(51) International Patent Classification: H04L 29/12, 12/28, 12/46

(21) International Application Number: PCT/US00/16432

(22) International Filing Date: 14 June 2000 (14.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/140,906 23 June 1999 (23.06.1999) US

(71) Applicant: AT & T WIRELESS SERVICES, INC. [US/US]; 14520 NE 87th Street, Redmond, WA 98052 (US).

(72) Inventors: CHIEN, Herman; 17706 NE 134th Place, Redmond, WA 98052 (US). FUNG, Kevin; 3800 South Horton, Seattle, WA 98144 (US). HONG, Liang; 1022 224th Avenue NE, Redmond, WA 98053 (US). LEUCA, Illeana, A.; 11123 NE 37th Court, Bellevue, WA 98004

(74) Agent: DWORETSKY, Samuel, H; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).

(81) Designated States (national): BR, CA, MX.

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

(54) Title: REVERSE TUNNELING METHODS AND APPARATUS FOR USE WITH PRIVATE COMPUTER NETWORKS

(57) Abstract: Privately addressed computer devices in a private computer network are enabled to communicate over the Internet without acquiring public IP addresses. A computer system or network configuration includes a private computer network having one or more computer devices, each associated with a private IP address, and a tunnel server with an access port coupled to receive tunnel requests from the one or more computer devices and a resource port coupled to a service provider of the Internet. The tunnel server is operative to open a tunnel through the private computer network between the computer device and the tunnel server to support communication by the computer device over the Internet. In one particular application, the private computer network includes a fixed wireless system providing wireless communications between the computer devices and the tunnel server.
REVERSE TUNNELING METHODS AND APPARATUS
FOR USE WITH PRIVATE COMPUTER NETWORKS

RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 60/140, 906, filed June 23, 1999, and entitled "Method and Procedure for Transporting TCP/IP Datagrams Over the PWAN to Other Data Networks," which is incorporated herein in its entirety.

The following application, assigned to the Assignee of the current invention, and being filed concurrently, contains material related to the subject matter of this application, and is incorporated herein by reference:

Attorney Docket: 1999-0340 (STG166), by H. Chien et al., entitled "Methods and Apparatus for Use in Reducing Traffic Over a Communication Link Used by a Computer Network," Serial No. ________, filed ________.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to the fields of private and public computer network communication involving "tunnels" and virtual private networks (VPNs).

2. Description of the Related Art

The Internet is a dramatically different computer network than when it was first established in the early 1980s. The Internet has entered the public consciousness as the world's largest public data network, which is reflected by the tremendous popularity of the World Wide Web (WWW), the opportunities that businesses see in reaching customers from virtual storefronts, and the emergence of new types and methods of doing business.
Over the past few years, the Internet has experienced two major scaling issues as it has struggled to provide continuous and uninterrupted growth. One issue is the eventual exhaustion of the public IP address space; the other issue is the difficulty in routing traffic between the ever increasing number of networks on the Internet.

As is well-known, a computer device must be assigned a public IP address in order to communicate over the Internet. What was initially thought to be a large fixed number of public IP addresses allocated (4,294,967,296) is now considered to be quite limited. The address shortage problem is aggravated by the fact that portions of the IP address space have not been efficiently allocated. Also, the traditional model of classful addressing does not allow the address space to be used to its maximum potential. Some techniques, such as subnetting, have helped the address shortage problem but will not solve the problem. Private IP addresses are available, but only for internal private communication (e.g., within private computer networks).

Generally unrelated to the public IP address problem is the use of virtual private networks (VPNs) and its associated "tunneling" methods. A VPN allows the security, performance, availability, and multiprotocol support of a private computer network over the Internet. VPNs enjoy security via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of the Internet. One of the underlying technologies of VPNs is IP tunneling. In general, tunneling involves transmitting data structured in one protocol format within the format of another protocol. IP tunneling involves carrying a foreign protocol within a TCP/IP packet. Popular tunneling software includes Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer Two Forwarding (L2F).

Referring to FIG. 1, a computer system 100 which facilities prior art VPN and IP tunneling techniques is shown. Computer system 100 includes a plurality of personal computers (PCs) 102 which communicate with an Internet Service Provider (ISP) 104 for access to the Internet 106. The plurality of PCs 102 includes a PC 108, a PC 110, and a PC 112, which are not associated
with any private computer network and use public IP addresses. Computer system 100 also includes a private computer network 116 which communicates with an ISP 114 for access to the Internet 106. Private computer network 116 includes a plurality of private network devices 118, which use public IP addresses assigned by ISP 104, and a Network Access Server (NAS) 120 having IP tunneling software. Private network devices 118 may include a PC 122, a server 124, and a database 126. NAS 120 has an access port coupled to ISP 114 and a resource port coupled to the private network devices 118.

If PC 122 of private computer network 116 wishes to communicate via the Internet 106, access is allowed where no IP tunnel is established. Typically, appropriate public/private addresses are selected from a lookup table during communications; addresses are swapped and packets are therefore modified. These methods are based on the Network Address Translation (NAT) standard. Proxy servers, which may be Web servers, are similarly utilized to transfer information requests and return information between a private and public network.

If, on the other hand, PC 112 wishes to communicate with server 124 of private computer network 116, it sends a request to NAS 120 over the Internet 106. In response, NAS 120 executes appropriate conventional functions (e.g., authentication) to grant access to private computer network 116. NAS 120 establishes an IP tunnel 128 (represented by dashed lines in FIG. 1) for communication, with termination points at PC 112 and NAS 120, and assigns a public IP address to PC 112 for such communication.

For outbound communications (from NAS 120 over Internet 106 to PC 112), tunnel operation at NAS 120 involves wrapping the private IP addresses with the appropriate public IP addresses for communication over the Internet 106; tunnel operation for PC 112 involves unwrapping the public IP addresses to reveal the underlying private IP addresses. For inbound communications (from PC 112 over Internet 106 to NAS 120), tunnel operation for PC 112 involves wrapping the private IP addresses with public IP addresses for communication over the Internet 106; tunnel operation at NAS 120 involves
unwrapping the private IP addresses from within the public IP addresses for communication within private communication network 116. In addition, IP tunnel 128 typically involves encryption of the private protocol within the public IP protocol.

As described above, VPNs and IP tunnels provide security and performance of a private computer network over the Internet for PCs accessing the private computer network. Tunneling techniques, however, are not known to be used in connection with PCs of a private computer network for accessing resources via the Internet. What are needed are methods and apparatus to facilitate the use of private IP addresses for computer devices in a private computer network while allowing the computer devices to communicate over the Internet.

**SUMMARY OF THE INVENTION**

"Reverse tunneling" methods and apparatus for use with private computer networks are utilized to mitigate the problems described above. Since private address space is relatively large in comparison to public address space, and the demand for access to the Internet is high, the present invention provides a clever and fitting solution to both of these needs. As an additional benefit, full-time connectivity to a private network with unique content is provided with sufficient security.

More particularly, an inventive computer system is configured to facilitate the use of private IP addresses for computer devices in a private computer network while allowing the computer devices to communicate over the Internet. The computer system configuration includes a private computer network having computer devices associated with private IP addresses; a tunnel server; an access port of the tunnel server coupled to receive tunnel requests from the computer devices; and a resource port of the tunnel server coupled to a service provider of the Internet. The tunnel server is operative to facilitate a tunnel between the computer device and the tunnel server to facilitate communication between the computer device over the public
computer network. In a particular application, the private computer network includes a fixed wireless system which provides wireless communication between the computer devices and the tunnel server.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The nature, objects and advantages of the invention will become more apparent to those skilled in the art after considering the following detailed description in connection with the accompanying drawings, in which like reference numerals designate like parts throughout, wherein:

**FIG. 1** is an illustrative representation of a conventional computer system involving both public and private computer networks;

**FIG. 2** is an illustrative representation of a computer system involving both public and private computer networks and inventive aspects as described herein;

**FIG. 3** is an illustrative representation of a computer system involving both public and private computer networks and inventive aspects as described herein, where the private computer network involves a fixed wireless system;

**FIG. 4** is a flowchart describing a method of reverse tunneling in private computer networks;

**FIG. 5** is an illustrative representation of more detailed structure and functionality in the fixed wireless system of FIG. 3;

**FIG. 6** is an illustrative representation of more detailed structure and functionality of a service site of the fixed wireless system;
FIG. 7 is an illustrative representation of a first embodiment of a computer system with more detailed structure and functionality;

FIG. 8 is an illustrative representation of a second embodiment of a computer system with more detailed structure and functionality;

FIG. 9 is an illustrative representation of a third embodiment of a computer system with more detailed structure and functionality;

FIG. 10 is an illustrative representation of a fourth embodiment of a computer system with more detailed structure and functionality; and

FIGS. 11A and 11B together form is a process flow diagram of a method of reverse tunneling in a private computer network.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

What has been invented facilitates the ability of privately addressed devices in a private network to communicate over a public computer network. Since private address space is required to be relatively large in comparison to public address space, and since the demand for access to public networks is high, the present invention provides a clever and fitting solution to both of these needs. As an additional benefit, full-time connectivity to a private network with unique content is provided with sufficient security.

Broadly, a server configuration includes a tunnel server having an access port coupled to receive tunnel requests from devices such as computers within the private network, which may be a private computer network, and a resource port coupled to a service provider of a public network. In this regard, a "tunnel request" is a request to the tunnel server from a privately addressed device on the private network for the tunnel server to provide or open a tunnel between the device and the tunnel server through or in the private network. The tunnel server is operative to provide or open a tunnel
between the device and the tunnel server to facilitate communications between the device and another device which is publicly addressed and is on the public network. The public network is preferably a wide area network (WAN) or the Internet. The private addresses may include, for example, private addresses specified by a Request For Comments (RFC) standard. Such private addresses are not routable on the public network. As will be described in the detailed applications, the private network may include a fixed wireless system.

The unique method of the invention includes the steps of receiving, at an access port of a tunnel server, a tunnel request from a privately addressed computer device of a private computer network; facilitating creation of a tunnel through or in the private computer network, between the tunnel server and the computer device in response to the tunnel request; and facilitating, at the tunnel server with use of the tunnel, communication between the computer device and a service provider of a public computer network. Again, the public computer network is preferably a WAN or the Internet, and the private addresses may include private addresses specified by a Request For Comments (RFC) standard that are not routable on the public computer network. The private computer network may include a fixed wireless system.

Other unique methods involve the steps of receiving, at a tunnel server from a computer device of a private computer network, privately-addressed IP packet information; unwrapping, at the tunnel server, the privately-addressed IP packet information to reveal publicly-addressed IP packet information; and sending, from the tunnel server over a public computer network, the publicly-addressed IP packet information. This method may involve the further steps of receiving, at the tunnel server from the public computer network, publicly-addressed IP packet information; wrapping, at the tunnel server, the publicly-addressed IP packet information within privately-addressed IP packet information; and sending, from the tunnel server, the privately-addressed IP packet information for receipt by the computer device. Similarly, the unique methods may involve the steps of receiving, at a computer device of a private computer network from a tunnel
server, privately-addressed IP packet information; and unwrapping, at the computer device, the privately-addressed IP packet information to reveal publicly-addressed IP packet information. This method may involve the further steps of wrapping, at the computer device, publicly-addressed IP packet information within privately-addressed IP packet information; and sending, from the computer device, the privately-addressed IP packet information for receipt by the tunnel server.

A more detailed computer system configuration is therefore also adapted to facilitate the use of private IP addresses for computer devices in a private computer network while allowing those computer devices to communicate over the Internet. The detailed computer system configuration includes a private computer network that includes a fixed wireless system. The fixed wireless system involves a plurality of computer devices, each being typically located in a family residence and associated with a private IP address. Each one of the computer devices is coupled to a wireless receiver unit, and each wireless receiver unit is coupled to a wireless base unit through a wireless communication link. The computer system configuration includes a tunnel server having an access port coupled to receive tunnel requests from the computer devices (through the wireless base unit), and a resource port coupled to a service provider of the Internet. The tunnel server is operative to facilitate creation of a tunnel between the wireless transceiver unit and the tunnel server to facilitate communications between the wireless transceiver unit and the Internet.

Referring to FIG. 2, a computer system 200 which facilities IP tunneling techniques of the present invention is shown. Computer system 200 includes a plurality of computer devices 214, such as a server 216 or devices within a private computer network 218, which may be accessed via the Internet 106. Such devices may be publicly accessible, such as server 216, which has a public IP address. Computer system 200 also includes a private computer network 202 which communicates with an ISP 104 for access to the Internet 106. Private computer network 202 includes plurality of personal computers (PCs) 204 or other computing devices, such as a PC 208, a PC 210, and a PC
212, and a tunnel server 206 having IP tunneling software. Tunnel server 206 may be, for example, a Network Access Server (NAS).

The private addresses used in private computer network 202 may include, for example, addresses within the range of 10.0.0.0 - 10.255.255.255; however, other suitable addresses may be utilized as well, such as those specified by the Request For Comments (RFC) standard (e.g., RFC-1918). Presently-defined private address space includes address ranges 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, and 192.168.0.0 - 192.168.255.255. These private addresses are not routable on the public computer network.

Tunnel server 206 has an access port coupled to the plurality of PCs 204 and a resource port coupled to ISP 104. If PC 212 wishes to communicate with server 216 over the Internet 106, it invokes a request to tunnel server 206 within private computer network 202. In response, tunnel server 206 establishes an IP tunnel for communication therebetween. An IP tunnel 210 is represented in FIG. 2 by dashed lines, having terminal points at PC 212 (or other device acting on its behalf) and tunnel server 206.

For outbound communication (from PC 212 to tunnel server 206 to Internet 106), tunnel operation for PC 212 involves wrapping the appropriate public IP addresses with private IP addresses for communication within private computer network 202, and tunnel operation at tunnel server 206 involves unwrapping the public IP addresses from within the private IP addresses for communication over the Internet 106. For inbound communication (from Internet 106 to tunnel server 206 to PC 212), tunnel operation at tunnel server 206 involves wrapping the incoming public IP addresses with the private IP addresses for communication within private computer network 202, and tunnel operation for PC 212 involves unwrapping the incoming private IP addresses to reveal the underlying public IP addresses. Although tunnel operations are described as being performed by PC 212, these operations may be performed by an intermediary unit (such as a remote unit or receiver unit described below) from the PCs. In an alternate embodiment to that shown and described in relation to FIG. 2, the tunnel
connects the user to another different private computer network, such as a corporate Intranet.

FIG. 3 is an illustrative representation of a computer system involving both public and private computer networks, where the private computer network involves a fixed wireless system 302. Fixed wireless system 302 involves a plurality of residences 304, including residences 306-310, each having one or more computer devices. For example, residence 306 has a computer device 312; residence 308 has a computer device 314 and a computer device 316; and residence 310 has a computer device 318, a computer device 320, and a computer device 322. Fixed wireless system 302 includes a plurality of remote units 324, which are and may be referred to as wireless transceiver units. Each one of residences 304 includes a remote unit; for example, residence 306 has computer device 312 coupled to a remote unit 326; residence 308 has computer devices 314 and 316 coupled to a remote unit 328; and residence 310 has computer devices 318, 320, and 322 coupled to a remote unit 330. As indicated in FIG. 3, remote units 324 communicate with a base unit 332 via a wireless communication link. A plurality of other base units which serve other remote units are involved as well, such as a base unit 334 and its associated remote units.

Base unit 332, as well as other base units such as base unit 334, are coupled to a service node 336. Service node 336 includes an access router 342, a tunnel server 340, a dynamic host configuration protocol (DHCP) server 346, and a Web server 348. Base unit 332 is more particularly coupled to access router 342, which is in turn coupled to an access port of tunnel server 340. Access router 342 is also coupled to DHCP server 346 and Web server 348. The fixed wireless system, which includes service node 336, is a private network that utilizes private IP addresses. DHCP server 346 is operative to dynamically assign private IP addresses as necessary to computer devices within residences 304. The private addresses utilized may include addresses within the range of 10.0.0.0 - 10.255.255.255; however, other suitable private addresses may be utilized as well, such as those specified by a Request For Comments (RFC) standard (e.g., RFC-1918). These addresses are not routable
on the Internet. Access router 342 is operative to receive IP packets from remote units 324 through base unit 332, and route them as appropriate to either private resources (e.g., Web server 348) or to public resources (e.g., ISP 338 for the Internet) through tunnel server 340.

Tunnel server 340 may be a NAS. As indicated, tunnel server 340 has its access port coupled to access router 342 and a resource port coupled to ISP 338. If PC 314 wishes to communicate with server 352 over the Internet, it invokes a request to tunnel server 340. The request is sent through remote unit 328, base unit 332, and access router 342. In response, tunnel server 340 establishes an IP tunnel for communication therebetween. An IP tunnel 350 is represented in FIG. 3 by dashed lines, having terminal points at PC 314 and tunnel server 340.

For outbound communication (from PC 314 to tunnel server 340 to server 352), tunnel operation at PC 314 involves wrapping the appropriate public IP addresses with private IP addresses for communication within the private computer network, and tunnel operation at tunnel server 340 involves unwrapping the public IP addresses from within the private IP addresses for communication to server 352. For inbound communication (from server 352 to tunnel server 340 to PC 314), tunnel operation at tunnel server 340 involves wrapping the incoming public IP addresses with the private IP addresses for communication within the private computer network, and tunnel operation at PC 314 involves unwrapping the incoming private IP addresses to reveal the underlying public IP addresses. Although some tunnel operations are described as being performed by PC 314, these operations may be alternatively performed by the remote units (e.g., remote unit 328 for PC 314).

In an alternate embodiment to that shown and described in relation to FIG. 3, the tunnel connects the user to another different private computer network, such as a corporate Intranet.

FIG. 4 is a flowchart describing a method of reverse tunneling in private computer networks. This method may be utilized in any of the systems described in relation to FIGs. 2 and 3, as well as ones to be described in more detail below. The method relates more particularly to operations
performed by the tunnel server. Beginning at a start block 400 of FIG. 4, a tunnel server receives a tunnel request from a computer device of a private network having a private address (step 402). Next, a "reverse tunnel" between the tunnel server and the computer device is established to facilitate communications between the computer device in the private network and a computer device in a public network (step 404). In this tunnel, a public protocol (e.g., IP protocol) is wrapped within a private protocol of the private network, and unwrapped for communications outside the private network. The flowchart ends at a finish block 406, but may be repeated for other computer devices and additional tunnel requests.

What is now described are additional details for implementing a variety of such systems as one skilled in the art will readily appreciate. FIG. 5 is an illustrative representation of more detailed structure and functionality in the fixed wireless system of FIG. 3. The fixed wireless system (FWS) high speed data (HSD) infrastructure is comprised of four major components and three interfaces that allow the transport of the data from hosts at user's home to an Internet Service Provider (ISP) of choice for Internet access. The four major components of the HSD infrastructure are a Home Phoneline Networking Alliance (HPNA) Interface Adapter 502 on the PC, a transceiver unit or remote unit (RU) 504 with the HPNA interface, a Base 506, and a data service node (DSN) 508. Connecting these components together are the three interfaces - a Home (H)-interface 510 that connects the PCs to the RU 504; an airlink (A)-interface 512 between RU 504 and Base 506; and a Network (N)-interface 514 that links the Base 506 to the router on the DSN 508. The RU 504 serves as the gateway of the home local area network (HLAN) subnet; the Base 506 performs a switching function between the RU 504 and the router on the DSN 508.

FIG. 6 is an illustrative representation of more detailed structure and functionality of a service site (DSN 508 of FIG. 5) of the fixed wireless system. The DSN 508 connects the HSD infrastructure to the public Internet. It maintains several servers and databases to make the IP infrastructure possible. The DSN 508 contains one router that routes between the Base 506
and the interface to the Internet (ISP). The router has a LAN interface that connects to a DHCP server 602. The router function is split into two parts, an Access Router (AR) 604 that gets traffic from the Bases, and Border Router (BR) 606 that connects to the ISPs. The AR 604 is the interface between DSN 508 and Base 506; the BR 606 is the interface between DSN 508 and the ISPs. AR 604 performs the access concentration function and routes the packets to the servers and/or the BR 606 on the DSN 508 whereas the BR 606 performs normal routing and filtering functions to direct the user traffic to/from different ISPs. The DSN 508 also contains DHCP server 602 to perform IP address and PC configuration management.

In the HSD architecture, the DHCP server 602 assigns the IP address and the local configuration parameters based on the bootstrap protocol (BOOTP) relay agent IP address and the network it is representing. More particularly, if the DHCPCDISCOVER message contains a giaddr value (i.e., the client is not on the same LAN segment as the server), the server uses a giaddr value (the IP address) to go over the list of the networks that it is responsible for. If the search fails, it should ignore the request. If the search is successful, it will select an unused IP address along with the configuration parameters for that local network and return the offer back to the relay agent. The selection of the IP address could be static or dynamic. That is, the association between the MAC address and the IP address could be fixed (static) so that the same PC client always gets the same IP address. Otherwise, the selection is dynamic. Table 1 is an example of part of the DHCP network table on a Solaris 2.6, UNIX system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>angel</td>
<td>m</td>
<td>Include=Locale:Timeserv=10.255.254.2:LeaseTim=8640 0:LeaseNeg:MTU=576:Subnet=255.0.0.0:Broadcast=10.25 5.255.255;</td>
</tr>
</tbody>
</table>
In this example, what is defined is a profile name *angel* that represents the local configuration parameter. The profile contains information that the server will include in the response sent back to the client. In this case, since the subnet mask is 255.0.0.0, the client treats the entire Net 10 as a flat network, including the servers on the DSN 508. Note that the RU proxy-ARPs (Address Resolution Protocol) for the entire HSD infrastructure and the only traffic going out of the HLAN will be destined to the infrastructure including the tunnel server. Therefore, there is no need for the DHCP server 602 to send the Router option back to the client to configure the default gateway. The PC sends out the ARP request for the IP address of the server because the address range for the HSD infrastructure, 10.255.254.0/23, is considered on the same physical LAN when the client is configured, with the mask 255.0.0.0.

In addition to the server configuration table, there are host tables -- one for each HLAN. One typical example on a Solaris implementation is given in Table 2. When a DHCP request arrives, the server will use the relay agent IP address to figure out which subnet the request came from. (To clarify, the relay agent IP address is the address of the RU, which is the traditionally chosen +1 gateway address in the subnet assigned to the home. For example, if the home has addresses in the range 10.0.0.8 through 10.0.0.15, the 10.0.0.8 and 10.0.0.15 addresses are excluded from use, "+1" address at 10.0.0.9 is the address of the RU, and 10.0.0.10 through 10.0.0.14 are DHCP assignable to the PCs.) For example, if the giaddr (router IP) is 10.6.1.1, the server uses the subnet mask information from /etc/netmasks, which will have the value of 255.255.255.248 pre-configured for Net 10. In this case, the subnet for the request is 10.6.1.0. The server uses the DHCP Network database with the name '10.6.1.0' for the IP address assignment.

If the DHCP request is for renewal, the source IP address (PC IP) is used along with the netmask to locate the DHCP Network database. For example, if the PC IP is 10.6.1.2, by masking 10.6.1.2 with the subnet mask (255.255.255.248); the server knows that the request comes from the subnet 10.6.1.0, subsequently, the associated DHCP network database is used for extending the lease.
An example of the IP address table for network 10.6.1.0 is shown in Table 2.

<table>
<thead>
<tr>
<th>Client ID (MAC)</th>
<th>Flags</th>
<th>Client IP</th>
<th>Server IP</th>
<th>Lease</th>
<th>Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>010080C881FB55</td>
<td>0</td>
<td>10.6.1.2</td>
<td>10.255.254.2</td>
<td>879835356</td>
<td>angel</td>
</tr>
<tr>
<td>0100C023698087</td>
<td>0</td>
<td>10.6.1.3</td>
<td>10.255.254.2</td>
<td>879809556</td>
<td>angel</td>
</tr>
<tr>
<td>0100C02369807B</td>
<td>0</td>
<td>10.6.1.4</td>
<td>10.255.254.2</td>
<td>881954992</td>
<td>angel</td>
</tr>
<tr>
<td>01080007818B51</td>
<td>0</td>
<td>10.6.1.5</td>
<td>10.255.254.2</td>
<td>879365458</td>
<td>angel</td>
</tr>
<tr>
<td>01080307435567</td>
<td>0</td>
<td>10.6.1.6</td>
<td>10.255.254.2</td>
<td>879364411</td>
<td>angel</td>
</tr>
</tbody>
</table>

Table 2 only shows five usable addresses (the host addresses that have all zeros and all ones are not available.) As demonstrated here, the first field of each entry is the MAC address of the device that uses the IP address. The second field defines the use of the IP address. It is a bitmap value where a '0' indicates that the address is available for DHCP allocation, and a '3' indicates that the address is a permanent (no lease expiration) and manual (cannot be assigned) address. The third field indicates the IP address itself. The fourth field shows the IP address of the DHCP server. The fifth field is the lease expiration time stamp (a negative one, -1, means never expires). The last field indicates the profile name for the local configuration parameters to use.

In summary, the DHCP needs the provisioning of the following data: (1) Standard RU subnet tables. Each table contains five IP addresses. The first subnet starts from 10.0.0.0 and ends 10.108.255.248. If the Expanded RU subnet is not used, one can continue the use of the first half from 10.109.0.0 to 10.127.255.248 and extend to the second half of the Net 10 (from 10.128.0.0 to 10.191.255.248.) Therefore the total number of standard tables to be provisioned is either 737,280 or 1.5 M. (2) (Optional) Expanded RU subnet tables. Each table contains 13 IP addresses. The subnet starts from 10.128.0.0 and ends at 10.223.255.240. The total number of this Expanded subnet to be provisioned is 368,640. (3) Globally, the Subnet Mask, the Broadcast Address,
the Lease Time, and the DHCP Server IP Addresses. Although a particular implementation is described, one skilled in the art can readily appreciate that there are a number of other suitable ways to “carve up” address space.

Internet Access via Tunneling. The high speed data (HSD) IP network provides the basic IP connectivity throughout the fixed wireless system (FWS) infrastructure. Because of the shortage in public IP address space and the potential large number of addresses needed for HSD service, the private IP address space specified in RFC-1918 is to be used for assigning addresses to the HSD HLAN PCs as well as infrastructure devices, such as private network servers. This limits the HSD users to communicate only within the FWS Local Service Area (LSA). In order to communicate with servers on the public Internet, a public address has to be used. As such, the need arises to relay the user data between two networks using different address schemes.

This could be done by having a Network Address Translation (NAT) function between the FWS area and the public Internet to perform the private/public address translation. However, there are a few limitations on the NAT technology. It lacks the support on applications that hide the address information inside the payload including H.323 IP phone, video conferencing (NetMeeting), and the emerging IPSec security standards. NAT also cannot scale well due to the processing power required on performing the dynamic address translation function.

To access the public Internet, HSD users also need to subscribe to an ISP’s Internet access service, and the HSD infrastructure needs to redirect all user traffic destining to the public Internet to the subscribed ISP network. One way to perform this subscription-based routing is to use a Policy-based Routing (PBR) feature on the router to route user’s data traffic destined for the public Internet to the subscribed ISP transport network. The PBR routes the traffic based on the policy set up for a particular user. In this case, the user is identified by the source IP address, and the policy points to the interface that connects to a specific ISP transport network. The weakness of this technology is the scalability. Potentially the policy table could be huge, upward of 5000 entries, one entry for each PC. Updating the table could be
frequent as well - the entry is updated every time the user switches the ISP connection from one to another. This poses a serious OA&M problem.

The inventive technology adopted for the HSD architecture fulfills both the address translation and the ISP traffic-redirection tasks simultaneously. It is also transparent to the FWS IP routed network and is free of the problems mentioned previously. This technology is the emerging tunneling protocol specified for the mobile IP and port wholesale services. The tunneling technology allows the client to tunnel to the server that performs the relaying function between the private address network (LSA) and the public addressed network (Internet.)

Tunnel Architecture. The tunneling technology usually involves a control channel and a tunnel. The control channel is used to establish the tunnel by assigning the tunnel ID and to perform the link integrity check. The tunnel channel subsequently is used to encapsulate the user datagrams between the tunnel client and the server.

There are various tunneling protocols being proposed as the IETF standards which may be utilized. The Point-to-Point Tunneling Protocol (PPTP) championed by Microsoft is available as client for Windows 95 and server for Windows NT [258, 259, and 260]. The Layer 2 Forwarding (L2F) protocol proposed by Cisco is only available on Cisco’s platform. The emerging standard Layer 2 Tunneling Protocol (L2TP) [257] brings the PPTP and the L2P under one protocol standard and has been viewed as the future standard for tunneling the PPP packets. Other tunneling protocols such as Mobile IP, IPSec in the tunnel mode, and the latest Distributed NAT (DNAT) are all potential candidates to use.

When the PPTP or the L2TP tunnel standard is used, PPP is used inside the tunnel to negotiate other features including the compression (via Compression Control Protocol (CCP)) and the encryption (via Encryption Control Protocol (ECP)). The standard IP Control Protocol (IPCP) as part of the PPP stack will also be used to assign the PC client public IP address and ISP’s DNS server IP address.
Depending on the preference and support of the tunnel server operator, the user may use different tunnel software packages for different ISPs, but the choice of the tunnel is transparent to the HSD infrastructure since the infrastructure will route the tunnel datagram transparently between the tunnel client and server. Nevertheless, there are four different ISP Access architectures described depending on the location of the server and the ownership of the server. However, other architectures may be devised by those skilled in the art. For simplicity and generality, the use of a Network Access Server (NAS) is described to represent the tunnel server, and assumes that the location of the NAS reflects the owner and the operator of the NAS. Four architecture options will be described: NAS at ISP, NAS at DSN - dedicated NAS & BR per ISP, NAS at DSN - dedicated NAS but shared BR, and NAS at DSN - shared NAS and BR.

FIG. 7: NAS at ISP. Because of the current availability of the PPTP client software, PPTP is utilized to demonstrate the tunneling architecture. A PPTP server 702 of an ISP 704 is connected to a DSN 706 directly and appears to the FWS HSD user as part of the FWS Intranet. Once the user’s PC has gone through the DHCP negotiation to obtain an infrastructure private IP address, it will be able to access any servers within the infrastructure including the PPTP server 702 on the ISP side.

In this example, the Home-1 user establishes a PPTP tunnel to ISP-1 by specifying the tunnel server’s private address (10.255.255.1) and the account information in order to access the services accessible only via the public Internet. In this architecture, both an AR 708 and a BR 710 only need to know how to route the IP datagrams within the HSD infrastructure, including the HSD private network extension to the ISP NAS. The routes can be statically configured and no routing protocol among the routers is needed.

FIG. 8: NAS at DSN - Dedicated NAS and BR Per ISP. The owner of the fixed wireless system may own and operate the NAS. There are three options to interconnect between the NAS and the ISPs. In the following description, the option of dedicating the NAS and the BR per ISP is discussed. Each ISP 802 has one or more dedicated NAS 804 connecting to a dedicated
BR 806. All the NASs 804, even when supporting different ISPs 802, can be on
the same LAN segment connecting the AR 808. The HSD user addresses the
NAS 804, when connecting to a specific ISP 802, either by an IP address or a
host/domain name. In the case, if multiple NASs 804 are used for an ISP 802,
using the host/domain name approach allows a way to balance the traffic to
different NASs 804 dedicated to the same ISP 802. On the other side of the
NAS 804 towards the BR 806, only the NASs 804 supporting the same ISP 802
can be on the same LAN segment as the BR 806 that connects to the ISP
network.

The provisioning of the BRs 806 is similar to that described in relation
to FIG. 7 except that, since the public IP addresses are exposed on the BR
interface, a default route entry is needed on the BR 806 to route the IP
datagrams to the ISP network. Also on the BR 806, since each NAS 804
controls one pool of public IP address for PPTP assignments, there must be
one route per IP pool of subnet pointing back to the NAS that controls that
subnet.

On the NAS 804, since public IP is also exposed, the NAS 804 has to
have a default route to the BR 806 that has the connectivity to the ISP
network. It should also have a route to the Net 10 (with AR 808 as the next
hop). It should not have a route to other HSD infrastructure except the one
that connects to the OSS network for management functions (OAM&P).

FIG. 9: NAS at DSN - Dedicated NAS and Shared BR. In the following
description, the option of dedicating the NAS but with the BR shared among
many ISPs is discussed. Each ISP 902 has one or more dedicated NAS 904
connecting to a shared BR 906. As described in relation to FIG. 8, all the NASs
904 can be on the same LAN segment connecting the AR 908. The HSD user
addresses the NAS 904, when connecting to a specific ISP 902, either by an IP
address or a host/domain name to allow load balancing. On the other side of
the NAS 904 towards the BR 906, all the NASs 904 are also on the same LAN
segment with one BR 906 that connects to many ISPs 902.

In this architecture, since the BR 906 is connected to many ISP
networks, the Policy Based Routing feature is required to route the IP
datagrams, destined to the Internet, to different ISP interfaces based on the source address of the datagrams. In this case, since the source address always be from a limited number of IP subnets (pools), the policy can be concise and static and thus makes the routing very efficient. The default route should not exist since the traffic to the Internet is policy routed. In the reverse direction, again, since each NAS 904 controls one pool of public IP address for PPTP assignments, there must be one route per IP pool of subnet on the BR 906 pointing back to the NAS that controls that subnet.

On every NAS 904, the same default route to the BR 906 that has the connectivity to all the ISP networks is sufficient. All the NASs 904 should also have a route to the Net 10 (with AR as the next hop) and should not have the route to other HSD infrastructure except the one that connects to the OSS network for OAM&P purpose.

FIG. 10: NAS at DSN - Shared NAS & BR. In the following discussion, the option of sharing both the NAS and the BR to connect to many ISPs is discussed. This architecture allows the sharing of the NAS and the BR with the connections to ISP networks for Internet access. This is particularly attractive to small ISPs that cannot afford the dedicated resources to connect to the FWS POP.

As described in relation to FIG. 8, all the NASs 1002 can be on the same LAN segment connecting the AR 1004. The HSD user addresses the NAS 1002, when connecting to a specific ISP 1006, either by an IP address or a host/domain name to allow load balancing. The only difference is that each user needs to identify the choice of ISP 1006 by including the ISP 1006 fully qualified domain name (FQDN) as part of the user name. The NAS 1002 host/domain name is no longer used to identify the ISP 1006 of choice but is used as a generic name for load balancing purpose.

Since each NAS 1002 serves many ISP domains, the use of a Remote Authentication Dial-In User Service (RADIUS) server with a centralized database will simplify the provisioning process required on each NAS 1002 for authentication and IP address pooling. RADIUS is well-known and involves an access control protocol that uses a challenge/response method for
authentication. In this case, each NAS 1002, acting as a RADIUS client, consults the RADIUS server for user authentication and IP address assignment. The NAS supplies the user/ISP FQDN to the server upon the initial connection request from the user. The RADIUS server, based on the ISP FQDN, retrieves the user account information, performs the authentication, selects an available IP address from the proper IP address pool, and returns the result back to the NAS 1002.

The IP address pool databases may reside anywhere as long as the RADIUS server in the DSN can reach them to authenticate subscribers. In one implementation, a RADIUS proxy is used in the DSN and authentication queries of ISP databases at the ISP are made; the NAS selects the IP address from a NAS-managed pool of addresses already designated by the ISP for use by the NAS.

Since the BR 1008 is shared, all the NASs are also on the same LAN segment with one BR 1008 that connects to many ISPs 1006. As described in relation to FIG. 9, since the BR 1006 is connected to many ISP networks, the Policy Based Routing feature is required to route the IP datagrams to different ISP interfaces based on the source address of the datagrams. In this case, since the source address always is from a limited number of IP subnets (pools), the policy can be concise and static and thus makes the routing very efficient. The default route should not exist since the traffic to the Internet is policy routed.

In the reverse direction, since each NAS 1002 can terminate many PPTP sessions using addresses from different ISP IP address pools, and since such address assignment is dynamic depending on what NAS 1002 is used at the time the tunnel is established, a dynamic routing protocol is run to keep track of the IP address assignments. Since this is only needed every time a tunnel is established, and since host address route announcement is used here, any dynamic routing protocol is sufficient for this purpose. Also as described in relation to FIG. 9, every NAS 1002 needs one default route to the BR 1008, a route to the Net 10, and one route to the OSS network for OAM&P purpose.
In FIGS. 11A and 11B, PPTP is used as the tunneling protocol in conjunction with the NAS at ISP architecture to describe the call flow in establishing the tunnel and for Internet access. As shown in FIG. 11A, PC broadcasts the ARP query for the gateway physical address (step 1102). RU responds with an ARP response (step 1104). PC initiates the PPTP tunnel set up by establishing a TCP session for PPTP control channel (step 1106). The TCP Sync packet is sent to the PPTP server on TCP port 1723. RU performs the basic frame filtering and forwards the IP packet to the Base (step 1108). Base and Router forward the IP datagram to the PPTP server on the ISP side (step 1110). The ISP has the direct connection via Frame Relay/Lease Line to the DSN complex. (The PPTP server is an extension of the HSD infrastructure if HSD uses the private IP address space. That means the PPTP server will have a private IP address assigned to it (10.255.255.1) and the router is capable of routing the packets to it.) PPTP server acknowledges the TCP sync packet by sending back with a TCP sync-ack packet to the PC (step 1112). RU, once it receives the IP datagram, performs the filtering and forwards the datagram to the home PC (step 1114).

Continuing on to FIG. 11B, once the TCP session for the PPTP control channel is established, the PC client starts the PPTP tunnel setup process (step 1116). Messages are sent via the established TCP connection (destination IP=PPTP server, destination port=1723). Once the tunnel is granted, the subsequent data traffic will use the PPTP tunnel (modified GRE), not the TCP control channel, for any encapsulation to the PPTP server. The first user data will be the PPP LCP negotiation (including CCP and ECP), account authentication, and the IPCP session to assign the tunnel an IP address (in this case 205.172.9.72) (step 1118). Once the PPP session is set up, the PPP is in the open state and awaits any application data transfers. All the subsequent TCP/IP traffic for the user application is encapsulated in the following fashion (step 1120): The user TCP/IP data will have a source IP address (205.172.9.72) assigned by the PPTP server for the tunnel interface. It is then wrapped by the PPP header (2-byte Protocol ID). The entire PPP frame is encapsulated by the PPTP specific GRE header then the IP header (IP
Prot=0x880B to indicate GRE packet). In this case, the destination address of the outer IP is the PPTP server IP address (10.255.255.1), and the source IP address is the PC's original IP address assigned by the DHCP server (10.1.0.2). The PPTP server reverses the process to restore the user TCP/IP datagram and routes it to the Internet based on the destination IP address of the datagram (step 1122). The returning IP traffic destined to an IP address assigned to a PPTP tunnel end-point will be wrapped with the proper PPP header and GRE header, and then be forwarded to the HSD infrastructure using the infrastructure IP addresses.

It should be readily apparent and understood that the foregoing description is only illustrative of the invention and in particular provides preferred embodiments thereof. Various alternatives and modifications can be devised by those skilled in the art without departing from the true spirit and scope of the invention. Accordingly, the present invention is intended to embrace all such alternatives, modifications, and variations which fall within the scope of the appended claims.

What is claimed is:
CLAIMS

1. An apparatus for enabling privately addressed devices in a private network to communicate over a public network, the apparatus comprising:
   a tunnel server;
   an access port of the tunnel server coupled to receive requests for tunnels through a private network from privately addressed devices on the private network; and
   a resource port of the tunnel server coupled to a service provider of a public network.

2. The apparatus according to claim 1, wherein the tunnel server includes means for establishing a tunnel through the private network.

3. The apparatus according to claim 1, the tunnel server including means for unwrapping public addresses from privately addressed information.

4. The apparatus according to claim 1, wherein the public network comprises a wide area network (WAN).

5. The apparatus according to claim 1, wherein the public network comprises the Internet.
6. The apparatus according to claim 1, wherein the private addresses include at least some addresses that are not routable on the public network.

7. The apparatus according to claim 1, wherein the private network comprises a fixed wireless system.

8. A method for enabling privately addressed for devices in a private network to communicate over a public network, the method comprising:
   receiving a tunnel request from a privately addressed device of a private network;
   creating a tunnel through the private network in response to the tunnel request; and
   conducting communication through the tunnel between the device and a service provider of a public network.

9. The method according to claim 8, wherein creating the tunnel comprises:
   creating a tunnel through the private network between the device and a tunnel server.

10. The method according to claim 8, wherein conducting communication comprises conducting communication between the device and a service provider of a wide area network (WAN).

11. The method according to claim 8, wherein conducting communication comprises conducting communication between the device and a service provider of the Internet.

12. The method according to claim 8, wherein the private addresses include addresses that are not routable on the public network.
13. The method according to claim 8, wherein receiving a tunnel request comprises receiving a tunnel request from a device within a fixed wireless system.

14. A method executed by a tunnel server for enabling computer devices with private IP addresses in a private computer network to communicate over the Internet, the method comprising:
   receiving privately-addressed IP packet information from a computer device of a private computer network;
   unwrapping the privately-addressed IP packet information to obtain publicly-addressed IP packet information; and
   sending the publicly-addressed IP packet information over the Internet.

15. The method according to claim 14, further comprising:
   receiving publicly-addressed IP packet information from the public computer network;
   wrapping the publicly-addressed IP packet information within privately-addressed IP packet information; and
   sending the privately-addressed IP packet information for receipt by the computer device.

16. A server system for enabling computer devices with private IP addresses in a fixed wireless system to communicate over the Internet, the server system comprising:
   a tunnel server;
   an access port coupling the tunnel server to the fixed wireless system to receive requests for tunnels through the fixed wireless system from the computer devices; and
   a resource port coupling the tunnel server to a service provider of the Internet.
17. A computer system comprising:
a private computer network;
one or more computer devices coupled to the private computer network;
each one of the one or more computers having a private IP address;
a tunnel server;
an access port coupling the tunnel server to the private network to receive tunnel requests from the one or more computer devices having the private IP addresses; and
a resource port coupling the tunnel server to an Internet service provider.

18. The computer system according to claim 17, wherein the private computer network further comprises a fixed wireless system including:
a wireless receiver unit coupled to at least one of the computer devices;
and
a wireless base unit coupled to the wireless receiver unit to receive the tunnel requests and pass them to the tunnel server.

19. The computer system according to claim 17, further comprising:
means in the tunnel server for providing assignment of a public IP address in response to a tunnel request.

20. The computer system configuration according to claim 17, wherein:
the tunnel server includes means for creating a tunnel in response to a tunnel request; and
the tunnel server includes means for assigning a public IP address.
21. A processor apparatus, comprising:
   a server for forming a tunnel for communications;
   an access port for coupling the server to a privately addressed device
   on a private computer network through a tunnel in the private computer
   network; and
   a resource port for coupling the server to a public computer network.

22. The processor apparatus according to claim 21, wherein the
    public computer network is the Internet.

23. The processor apparatus according to claim 21, wherein the
    resource port is for coupling the server to an Internet Service Provider (ISP) or
    the like.

# # #
START

RECEIVING A TUNNEL REQUEST FROM A COMPUTER DEVICE HAVING A PRIVATE ADDRESS OF A PRIVATE NETWORK

ESTABLISHING A TUNNEL BETWEEN THE TUNNEL SERVER AND THE COMPUTER DEVICE TO FACILITATE COMMUNICATIONS BETWEEN THE COMPUTER DEVICE IN THE PRIVATE NETWORK AND A COMPUTER DEVICE IN A PUBLIC NETWORK

FINISH

FIG. 4
Routing Table

<table>
<thead>
<tr>
<th>Int</th>
<th>IP Subnet</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0.1</td>
<td>10.0.0.0</td>
<td>255.255.192.0</td>
</tr>
<tr>
<td>S0.2</td>
<td>10.0.64.0</td>
<td>255.255.192.0</td>
</tr>
<tr>
<td>S0.3</td>
<td>10.0.128.0</td>
<td>255.255.192.0</td>
</tr>
</tbody>
</table>

Each sub-interface represents one Base. (In this example, each Base serves 512 RU subnets.)

Unchannelized T1 Inside
Channelized T3

Data Service Node
10.0.0.0-10.255.255.255

DHCP/BOOTP Table

<table>
<thead>
<tr>
<th>IP Subnet Mask</th>
<th>GW IP</th>
<th>Lease</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0</td>
<td>255.255.255.248</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>10.0.0.8</td>
<td>255.255.255.248</td>
<td>10.0.0.9</td>
</tr>
</tbody>
</table>

Net 10_0_0_0 Table

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x</td>
<td>10.0.0.2</td>
<td>86967212</td>
</tr>
<tr>
<td>y.y.y.y</td>
<td>10.0.0.3</td>
<td>86968012</td>
</tr>
<tr>
<td>0</td>
<td>10.0.0.4</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>10.0.0.5</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>10.0.0.6</td>
<td>0</td>
</tr>
</tbody>
</table>
FIG. 11B

MAC(src=PC, dest=RU)
IP(src=10.255.255.1, dest=10.1.0.2) - TCP
(1723, Syn)

PPTP Control Connection Establishment
IP(src=10.1.0.2, dest=10.255.255.1). Start-Control-Conn-Request
IP(src=10.255.255.1, dest=10.1.0.2). Start-Control-Conn-Reply
IP(src=10.1.10.2, dest=10.255.255.1). Incoming-Call-Request (Call ID & Ser No)
IP(src=10.255.255.1, dest=10.1.0.2). Incoming-Call-Reply (Call ID & Peer's Call ID)

PPP Session Establishment
MAC(src=RU, dest=PC)
IP(src=10.1.0.2, dest=10.255.255.1, Prot=47) - GRE(Prot=0x880B)

Normal Data Flow
Step 1120
FTP
HTTP
SMTP

Step 1122
IP with SRC=205.172.9.72
PPTP/GRE Encapsulated PPP Packets
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L12/28 H04L12/46

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

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

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)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>
| X        | W.T. TEO, Y. LI: "Mobile IP extension for Private Internets Support (MPN)"
INTERNET DRAFT, ‘Online!’
November 1998 (1998-11), pages 1-22,
XP002106957
Retrieved from the Internet:
<URL:http://cram.isc.nus.sg:8080/cram/draft-teoyli-mobileip-mpn-01.txt>
'retrieved on 1999-06-22!
page 1, line 1 - page 19, line 11 |
| A        | EP 0 917 318 A (LUCENT TECHNOLOGIES INC) 19 May 1999 (1999-05-19)
abstract
page 2, line 56 - page 3, line 17
page 5, line 3 - page 6, line 14 |

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 in the same year as the international filing date

"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
"A" document member of the same patent family

Date of the actual completion of the international search
7 November 2000

Date of mailing of the international search report
14/11/2000

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

Authorized officer
Lievens, K
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>DEMIZU N ET AL: &quot;DDT - A versatile tunneling technology&quot;</td>
<td>1, 8, 14, 16, 17, 21</td>
</tr>
<tr>
<td></td>
<td>COMPUTER NETWORKS AND ISDN SYSTEMS, NL, NORTH HOLLAND PUBLISHING. AMSTERDAM,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vol. 27, no. 3, 1 December 1994 (1994-12-01), pages 493-502, XP004037982</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISSN: 0169-7552 abstract page 493, left-hand column, line 11 - page 496,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>right-hand column, line 17</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249830 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249831 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249836 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249837 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249838 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249839 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249862 A</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td>CA 2249863 A</td>
</tr>
<tr>
<td>JP</td>
<td></td>
<td>JP 11275154 A</td>
</tr>
<tr>
<td>JP</td>
<td></td>
<td>JP 11275155 A</td>
</tr>
<tr>
<td>JP</td>
<td></td>
<td>JP 11275157 A</td>
</tr>
<tr>
<td>JP</td>
<td></td>
<td>JP 11331276 A</td>
</tr>
</tbody>
</table>