming exchange sends out reaches ******** via a virtual path. The virtual path beforehand defined as a virtual path which can turn into a spare virtual path may be sufficient as this virtual path, and the unspecified virtual path in which failure is not recognized may be sufficient as it.

[0022]A fault restoration message cell collects the empty band region information on the virtual path passed while reaching ******** from an incoming exchange. If a way of speaking is changed, the transit exchange inserted in the virtual path to pass carries the empty band region information in a self transit exchange in the message area of a fault restoration message cell, when passing a fault restoration message cell. The number of the transit exchanges passed simultaneously also carries as information. In ********, empty band region information and a number of a transit exchange of passed information are referred to, and the virtual path optimal as a spare virtual path is chosen. Henceforth, a virtual channel is set as this virtual path, and communication is resumed.

[0023]sending out of a fault restoration message cell -- present -- the virtual path of business -- or -- present -- it may control to be carried out when a certain failure has been recognized by the transit exchange on the virtual path of business -- by carrying out. Or it is also good to send out a fault restoration message cell also at the time of usual, and to always choose the virtual path candidate optimal as a spare virtual path.
[0024]In this invention, it is characterized [main] by each switchboard contained in an ATM communication network carrying out such fault restoration control to autonomous distribution.
[0025]
[Example]
(The first example) The composition of the first example of this invention is explained with reference to drawing 1 - drawing 5. Drawing 1 is an entire configuration figure of this invention. Drawing 2 is an important section block lineblock diagram of an incoming exchange. Drawing 3 is a lineblock diagram of a fault restoration message cell. Drawing 4 is an important section block lineblock diagram of a transit exchange. Drawing 5 is an important section block lineblock diagram of ********.
[0026]******** 1 and the incoming exchange 6 whose this invention is subscriber exchange, and physical transmission-line P-R which connects this ******** 1 and between incoming-exchange 6, It is an ATM communication network which is provided with the transit exchanges 2, 3, 4, 5, 7, 8, and 9 inserted in this physical transmission-line P-R and with which a virtual path is set up between ******** 1 and the incoming exchange 6.
[0027]Here the place by which it is characterized [of this invention] to the incoming exchange 6. Have the fault restoration message cell generation part 12 as a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have the destination area H and message area M, and the information for arriving at the destination area H at ******** 1 via the one or more transit exchanges 2, 3, 4, 5, 7, 8, and 9 is carried, It is in the place which equipped the transit exchanges 2, 3, 4, 5, 7, 8, and 9 with the fault restoration message cell information mount part 14 as a means which makes the empty band region information on the transit exchanges 2, 3, 4, 5, 7, 8, and 9 carry in message area M of the fault restoration message cell via which it goes.
[0028]In this invention example, in order to explain plainly, express as if it was the communication apparatus provided with hardware constitutions which are different, respectively in ******** 1, the incoming exchange 6, and the transit exchanges 2, 3, 4, 5, 7, 8, and 9, but. These are realizable as one communication apparatus provided with each function in common.
[0029]It is provided by hop counter field HC which carries the number of the transit exchanges 2, 3, 4, 5, 7, 8, and 9 via which it goes in message area M, and to the transit exchanges 2, 3, 4, 5, 7, 8, and 9. Whenever a fault restoration message cell passes, a means

to add the number of the transit exchanges carried in this hop counter field HC was combined with the fault restoration message cell information mount part 14, and it has it.
[0030]******** 1 and the incoming exchange 6 are equipped with the failure detection part 10 as the transit exchanges 2, 3, 4, 5, 7, and 8 inserted in the virtual path, and a means to recognize the possibility of failure of nine, The fault restoration message cell generation part 12 sends out a fault restoration message cell according to the output of this failure detection part 10.
[0031]******** 1 is equipped with the spare-routes set part 16 as a means which receives the fault restoration message cell which comes via two or more virtual paths, A means to choose the virtual path used according to the number of the empty band region information included in this fault restoration message cell and transit exchanges was combined with the spare-routes set part 16, and it has it.
[0032]VC route is set as the incoming exchange 6 through one or more VP from ******** 1. In ******** 1, when a call occurs, a certain route is chosen from two or more VC routes, and a call admission judging (Connection Admission Control:CAC) is performed. For example, selection of a route is chosen at random. It becomes call loss, if a call is received by CAC, VC connection will be set up and a call will not be received by it.
[0033]Next, operation of the first example of this invention is explained with reference to drawing 6. Drawing 6 is a figure for explaining operation of the first example of this invention. As shown in drawing 6, only paying attention to one working route, the failure recovery method of the first example of this invention when failure occurs is shown in the transit exchange 5. The working route (1->4->5->6) is set up via two transit exchanges between ******** 1 and the incoming exchange 6, a working route is this time, and it is B. The zone of [Mbps] is used.
[0034]To this working route, a call is received after CAC, and VC connection is set up or it is cut. The usage band of this working route is called for, for example in ******** 1 by observing the number of cells currently used by the working route in a certain window size. There are a jumping window and a sliding window as a window used for observation.
[0035]Here, a jumping window is the observation method which changes without a window position (observation post) overlapping with a constant period, and a sliding window is the observation method which changes gradually, while a window position overlaps with a constant period. When it says very roughly, observation with a high-speed jumping window is an advantage, and observation with an exact sliding window is an advantage.
[0036]In drawing 6 which prepares for a working route becoming unusable and sets up two or more spare routes beforehand by failure, two spare routes (the route P:1->2->3->6, the route R:1->7->8->9->6) are set up. When failure occurs, the switchboard 1 from a twist and the incoming exchange 6 recognize that a working route is in an unusable state to the cell which notifies alarm, and others. the call of VC newly demanded after a failure occurrence

although relief of VC connection set as the working route at present is not performed -- the maximum reception ******** -- an alternative route is searched like. Here, the sender and ******** 1 to which the incoming exchange 6 sends out a fault restoration message cell serve as Chooser which receives a fault restoration message cell, changes it out of spare routes, and chooses a route. The incoming exchange (sender) 6 sends out a fault restoration message cell, in order to investigate the state to spare routes. A fault restoration message cell investigates the state of VP on the course of the spare routes P and R in accordance with the course of the spare routes P and R. The route R is raised to an example and explained. Minimum b_{min}(4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in message area [of a fault restoration message cell] M as a pay load. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell. The fault restoration message cell which goes via the route R is sent out to the transit exchange 9 from the incoming exchange 6, and in the transit exchange 9, if it $b<B_{min}$ Becomes, it will make the value of the intact VP zone b b_{min}. In the transit exchange 9, b is called for, when VP intact zone in a certain window size observes the number of use cells. There are a jumping window and a sliding window as a window used for observation. Hop counter HC is further sent out to the following switchboard, unless it counts up one and the hop limit HL is exceeded, whenever it goes via the transit exchange 9->8->7. However, spare routes are usually set up beforehand not exceed a hop limit. In the following switchboard 8, it is b= 2, and since it is $b<B_{min}$, it is set to b_{min}=2. Repeating the process of fault restoration message cell sending out similarly, a fault restoration message cell reaches ******** 1. The fault restoration message cell A sent out on spare-routes P reaches ******** 1 similarly. One or more ******** 1 are chosen as a route of a switch destination from the spare routes P or R in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route. In the example of drawing 7, although drawing 7 is a figure showing the route change situation in the first example of this invention, since the minimum of VP intact zone is [the route P] the largest in spare routes, the route P is chosen as a route of a switch destination, and the route P is used as a working route after fault restoration.

[0037]Therefore, since a switchboard exchanges information with an autonomous distribution target by sending out of a fault restoration message cell, a route is changed at the time of failure of a switchboard and failure is restored, Even if it is not a high reliability switchboard like before made double, using a switchboard with simple composition, or since it can do, the cost reduction of a switchboard can be planned.

[0038]The (second example), next the second example of this invention are described with reference to drawing 8. Drawing 8 is a figure for explaining operation of the second example of this invention. Although the fault restoration message cell was sent out in the first

example of this invention at the time of a failure occurrence, At the second example of this invention, it is usually the incoming exchange (sender) 6 to RM (Resource Management) also by the time like drawing 8. A cell is sent out and the state of the spare routes P and R is supervised. Operation of an RM cell is the same as operation of the fault restoration message cell of the first example of this invention. Out of the spare routes P or R, in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route, it has ******** (Chooser) 1 at the time of the obstacle of a working route, and it determines the route of the switch destination.

[0039]Here, an RM cell is periodically sent out from the incoming exchange (sender) 6, and ******** (Chooser) 1 which received the RM cell updates the route of the switch destination according to reticulated voice. The sending-out interval of an RM cell is determined from the degree of change of reticulated voice.

[0040]When failure occurs, the switchboard 1 from a twist recognizes that a working route is in an unusable state to the cell which notifies alarm, and others. The switchboard 1 from ******** is changed to the switch destination route with which it equipped usual at the time of a working route obstacle, and the obstacle of a working route is used as a working route.

[0041]Therefore, shortening of fault restoration time can be attained by sometimes sending out RM (Resource Management) cell from the incoming exchange (sender) 6, sometimes supervising the state of spare routes, and usually deciding the switch destination route to be it in preparation for the time of the obstacle of a working route.

[0042]The (third example), next the third example of this invention are described with reference to drawing 9. Drawing 9 is a figure for explaining operation of the third example of this invention. In the first example of this invention, the spare routes P and R were set up beforehand, and the fault restoration message cell was sent out on spare-routes P and R at the time of a failure occurrence. In the third example of this invention, the spare routes P and R are not set up beforehand, but a fault restoration message cell is sent out with flooding (Flooding) like drawing 9, and ******** 1 chooses spare routes according to the fault restoration message cell which reached ******** 1.

[0043]Here, flooding is "Flood, i.e., the term based on the image of sending out a cell to the unspecified direction just like a "flood",", and it uses for the meaning of sending out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard.

[0044]As the first example of this invention explained, minimum b_{min}(4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in the pay load of a fault restoration message cell. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell.

[0045]First, the incoming exchange (sender) 6 sends out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard. The switchboard which

received the fault restoration message cell will make the value of the intact VP zone b b_{min}, if it $b<B_{min}$ Becomes. In a switchboard, b is called for, when VP intact zone in a certain window size observes the number of use cells. The information on the switchboard via which it went is written in as channel information. Whenever hop counter HC goes via a switchboard, one is counted up, and if it is over the hop limit HL or has already gone via the same switchboard by channel information RD, a fault restoration message cell will be discarded. Otherwise, a fault restoration message cell is further sent out to all the switchboards which send out VP to a self-switchboard, the switchboard which received the fault restoration message cell repeats the same operation, and a fault restoration message reaches ********.

[0046]One or more ******** (Chooser) 1 are chosen from the fault restoration message cell which arrived as a route of a switch destination in consideration of the route information (minimum b_{min} of VP intact zone, hop number) and others based on the usage band B and the fault restoration message cell which arrived of a working route.

[0047]Therefore, fault restoration which was flexibly equivalent to net topology, VP capacity, and other change can be performed by sending out a fault restoration message cell with flooding, and making a fault restoration message cell reach ******** 1, without setting up spare routes beforehand.

[0048]The fault restoration concept by the fault restoration method of this invention is shown in drawing 10 and drawing 11. Drawing 10 is a figure showing the concept of the fault restoration method of this invention. Drawing 11 is a key map of the ATM communication network which applied the fault restoration method of this invention. Drawing 10 (b) and (c) is a fault restoration concept of VP level and a physical level known from the former. An ATM communication network can consist of this inventions, without using a highly reliable switchboard by performing fault restoration of VC route level, as shown in drawing 11 as shown in drawing 10 (a).

[0049]

[Effect of the Invention]As explained above, according to this invention, fault restoration control on condition of failure of a switchboard can be performed. For this reason, the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. Therefore, the cost of a switchboard can be reduced. Fault restoration can be performed without forming the device which performs fault restoration intensively.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The entire configuration figure of this invention.

[Drawing 2]The important section block lineblock diagram of an incoming exchange.

[Drawing 3]The lineblock diagram of a fault restoration message cell.
[Drawing 4]The important section block lineblock diagram of a transit exchange.
[Drawing 5]The important section block lineblock diagram of ********.
[Drawing 6]The figure for explaining operation of the first example of this invention.
[Drawing 7]The figure showing the route change situation in the first example of this invention.
[Drawing 8]The figure for explaining operation of the second example of this invention.
[Drawing 9]The figure for explaining operation of the third example of this invention.
[Drawing 10]The figure showing the concept of the fault restoration method of this invention.
[Drawing 11]The key map of the ATM communication network which applied the fault restoration method of this invention.
[Drawing 12]The figure showing the concept of the conventional fault restoration method.
[Drawing 13]The key map of the high-reliability-ized switchboard.
[Description of Notations]
1 ********
2-5, 7-9 Transit exchange
6 Incoming exchange
10 Failure detection part
12 Fault restoration message cell generation part
14 Fault restoration message cell information mount part
16 Spare-routes set part
H Destination area
HC Hop counter
HL Hop limit
M Message area
RD Channel information
b_{min} minimum
P, Q, and R Route

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－18492

(43)公開日　平成９年(1997)１月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/28		9466－5K	Ｈ０４Ｌ	11/20	Ｄ
	12/02			Ｈ０４Ｑ	3/00	
Ｈ０４Ｑ	3/00		9466－5K	Ｈ０４Ｌ	11/02	Ａ

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願平7－166048

(22)出願日　平成７年(1995)６月30日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　大木　英司
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　山中　直明
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　井出　直孝　(外１名)

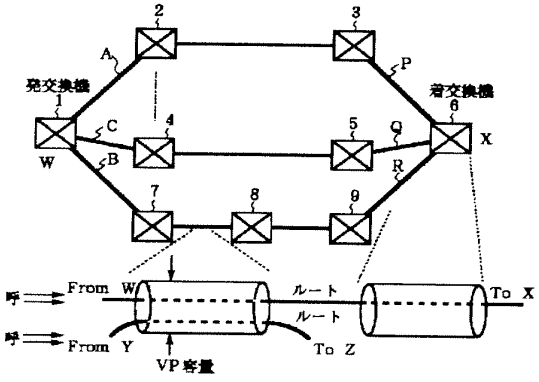
(54)【発明の名称】　ＡＴＭ通信網および故障復旧方法

(57)【要約】

【目的】　交換機の故障を前提とした故障復旧対策を行う。

【構成】　交換機の故障時に、着交換機から故障復旧メッセージセルを送出して交換機が自律分散的に情報を交換し、発交換機に網状態を通知してルートの切替えを行い、交換機故障によるルート障害がＶＣルートレベルにより復旧される。

【効果】　交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。このため交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。



1

【特許請求の範囲】

【請求項１】　複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にバーチャルパスが設定されるＡＴＭ通信網において、

前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、

前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたことを特徴とするＡＴＭ通信網。

【請求項２】　前記メッセージ領域には、経由する中継交換機の数を搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数を加算する手段を備えた請求項１記載のＡＴＭ通信網。

【請求項３】　前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出する請求項１または２記載のＡＴＭ通信網。

【請求項４】　前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えた請求項１ないし３のいずれかに記載のＡＴＭ通信網。

【請求項５】　加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択することを特徴とする故障復旧方法。

【請求項６】　前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項５記載の故障復旧方法を自律分散的に実行する方法。

【請求項７】　加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択することを特徴とする故障復旧の待機方法。

【請求項８】　前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項７記載の故障復旧の待機方法を自律分散的に実行する方法。

【請求項９】　一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送出することを特徴とする故障復旧方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はＡＴＭ（非同期転送モード）通信網に利用する。特に、伝送路に介挿された通信装置の故障に対する故障復旧技術に関する。

【０００２】

【従来の技術】ＡＴＭ通信網は、物理的には、バーチャルチャネル(Virtual Channel: 以下ＶＣという）を単位としてスイッチングを行うバーチャルチャネルハンドラ(Virtual Channel Handler、交換機）と、バーチャルパス(Virtual Path:以下ＶＰという）を単位として情報転送の方路を設定するバーチャルパスハンドラ(Virtual Path Handler:ＶＰＨ、またはクロスコネクト、ＸＣ）とが伝送路により接続されて構成される。理論的には、ＶＣＨ間がＶＰにより接続され、ＶＰは零または１以上のＶＰＨを経由してＶＣＨで終端される。

【０００３】従来の通信装置の故障に対する故障復旧方法を図１２に示す。図１２は従来の故障復旧方法の概念を示す図である。従来の故障復旧方法には、図１２（ｂ）に示す物理レベルの故障復旧と図１２（ａ）に示すＶＰレベルの故障復旧がある。物理レベルの故障復旧を実現するためには、物理伝送路リンクを２重化しておき、一方を現用系、もう一方を予備系としておく。もし、現用系の通信装置に故障が発生したら、現用系から予備系に切替えられ、故障が復旧される。しかし、物理レベルの故障復旧では、常時、物理伝送路リンクを２重化しておかなければならず、網リソースを効率的に利用できないという問題がある。

【０００４】そこで、ＡＴＭ通信網の特徴であるＶＰの概念を適用したＶＰレベルの故障復旧方法がある。ＶＰは、情報転送単位であるセルに付与されたヘッダ領域中

のＶＰＩ(Virtual Path Identifier) により識別され、ＶＰＨにおいては、パスの接続先を記述したパス接続（ルーティング）テーブルにより経路が設定される。ＶＰレベルの故障復旧は、ＶＰの経路と容量が独立に設定できることを利用して、故障により切断されたＶＰを、故障箇所を迂回して新たに形成されたＶＰに切り換えることにより実現される。特に、故障発生時に、ＡＴＭ通信網を一元的に監視している集中局があらかじめ設定された迂回パス情報に基づき網内の各ノード（ＶＣＨ、ＶＰＨその他）に対して制御を行う方式を集中制御方式、各ノードが自律分散的に迂回パスを探索・復旧させる故障復旧方式をセルフヒーリング方式という。ＶＰレベルの故障復旧では、物理レベルの故障復旧と比較して、伝送路の網リソースを効率良く利用できる点や網の変化に柔軟に対応できる点で、優れている。したがって、従来の故障復旧方法として、物理レベルとＶＰレベルとを組み合わせた故障復旧方法が適用されている。

【０００５】

【発明が解決しようとする課題】しかし、従来の物理レベルとＶＰレベルのみの故障復旧方法では、ＶＣＨ（交換機）の故障は前提とされないため、高信頼な交換機が必要である。また、複数のメディアが混在するＡＴＭ通信網においては、メディア毎に要求される信頼度が異なるが、最も高く要求される信頼度に合わせて信頼性を満足するように交換機が設計されており、あまり、信頼度を要求しないメディアに対しては、冗長であった。図１３は高信頼化された交換機の概念図であるが、高信頼化された交換機では、図１３のようにスイッチ部、Ｉ／Ｏ部、およびＣＰＵ部が二重化されており、さらに、これらのユニットはクロスルートで結合されている。このような２重化によって高信頼化された交換機のコストは、単純な構成を持つ交換機のコストと比べ、４倍から６倍程度高くなってしまう。

【０００６】本発明は、このような背景に行われたものであり、交換機の故障を前提とした故障復旧対策を行うことができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、交換機のコストを低減することができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】単純な構成を持つ交換機を通信装置として適用するとき、交換機の故障時のＶＣルート障害を敏速に復旧する必要がある。そこで、本発明は、交換機の故障時にＶＣルート障害を敏速に復旧する方法を提供することを特徴とする。その方法としては交換機の故障時に、発着交換機間の現用ルート障害を復旧するために着交換機から故障復旧メッセージセルを送出し、交換機が自律分散的に情報を交換して発交換機に網状態を通知し、ルートの切替えを行い、交換機故障によるルート障害がＶＣルートレベルにより復旧される。これをＶＣルートレベルのセルフヒーリングという。

【０００８】従来技術では、ＶＰレベルのセルフヒーリングが行われていたが、本発明の特徴とするところは、ＶＣルートレベルのセルフヒーリングによって、交換機故障時のＶＣルート障害を復旧することができることにある。

【０００９】すなわち、本発明の第一の観点は、複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にバーチャルパスが設定されるＡＴＭ通信網である。

【００１０】ここで、本発明の特徴とするところは、前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたところにある。

【００１１】前記メッセージ領域には、経由する中継交換機の数を搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数を加算する手段を備えることが望ましい。

【００１２】前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出することが望ましい。

【００１３】前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えることが望ましい。

【００１４】本発明の第二の観点は故障復旧方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞ

れ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択するところにある。

【００１５】この故障復旧方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧方法を自律分散的に実行することが特徴である。

【００１６】本発明の第三の観点は故障復旧待機方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択するところにある。

【００１７】この故障復旧待機方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧待機方法を自律分散的に実行することが特徴である。

【００１８】本発明の第四の観点は故障復旧方法であり、その特徴とするところは、一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送出するところにある。

【００１９】この明細書では、加入者交換機と中継交換機とをあたかも異なる通信装置であるかのような表現を用いているが、これは説明をわかりやすくするためのものであり、同一のハードウェア構成の通信装置により実現することができる。

【００２０】

【作用】本発明の方法では、ＶＣルートレベルのセルフヒーリングによって、着交換機から故障復旧メッセージセルを送出して、交換機が自律分散的に情報を交換し、発交換機に網状態を通知し、ルートの切替えを行い、交換機故障時のＶＣルート障害を復旧することができるので、高信頼な交換機を使用する必然性がなくなり、単純な構成を持つ交換機を使用することにより、コスト削減が図られる。

【００２１】着交換機が送出する故障復旧メッセージセルはバーチャルパスを介して発交換機に到達する。このバーチャルパスは、予備のバーチャルパスとなりうるバーチャルパスとしてあらかじめ定められているバーチャルパスでもよいし、故障が認識されていない不特定のバーチャルパスでもよい。

【００２２】故障復旧メッセージセルは、着交換機から発交換機に到達する間に通過するバーチャルパスの空帯域情報を収集する。言い方を替えると、通過するバーチャルパスに介挿されている中継交換機は、故障復旧メッセージセルを通過させるときに、自己の中継交換機における空帯域情報を故障復旧メッセージセルの例えばメッセージ領域に搭載する。また、同時に通過した中継交換機の数も情報として搭載する。発交換機では、空帯域情報および通過した中継交換機の数の情報を参考にして予備のバーチャルパスとして最適なバーチャルパスを選択する。以降は、このバーチャルパスにバーチャルチャネルを設定して通信を再開する。

【００２３】故障復旧メッセージセルの送出は現用のバーチャルパスあるいは現用のバーチャルパス上の中継交換機に何らかの故障が認識されたときに行われるように制御してもよいし、あるいは、平常時にも故障復旧メッセージセルを送出し、常時、予備のバーチャルパスとして最適なバーチャルパス候補を選択しておくこともよい。

【００２４】本発明では、このような故障復旧制御をＡＴＭ通信網に含まれる各交換機が自律分散に行うことを主要な特徴としている。

【００２５】

【実施例】

（第一実施例）本発明第一実施例の構成を図１～図５を参照して説明する。図１は本発明の全体構成図である。図２は着交換機の要部ブロック構成図である。図３は故障復旧メッセージセルの構成図である。図４は中継交換機の要部ブロック構成図である。図５は発交換機の要部ブロック構成図である。

【００２６】本発明は、加入者交換機である発交換機１および着交換機６と、この発交換機１および着交換機６相互間を接続する物理伝送路Ｐ～Ｒと、この物理伝送路Ｐ～Ｒに介挿される中継交換機２、３、４、５、７、８、９とを備え、発交換機１および着交換機６の間にバーチャルパスが設定されるＡＴＭ通信網である。

【００２７】ここで、本発明の特徴とするところは、着交換機６には、バーチャルパスに故障復旧メッセージセルを送出する手段としての故障復旧メッセージセル生成部１２を備え、この故障復旧メッセージセルは、宛先領域Ｈおよびメッセージ領域Ｍを有し、その宛先領域Ｈに一以上の中継交換機２、３、４、５、７、８、９を経由して発交換機１に到達するための情報が搭載され、中継交換機２、３、４、５、７、８、９には、経由する故障復旧メッセージセルのメッセージ領域Ｍにその中継交換機２、３、４、５、７、８、９の空帯域情報を搭載させる手段としての故障復旧メッセージセル情報搭載部１４

を備えたところにある。

【００２８】本発明実施例では、説明をわかりやすくするために、発交換機１、着交換機６、中継交換機２、３、４、５、７、８、９をそれぞれあたかも異なるハードウェア構成を備えた通信装置であるかのように表現するが、これらは各機能を共通に備えた一つの通信装置として実現することができる。

【００２９】メッセージ領域Ｍには、経由する中継交換機２、３、４、５、７、８、９の数を搭載するホップカウンタ領域ＨＣが設けられ、中継交換機２、３、４、５、７、８、９には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域ＨＣに搭載された中継交換機の数を加算する手段を故障復旧メッセージセル情報搭載部１４に併せて備えている。

【００３０】発交換機１および着交換機６には、バーチャルパスに介挿された中継交換機２、３、４、５、７、８、９の故障の可能性を認識する手段としての故障検出部１０を備え、故障復旧メッセージセル生成部１２は、この故障検出部１０の出力にしたがって故障復旧メッセージセルを送出する。

【００３１】発交換機１には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段としての予備ルート設定部１６を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を予備ルート設定部１６に併せて備えている。

【００３２】ＶＣルートは発交換機１から１つ以上のＶＰを経て着交換機６に設定される。発交換機１において、呼が発生したときに、複数のＶＣルートの中からあるルートを選択して、呼受付判定(Connection Admission Control:CAC)を行う。例えば、ルートの選択は、ランダムに選択される。ＣＡＣによって、呼が受付けられたら、ＶＣコネクションを設定し、呼が受付けられなければ呼損となる。

【００３３】次に、本発明第一実施例の動作を図６を参照して説明する。図６は本発明第一実施例の動作を説明するための図である。図６に示すように、１つの現用ルートのみに着目し、中継交換機５に故障が発生したときの、本発明第一実施例の故障回復方法を示す。発交換機１と着交換機６との間に現用ルート（１→４→５→６）が２つの中継交換機を介して設定されており、現用ルートは現時点でＢ〔Ｍｂｐｓ〕の帯域を使用している。

【００３４】この現用ルートに対して、ＣＡＣの後に呼が受付けられ、ＶＣコネクションが設定されたり、切断されたりしている。この現用ルートの使用帯域は、例えば、発交換機１において、あるウィンドウサイズ内の現用ルートで使用されているセル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。

【００３５】ここで、ジャンピングウィンドウとは、ウィンドウ位置（観測位置）が一定周期でオーバーラップすることなく遷移する観測方法であり、スライディングウィンドウとは、ウィンドウ位置が一定周期でオーバーラップしながら徐々に遷移する観測方法である。ごく大まかにいうとジャンピングウィンドウは高速な観測が利点であり、スライディングウィンドウは正確な観測が利点である。

【００３６】故障により、現用ルートが使用不可能になることに備えて、複数の予備ルートを予め設定しておく、図６では、２つの予備ルート（ルートＰ：１→２→３→６、ルートＲ：１→７→８→９→６）が設定されている。故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機１および着交換機６が認識する。現用ルートに現時点で設定されていたＶＣコネクションの救済は行わないが、故障発生後に、新たに要求してくるＶＣの呼を最大限受付けられるように、迂回ルートを探索する。ここで、着交換機６は故障復旧メッセージセルを送出するセンダ、発交換機１は故障復旧メッセージセルを受取り予備ルートの中から切替えルートを選択するチューザとなる。着交換機（センダ）６は、予備ルートに対してその状態を調べるために、故障復旧メッセージセルを送出する。故障復旧メッセージセルは予備ルートＰおよびＲの経路に沿って、予備ルートＰおよびＲの経路上のＶＰの状態を調べる。ルートＲを例に上げて説明する。故障復旧メッセージセルのメッセージ領域Ｍにはペイロードとして、

（１）ホップカウンタＨＣ
（２）ホップリミットＨＬ
（３）ＶＰ未使用帯域の最小値b_{min}
（４）経路情報ＲＤ

が書込まれる。ホップリミットＨＬは、遅延条件その他を考慮して、予め設定されている。最小値b_{min}の値を∞としておき、最小値b_{min}の値は故障復旧メッセージセルに書込まれている。ルートＲを経由する故障復旧メッセージセルは、着交換機６から中継交換機９に送出され、中継交換機９では、

$b < b_{min}$

ならば、未使用ＶＰ帯域ｂの値をb_{min}とする。ｂは中継交換機９において、例えば、あるウィンドウサイズ内のＶＰ未使用帯域は、使用セル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。ホップカウンタＨＣは中継交換機９→８→７を経由する毎に、１つカウントアップされ、ホップリミットＨＬを超えない限り、さらに次の交換機に送出される。しかし、通常、予備ルートは、ホップリミットを超えないように予め設定されている。次の交換機８では、ｂ＝２であり、$b < b_{min}$なので、b_{min}＝２となる。同様に

故障復旧メッセージセル送出のプロセスを繰り返し、故障復旧メッセージセルは、発交換機１に到着する。また、予備ルートＰ上に送出された故障復旧メッセージセルＡも同様にして、発交換機１に到着する。発交換機１は、予備ルートＰまたはＲの中から、現用ルートの使用帯域Ｂや予備ルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、切替先のルートとして１つまたは複数選択する。図７は本発明第一実施例におけるルート切替状況を示す図であるが、図７の例では、予備ルートの中でルートＰが最もＶＰ未使用帯域の最小値が大きいので、ルートＰが切替先のルートとして選択され、故障復旧後はルートＰが現用ルートとして使用される。

【００３７】したがって、交換機の故障時に、故障復旧メッセージセルの送出により交換機が自律分散的に情報を交換し、ルートの切替えを行い、故障が復旧されるので、従来のような２重化された高信頼な交換機でなくても単純な構成を持つ交換機を用いることかできるため、交換機のコスト削減が図れる。

【００３８】（第二実施例）次に、本発明第二実施例を図８を参照して説明する。図８は本発明第二実施例の動作を説明するための図である。本発明第一実施例では、故障発生時に故障復旧メッセージセルを送出していたが、本発明第二実施例では、図８のように、通常時でも、着交換機（センダ）６からＲＭ(Resource Management) セルを送出して、予備ルートＰおよびＲの状態を監視しておく。ＲＭセルの動作は、本発明第一実施例の故障復旧メッセージセルの動作と同様である。発交換機（チューザ）１は、予備ルートＰまたはＲの中から、現用ルートの使用帯域Ｂや予備ルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、現用ルートの障害時に備えて、切替先のルートを決めておく。

【００３９】ここで、着交換機（センダ）６からＲＭセルは、定期的に送出され、ＲＭセルを受け取った発交換機（チューザ）１は、網状態に応じて切替先のルートを更新しておく。ＲＭセルの送出間隔は、網状態の変化の度合いから決定される。

【００４０】故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機１が認識する。現用ルートの障害を検知した発交換機１は、通常に現用ルート障害時に備えてあった切替先ルートに切替えられ、現用ルートとして使用される。

【００４１】したがって、通常時に、着交換機（センダ）６からＲＭ(Resource Management) セルを送出して、予備ルートの状態を監視して、現用ルートの障害時に備えて切替先ルートを決めておくことにより、故障復旧時間の短縮化が図れる。

【００４２】（第三実施例）次に、本発明第三実施例を図９を参照して説明する。図９は本発明第三実施例の動作を説明するための図である。本発明第一実施例では、予め予備ルートＰおよびＲを設定しておき、故障発生時に予備ルートＰおよびＲ上に故障復旧メッセージセルを送出していた。本発明第三実施例では、予め予備ルートＰおよびＲを設定しておかず、図９のようにフラッディング(Flooding)により故障復旧メッセージセルを送出し、発交換機１に到達した故障復旧メッセージセルにしたがって発交換機１が予備ルートを選択する。

【００４３】ここで、フラッディングとは、“Ｆｌｏｏｄ”すなわち、あたかも“洪水”のように不特定方向に対してセルを送出させるというイメージに基づいた用語であり、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出するという意味に用いる。

【００４４】故障復旧メッセージセルのペイロードには、本発明第一実施例で説明したように、

（１）ホップカウンタＨＣ
（２）ホップリミットＨＬ
（３）ＶＰ未使用帯域の最小値b_{min}
（４）経路情報ＲＤ

が書込まれる。ホップリミットＨＬは、遅延条件その他を考慮して、予め設定されている。最小値b_{min}の値を∞としておき、最小値b_{min}の値は故障復旧メッセージセルに書込まれている。

【００４５】まず、着交換機（センダ）６は、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出する。故障復旧メッセージセルを受信した交換機は、$b < b_{min}$ ならば、未使用ＶＰ帯域ｂの値をb_{min}とする。ｂは交換機において、例えば、あるウィンドウサイズ内のＶＰ未使用帯域は、使用セル数を観測することによって求められる。経由した交換機の情報が経路情報として書込まれる。ホップカウンタＨＣは交換機を経由する毎に、１つカウントアップされ、もし、ホップリミットＨＬを超えているか、または、経路情報ＲＤにより既に同じ交換機を経由していれば、故障復旧メッセージセルは廃棄される。そうでなければ、さらに、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出し、故障復旧メッセージセルを受信した交換機は同様の動作を繰り返し、故障復旧メッセージは、発交換機に到着する。

【００４６】発交換機（チューザ）１は、到着した故障復旧メッセージセルから現用ルートの使用帯域Ｂや到着した故障復旧メッセージセルを基にしたルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、切替先のルートとして１つまたは複数選択する。

【００４７】したがって、予め予備ルートを設定しておくことなく、フラッディングにより故障復旧メッセージセルを送出し、発交換機１に故障復旧メッセージセルを到着させることにより、網トポロジやＶＰ容量その他の変化に柔軟に対応した故障復旧を行うことができる。

【００４８】本発明の故障復旧方法による故障復旧概念を図１０および図１１に示す。図１０は本発明の故障復旧方法の概念を示す図である。図１１は本発明の故障復旧方法を適用したＡＴＭ通信網の概念図である。図１０（ｂ）および（ｃ）は、従来から知られているＶＰレベルおよび物理レベルの故障復旧概念である。本発明では図１０（ａ）に示すように、ＶＣルートレベルの故障復旧を行うことにより図１１に示すように、高信頼性の交換機を用いることなくＡＴＭ通信網を構成することができる。

【００４９】

【発明の効果】以上説明したように、本発明によれば、交換機の故障を前提とした故障復旧制御を行うことができる。このため、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。したがって、交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。

【図面の簡単な説明】

【図１】本発明の全体構成図。

【図２】着交換機の要部ブロック構成図。

【図３】故障復旧メッセージセルの構成図。

【図４】中継交換機の要部ブロック構成図。

【図５】発交換機の要部ブロック構成図。

【図６】本発明第一実施例の動作を説明するための図。

【図７】本発明第一実施例におけるルート切替状況を示す図。

【図８】本発明第二実施例の動作を説明するための図。

【図９】本発明第三実施例の動作を説明するための図。

【図１０】本発明の故障復旧方法の概念を示す図。

【図１１】本発明の故障復旧方法を適用したＡＴＭ通信網の概念図。

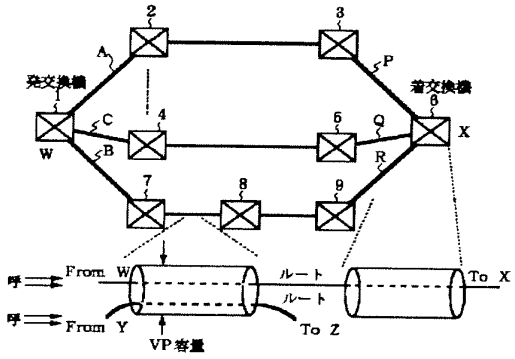
【図１２】従来の故障復旧方法の概念を示す図。

【図１３】高信頼化された交換機の概念図。

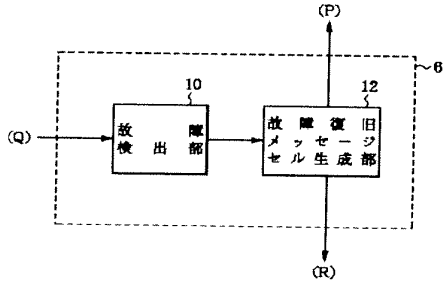
【符号の説明】

１　発交換機
２～５、７～９　中継交換機
６　着交換機
１０　故障検出部
１２　故障復旧メッセージセル生成部
１４　故障復旧メッセージセル情報搭載部
１６　予備ルート設定部
Ｈ　宛先領域
ＨＣ　ホップカウンタ
ＨＬ　ホップリミット
Ｍ　メッセージ領域
ＲＤ　経路情報
b_{min}　最小値
Ｐ、Ｑ、Ｒ　ルート

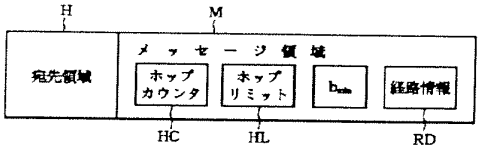
【図１】



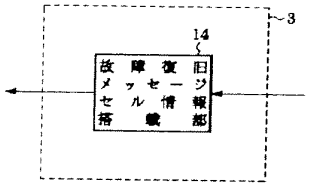
【図２】



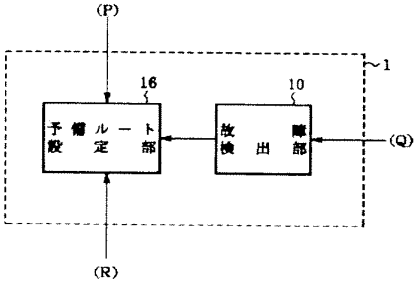
【図３】



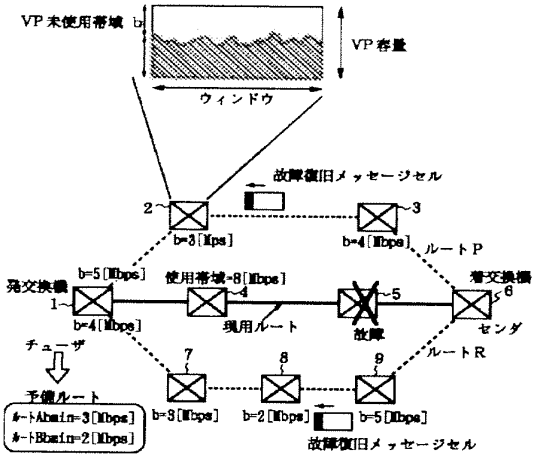
【図４】



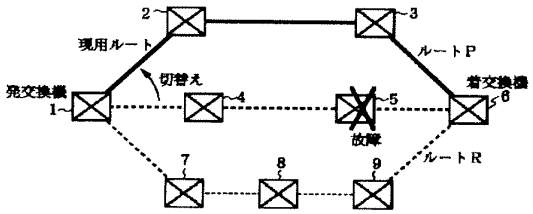
【図５】



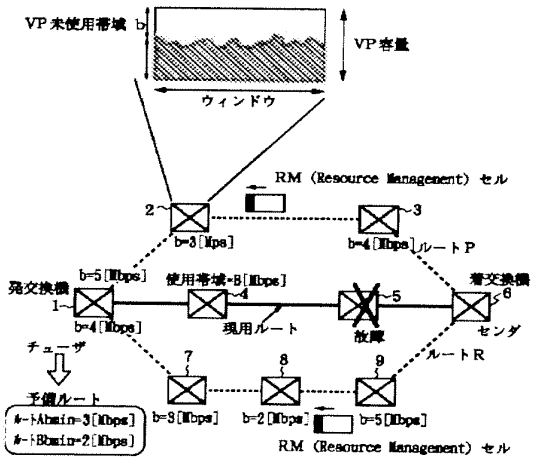
【図６】



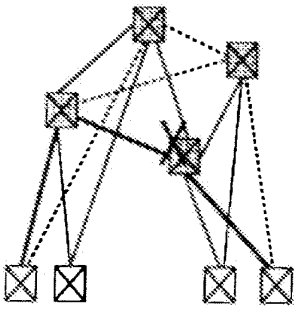
【図７】



【図８】

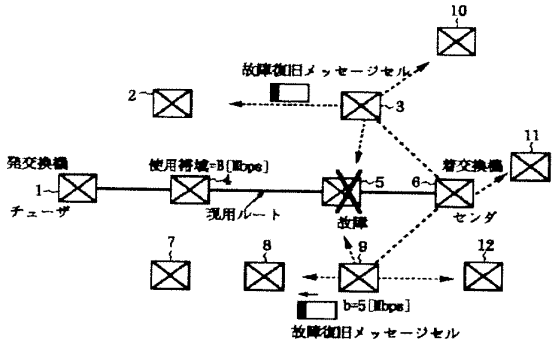


【図１１】

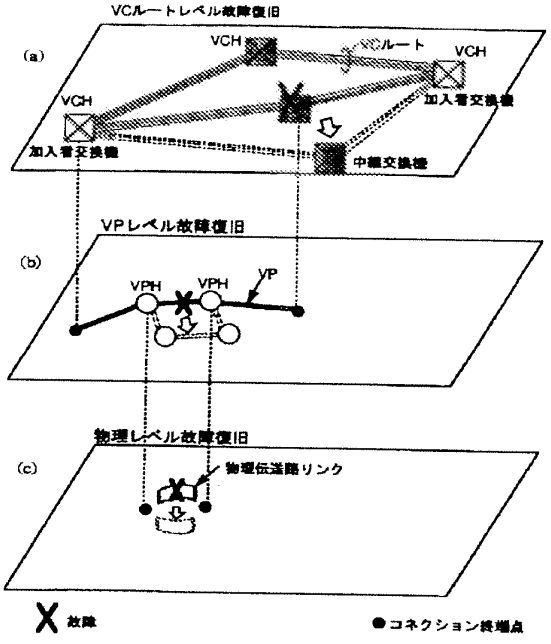


交換機のダウンサイジング化

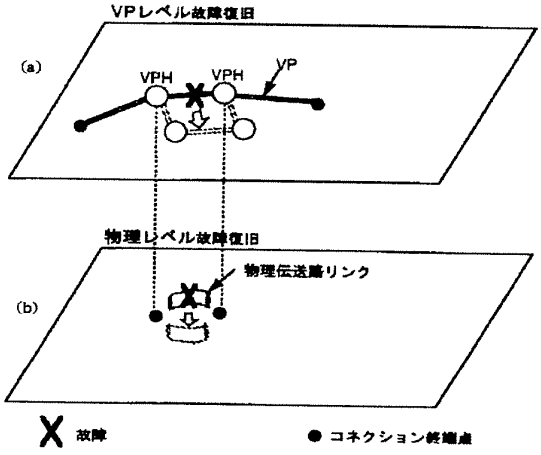
【図９】



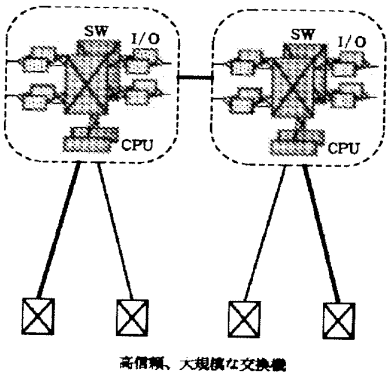
【図１０】



【図１２】



【図１３】



Electronic Patent Application Fee Transmittal

Application Number:	11840560
Filing Date:	17-Aug-2007
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royaee/Melissa Molchan
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2

Filed as Large Entity

Utility under 35 USC 111(a) 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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	7341556
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Melissa Molchan
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	02-APR-2010
Filing Date:	17-AUG-2007
Time Stamp:	12:28:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	7639
Deposit Account	501133
Authorized User	

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 (SB/08)	0063.pdf	84456 86dc39f0b7fa035d38f5ef10528f71f7b2333efc	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2		jp.pdf	2159740 c1f5c3a6d9721eec83fbef0087e759d448898a69	yes	53

Multipart Description/PDF files in .zip description

Document Description	Start	End
Foreign Reference	1	6
Foreign Reference	7	23
Foreign Reference	24	30
Foreign Reference	31	53

Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	NPL Documents	Davies.pdf	572855 570f1932ebcd625d840e44ae1e6c1c78603cf33c	no	15
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	NPL Documents	Feng.pdf	215626 58bf05014b12aa13483ab383b6d7b0c529b2e711	no	4
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	30430 b0c22ec434ceb8287316817ab0e9b2f311a59dec	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	3063107

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/840,560	08/17/2007	Victor Larson	077580-0063 (VRNK-1CP3CN2	1537

23630 7590 03/19/2010

MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

NOTIFICATION DATE	DELIVERY MODE
03/19/2010	ELECTRONIC

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

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

BostonIPDocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	11/840,560	LARSON ET AL.	
	Examiner	Art Unit	
	Krisna Lim	2453	

-- 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 *17 August 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) *1-3* 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) *1-3* 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:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ 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: _____.

Claims 1-3 are presented for examination.

The disclosure is objected to because of the following informalities:

(a) On page 1, the text of the first paragraph should be updated with the current status of the cited applications such as U.S. Patent Application Serial No., a filing date, U.S. Patent No., and the issued date. Appropriate correction is required.

The information disclosure statement filed 5/19/2009 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance. It has been placed in the application file, but the information referred to therein has not been considered.

Claim 1 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

At line 3, it is unclear from where a query message is sent. At line 4, it is unclear from where the query message is requesting a secure computer network address. It is unclear how a portal authenticates a query. Moreover, the interrelationship or inter-function between a portal and a domain name database is unclear.

Claims 2-3 rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: providing (sending/receiving) a query for a secure computer network address, authenticating the query, and providing an indication that the apparatus supports a secure network connections, etc.

Claims 2-3 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: providing (sending/receiving) a query for a secure computer network address, authenticating the query, and providing an indication that the apparatus supports a secure network connections, etc.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 2 is rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either an undue breath (i.e., a single means claim that does not appear in combination with another element) asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory

double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-3 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,418,504. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a system for providing a secure domain name service over a computer network comprising: a portal (domain name service system) connected to a computer network, the portal authenticating a query for a secure computer network address (an indication of the support of establishing a secure communication link); and a domain name database (to store a plurality of domain names) connected to the computer network through the portal, the domain name database storing secure computer network addresses for the computer network. The different is the broadest interpretation of the claimed languages.

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.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-3 are rejected under 35 U.S.C. §102(e) as being anticipated by Shrader [U.S. Patent No. 5,864,666].

Shrader anticipates the invention substantially as claimed. Taking claims 1-3 as an exemplary claim, the reference anticipates a system for providing a secure domain name service over a computer network (i.e., see the abstract, col. 4 (lines 11-23, 47-54), and col. 5 (lines 1-12)), comprising: a portal connected to a computer network, the portal authenticating a query (i.e., see col. 4, line 51) for a secure computer network address; and a domain name database (DB is inherent in any computer system) connected to the computer network through the portal, the domain name database storing secure computer network addresses for the computer network, wherein a computer network address having a top level domain reserved for secure network connections (i.e., see permit 9.24.104.241, etc. of Fig. 7).

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The references are cited in the Form PTO-892 for the applicant's review.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter.

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).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas, can be reached on 571-272-6776. 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).

KI

March 14, 2010

/Krisna Lim/
Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 11/840,560	Applicant(s)/Patent Under Reexamination LARSON ET AL.	
	Examiner Krisna Lim	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,864,666	01-1999	Shrader, Theodore Jack London	726/15
*	B	US-6,081,900	06-2000	Subramaniam et al.	726/19
	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.	Applicant(s)/Patent Under Reexamination
	11840560	LARSON ET AL.
	Examiner	**Art Unit**
	Krisna Lim	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/14/2010								
	1	✓								
	2	✓								
	3	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11840560	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

SEARCHED			
Class	Subclass	Date	Examiner
709	226, 221	3/14/2010	kl
726	15	3/14/2010	kl

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, Inventors	3/14/2010	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 1537

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/840,560	08/17/2007 **RULE**	709	2453	077580-0063 (VRNK-1CP3CN2

APPLICANTS

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

**** CONTINUING DATA **************************

This application is a CON of 10/714,849 11/18/2003 PAT 7,418,504
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

**** FOREIGN APPLICATIONS **************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/29/2007

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /KRISNA LIM/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		VA	40	3	3

ADDRESS

MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775
UNITED STATES

TITLE

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

FILING FEE RECEIVED		
1130	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/840,560
Filing Date	August 17, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	VU, Kim Y.
Docket Number	077580-0063 (VRNK-1CP3CN2)

Sheet	1	of	1

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1020	US	7,461,334	12/02/08	Lu, et al.	
	A1021	US	7,353,841	04/08/08	Kono, et al.	
	A1022	US	7,188,175	03/06/07	McKeeth, James A.	
	A1023	US	7,167,904	01/23/07	Devarajan, et al.	
	A1024	US	7,039,713	05/02/06	Van Gunter, et al.	
	A1025	US	6,757,740	06/29/04	Parekh, et al.	
	A1026	US	6,752,166	06/22/04	Lull, et al.	
	A1027	US	6,687,746	02/03/04	Shuster, et al.	
	A1028	US	6,338,082	01/08/02	Schneider, Eric	
	A1029	US	6,333,272	12/25/01	McMillin, et al.	
	A1030	US	6,314,463	11/06/01	Abbott, et al.	
	A1031	US	6,298,341	10/02/01	Mann, et al.	
	A1032	US	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1033	US	6,199,112	03/06/04	Wilson, Stephen K.	
	A1034	US	6,052,788	04/18/00	Wesinger, et al	
	A1035	US	2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1036	US	2001/0049741	12/06/01	Skene, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	C1241	P. Mockapetris, "Domain Names – Implementation and Specification," Network Working Group, RFC 1035 (November 1987)	
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

BST99 1638591-1.077580.0063

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	762	(secure same domain same name same service)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/14 18:01
L2	0	l1 and (computer same network same addres)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/14 18:01
L3	319	l1 and (computer same network same address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/14 18:01
L4	296	l3 and (portal authenticat$4 query)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/14 18:02
L5	20	l4 and @ad<="20000215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/14 18:02
S1	59654	(network adj4 interface).ti, ab,clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/09 14:44
S2	1046	S1 and (network same utilization same information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/03/09 14:45

EAST Search History (Interference)

<This search history is empty>

3/14/10 6:08:36 PM
C:\Documents and Settings\klim\My Documents\EAST\Workspaces\11685142.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

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	5384848		1995-01-00	Kikuchi	
	2	6223287		2001-04-00	Douglas, et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS	Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	03/14/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11840560
Filing Date	2007-08-17
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-063(VRNK-1CP3CN2)

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	5303302		1994-04-12	Burrows	
	2	5629984		1997-05-13	McManis	

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11840560 11840560 - GAU: 2453
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	03/14/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

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	5771239		1998-06-23	Moroney, et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11840560 11840560 - GAU: 2453
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

	1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	03/14/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/840,560
Filing Date	August 17, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	VU, Kim Y.
Docket Number	077580-0063 (VRNK-1CP3CN2)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

*EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	
	A1019	6,246,670	06/12/2001	Karlsson, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER /Krisna Lim/ DATE CONSIDERED 03/14/2010

*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.

(1) ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	2	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(2)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	3	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(3)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	4	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(4)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	5	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(5)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	6	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER /Krisna Lim/	DATE CONSIDERED 03/14/2010

*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.

(6)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	7	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(7)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	8	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(8)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	9	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(9)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	10	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

.EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
.	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(10)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	11	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
.	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(11)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	12	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
EXAMINER /Krisna Lim/		DATE CONSIDERED 03/14/2010	

*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.

(12)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	13	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(13)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	14	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(14)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	15	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(15)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	16	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(16)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	17	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.
BST99 1620066-1.077580.0063

(17)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

COPY 5-20-09

11840560 - GAU: 2453 JFW

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/840,560
Filing Date	August 17, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	VU, Kim Y.
Docket Number	077580-0063 (VRNK-1CP3CN2)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	
	A1019	6,246,670	06/12/2001	Karlsson, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER /Krisna Lim/ DATE CONSIDERED 03/14/2010

*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.

(1)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	2	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(2)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	3	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(3)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	4	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

(4)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	5	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp— Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

(5)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	6	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER /Krisna Lim/	DATE CONSIDERED 03/14/2010

*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.

(6)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	7	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

ALL REFERENCES CONSIDERED (7) EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	8	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 03/14/2010

*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.

(8)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	9	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

(9)

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	10	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	11	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				Complete if Known	
				Application Number	11/840,560
				Filing Date	August 17, 2007
				First Named Inventor	Victor Larson
				Art Unit	2157
				Examiner Name	VU, Kim Y.
Sheet	12	of	17	Docket Number	077580-0063 (VRNK-1CP3CN2)

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
EXAMINER /Krisna Lim/		DATE CONSIDERED 03/14/2010	

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

(12)

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	13	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	14	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	15	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/14/2010

*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.

ALL REFERENCES CONSIDERED, EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	16	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.

ALL REFERENCES CONSIDERED, EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/840,560**
				Filing Date	**August 17, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**VU, Kim Y.**
Sheet	17	of	17	Docket Number	**077580-0063 (VRNK-1CP3CN2)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S 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, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/14/2010

*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.
BST99 1620066-1.077580.0063

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./