CONNECTION ORIENTED COMMUNICATIONS NETWORK

A simple, user-friendly and commercially secure means of providing access to the endless variety of services and sources of information that is and will be available via the Internet is described.

What is described is an adaptation of the principles employed in an Intelligent Network such as is described in Patent Application No. GB 2272603 and proposed for the telephone network and are applicable to ATM, X25 and similar networks.

To gain access to even the most remote and obscure source of information, a user simply opens a session with a Broker or Enquiry type service. As the user's needs are identified, the session will be transferred from Broker to Broker and from Server to Server until the final objective is reached. The user does not participate in the transfer activity.

Brokers do not reveal any information to their client users as they transfer sessions to other Brokers or Servers. Having gained access to a service via a Broker, a user cannot regain access to that service without again going via the Broker.

Servers deliver information directly to the user whose identitiy is verified. Brokers do not handle the information.

It is also shown how interworking with the existing Internet architecture and protocols can be carried out.

REQUIREMENTS OF THE FUTURE INTERNET

The Internet is increasingly being used for commercial and industrial purposes which, apart from causing an explosion in traffic, will require that the future network provides a highly efficient and commercially secure "on-demand" service.

The old-pals-act which enabled users to clamber around one another's networks (and be satisfied with the performance) cannot continue. Internet Providers must be independent of and impartial to the users.

The future Internet Providers will be similar to the telephone network Providers. Users will pay a fixed charge for Internet access and will almost certainly pay an additional usage charge. In some cases, a further charge may be levied by the distant terminal for the actual information delivered.

According to the present invention there is provided a communications network comprising means for interconnecting a user computer terminal to a further computer terminal, which further computer terminal is one of a plurality of computer terminals connected in the network, wherein a virtual message path is established from the further computer terminal to the user computer terminal in response to an open message sent from the user computer terminal to a user router which sends a service request to the

further computer terminal via one or more further routers.

The present invention will now be described by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows a block diagram of an Internet structure to illustrate Internet addressing;

Figure 2 shows diagrammetically the establishment of a virtual message path;

Figure 2A shows the structure of a host/router link header;

Figure 2B shows the format of a typical OPEN MESSAGE;

Figure 2C shows the format of a typical OPEN MESSAGE passed from Router to Router;

Figure 2D shows the format of a typical message packet passed along a message path;

Figure 3 shows diagrammatically the creation of a special service message path;

Figure 3A shows the format of a typical SERVICE_ACK message;

Figure 3B shows the format of a typical SERVICE_REQUEST MESSAGE;

Figure 3C shows the format of a typical OPEN_SERVICE message;

Figure 4 illustrates diagrammatically the usage of path-complete messages;

Figure 5 illustrates diagramatically the procedure for initiation of a service transfer;

Figure 6 illustrates diagrammatically the procedure for completion of a service transfer;

Figure 7 illustrates diagrammatically the procedure for establishing an incomplete

message path where an old Internet network provides the service;

Figure 7A illustrates the typical format of a typical OPEN_OLD message;

Figure 8 illustrates diagrammatically the use of an incomplete message path;

Figure 9 illustrates diagrammatically the sending a SERVICE_REQUEST via an old Internet network;

Figure 10 illustrates diagrammatically the establishment of an incomplete service delivery message path; and

Figure 11 illustrates diagrammatically the delivery of service via an incomplete message-path.

The "connection-oriented" requirement

The provision of an efficient on-demand service will require Internet "sessions" to use virtual-message-paths that must be opened and closed in a manner similar to the establishment of calls in a telephone network enabling the network to refuse traffic which exceeds the available capacity and ensuring that established sessions will not be violated.

Charging is another aspect of the future Internet that will require sessions to be opened and closed. Internet Providers will record the traffic at network terminals and at gateways to other networks for charging purposes, but will need to know which end terminal originated each active session; - that is "which end is paying?"

The simple-session requirement

Perhaps the majority of Internet usage will continue to be where a user establishes

a virtual-message-path across the Internet to conduct a simple one-to-one session.

The present method of gaining access to remote information during a simple session is for the terminating end to open a session with the remote source and relay information as required. This method is known as "chaining".

Alternatively, the terminating end may send to the user the address of the remote information. The user is required to end the current session and open a session with the new address to obtain the information. Returning an Internet address in this manner is known as "referral".

"Chaining" and "referral" will continue to be used in the future but in many cases it will be preferable to use the proposed means of "special-service" delivery.

The "special-service" requirement

In many cases, an Internet user may merely know that he wishes to buy software, insurance, or contact a large multi-national business organisation and will need to open an initial session with a broker or receptionist in order to proceed.

Having interrogated the user to identify the service required, the Broker/Receptionist may not need to participate in the ensuing activity but may be unwilling to use "referral" as this would give information to the user that could be used, or misused on future occasions.

e.g. the user could bypass the Broker on future occasions.

the user could pass the information to other users.

the user could amend the information to gain access to other services provided by the Server.

the information may enable privileged access to the service and privilege charges to be applicable.

"Chaining" may also be unacceptable. Apart from the additional handling and resources involved, the Server may be unwilling to deliver its service via a Broker and may require to deal directly with the user.

Service delivery requires that the user can be transferred from Broker to Broker and from Server to Server as service delivery proceeds, without being involved in the transfer activity.

OUTLINE OF SPECIAL-SERVICE IMPLEMENTATION

"Special-service" sessions will be established in reverse.

When a user requests access to a special-service, the special-service will be given identifiers enabling it to establish a virtual-message-path through the Internet to pick-up

the virtual-message-path from the user at the user's Internet Router (a message switching node of the Internet).

As the session proceeds, the identifiers may be passed from Broker to Broker and from Server to Server, enabling the user to be transferred from one to the other, or enabling other Brokers or Servers to be brought into the session.

This basic concept of special-service delivery is very simple, but because the present Internet is not connection-oriented, a detailed description of its implementation requires that the creation of a virtual-message-path for a simple session is described and that the method of interworking with existing equipment is included.

After accommodating the introduction of new transport layer protocols and reviewing the requirements of special-services in the Internet name and address structure, the implementation is detailed in three parts.

Part 1. Creating a virtual-message-path.

Part 2. Special-services.

Part 3. Accommodating existing equipment.

TRANSPORT LAYER PROTOCOL MIGRATION STRATEGY

In order to accommodate existing Internet equipment, all new equipment (hosts and Routers) will continue to handle the existing protocols (IP/TCP etc).

As the penetration of new style equipment increases, new transport layer protocols will be introduced which are more suited to a connection-oriented environment, but some time will elapse before such protocols are universally available.

The old protocols will continue to be used when no other protocol is mutually available. When old protocols are used in a connection-oriented manner, the IP header is redundant and should be ignored or even omitted. (It would be used only to make a checksum

To accommodate the introduction of new protocols, when opening a session, a user will indicate in the OPEN message the old and new protocols available for the transport layer session. The distant end will indicate in the OPEN_DONE message the chosen mutually available protocol. (If old network equipment is encountered, the session will use old network protocols)

INTERNET NAMES AND ADDRESSES

Internet names

To send a message or open a session in the Internet, a user provides the Internet name of the distant end. The intitial task in any activity is to consult a cache or Domain

Name Server to obtain the Internet address. As a result the choice of an Internet name is, and will remain, rather arbitrary.

Internet addresses

User addresses (See Figure 1)

For the majority of Internet users, the more significant bits of the user's address (netID) will identify the user's Router; the lesser bits (hostID) identifying the user's terminal.

The user's Internet address will not identify a particular Router if the user is connected to an elongated private network that gains access to the Internet via several Routers.

Such users present no problems for simple Internet sessions; whichever Router is used to establish a virtual-message-path at the start of the session will be the Router used throughout the session. However, when users have to be picked-up for special-service delivery, the user's address must identify the Router that invoked the service.

To accommodate special-service delivery to such users, each Router will allocate one address from its own address range. This address will be used by the Router as the USER'S INTERNET ADDRESS in all the SERVICE-REQUEST messages that it creates to invoke service delivery to such users; the address could in fact be used in all SERVICE-REQUEST messages. (The request message includes a reference number

enabling the user to be identified when service delivery arises)

Special-service Addresses

The future Internet address structure will include "networks" (netIDs) that are lists of Brokers and Services but have no relation to the location of the Routers and Servers. A single address (hostID) within such network might identify all the worldwide services provided by General Motors of America, adjacent addresses identifying Siemens of Germany, Reuters News Agency or Mitsubishi of Japan.

Thus, the netID part of the address is merely a "special-service" identifier and the hostID part is no more than an index number identifying the service.

PART 1

CREATING A VIRTUAL-MESSAGE PATH (See Figure 2)

The host/Router link

Internet terminals are called "hosts". A host may be a simple PC capable of little more than one task at a time; an ISDN type terminal with several ports, each capable of several sessions; or a mainframe computer with innumerable hardware and software "ports", each capable of countless simultaneous sessions.

Whatever the configuration, a session within a host can be uniquely identified by a "port" and "session" number.

A "session-reference number" identifies a session on the link between a host and its parent Router. All messages sent or received during a session will have the session-reference number in the host/Router link header. The reference may be supplemented by a sub-session number during multi-sessions.

The host relates the session-reference to the appropriate port and session, the Router relates the host/session-reference to the route and virtual-channel-number (VCN) that forms the next link in the chain toward the distant end.

The session-reference number will be allocated by the host on originating sessions or by the Router on terminating sessions.

The host/Router link header might appear as shown in Figure 2A.

The control flags may be used as follows:

00 - ordinary message packet (new version)

10 - session control message (OPEN/CLOSE etc.)

01 - (not used)

11 - old version message packet (no session-reference)

A host passes control messages (OPEN/CLOSE) received from the Internet to its control port. On hosts which deliver special-services, this port will require a standard port number in order to allow new version SERVICE-REQUEST messages to be received

via old version Internet equipment.

The OPEN message

To open a virtual-message-path through the Internet, a host sends an OPEN message to its Internet Router. The message contains the distant host's address and port number which are derived from the Internet name and protocol indicator (ftp, http, etc) specified by the user.

As new transport layer protocols are introduced, more than one protocol indicator might indicate the same port (ftp, newftp). The OPEN message will list the different protocols that are available at the user end and the distant end will indicate the chosen protocol in the OPEN DONE message. A typical OPEN MESSAGE is shown in Figure 2B.

VCN Allocation

Each Router uses the distant-host-address in the OPEN message to identify the route towards the destination and allocates a VCN to identify the session on the link to the next Router. The OPEN message is then passed on the control channel (VCN 0000) to the next Router in a message packet carrying the allocated VCN where the process will be repeated.

At the link level, an OPEN message being passed from Router to Router might appear as shown in Figure 2C.

Messages received on a link's control channel (VCN 0000) will be passed to the Router's session processor for attention.

To avoid VCN collisions, the Router at one end of a link may allocate VCNs in the range 0001 - 7 FFF while the Router at the other end allocates 8000 - FFFF. (This assumes that VCN 0000 is used in both directions for control messages.)

To accommodate the existing and other network-layer protocols, link implementation may find it convenient to allocate a separate control VCN for each protocol. Messages received on such VCNs will be passed directly to the appropriate handler.

All subsequent control messages - in either direction - will be sent on the control channel in a similar manner, with the link header being followed by the RELEVANT VCN and the control message itself.

OPEN_DONE

Reserving capacity

Routers will reserve capacity (in terms of anticipated mean bits per second) on the links employed as indicated in the OPEN_DONE message, and will refuse traffic which exceeds the capacity available.

A Router will convert an OPEN_DONE message into a FAILURE message if it

finds that it cannot provide the capacity indicated in the OPEN_DONE message. Upon receiving a FAILURE message the originating host will be required to send a CLOSE message to release the established part of the message-path.

Using the message-path

Once a message-path is established, the originating host will open a transport layer session. Message packets will be passed from Router to Router with the Link Header indicating the allocated VCN. Each Router will replace the incoming VCN with the outgoing VCN as the message is switched as shown in Figure 2D.

Diverting a message-path

2nd OPEN_DONE message

To OPEN a simple Internet session, a user may need to OPEN an initial session with the distant host's Port Mapper in order to learn the appropriate port number.

With new equipment, the distant host should be able to divert the Port Mapper session to the required port without requiring the user to re-open the session.

There may be need for a control message to change the chosen protocol and reserve appropriate network capacity.

The message content will be seen to identical to the OPEN_DONE message. Hosts and Routers should be prepared to accept a second such message, including that a

Router may change the message to a FAILURE message if it finds that it cannot provide the required capacity.

An OPEN_DONE message may also be sent to a host more than once during special-service delivery when a session is transferred from one Server to another.

Closing the message-path

When the session ends, the transport layer session will be closed followed by closure of the virtual-message-path.

Message-paths are controlled by the originating terminal and closed by the exchange of CLOSE and CLOSE_ACK messages. The CLOSE_ACK message being returned on a per link basis.

The terminating end may invite closure with a CLOSE_REQUEST message.

PART 2

SPECIAL SERVICES (See Figures 3 & 4)

INVOKING SPECIAL-SERVICE DELIVERY

To open a special-service session in the Internet, a host sends an OPEN message to its Internet Router as normal. The message includes the distant-host-address derived from the Internet name specified by the user.

When the user specifies the name of a special-service, the netID part of the distant-host-address will be a "special-service" identifier.

Upon receiving a "special-service" address, the Router returns a SERVICE_ACK message to the host (Figure 3A) and sends a SERVICE_REQUEST message (Figure 3B) to the nearest "Sorter". (A Sorter is located with any convenient Router and has an address in the range used by any other host connected to that Router.)

The SERVICE_ACK message

The SERVICE_ACK message contains no parameters. It informs the user that the session may involve more than one transport layer session and that the initiative to open and close those sessions will be at the distant end. The user must assume the default situation - that messages will be sent and received via old network equipment and will have IP/TCP type headers.

All messages sent or received during the session (old protocol or otherwise) will use the current message-path; with link headers quoting the SESSION_REFERENCE and the control bits set to 00 (or 10 for new version session control messages).

The SERVICE_REQUEST message

The SERVICE_REQUEST message contains:

(i) the special-service address

(ii) the REQUEST REFERENCE number (See NOTE)

(iii) the user's Internet name (prime user's name)

(iv) the user's Internet address (this may be an address used by the Router in all SERVICE_REQUEST messages)

(v) the transport layer protocols available

Items i and v are taken from the user's OPEN message,

Items ii, iii & iv are provided by the Router.

NOTE The REQUEST_REFERENCE number identifies the Router's current session-record.

To enable service delivery via old network equipment, the REQUEST_REFERENCE number takes the form of an Internet address, the net ID part of the address identifies the Router, the hostID is the reference number. Request-reference numbers occupy only a small part of the hostID range, the greater part being used by the hosts connected to the Router.

The Sorter opens the SERVICE_REQUEST message to identify the special-service address and uses a look-up table to re-address the message to the appropriate Broker or Server.

In the case of services which are provided by other network operators or in other countries, the Sorter will re-address the message to a Sorter in that network or country; there is no need for internetwork management of Sorters.

SERVICE_REQUEST messages use the control channel like any other control message and create a message-path as they are passed via Routers and Sorters to the Server; each Router and Sorter allocating a VCN or session reference as necessary.

The message-path created by the SERVICE_REQUEST message is used only as the RELEVANT_VCN to return the REQUEST_DONE or FAILURE message from the Server via the Sorter to the originating Router. The originating Router will CLOSE the path when the returned message is received. No capacity is reserved for the SERVICE_REQUEST session.

ESTABLISHING THE SERVICE DELIVERY PATH

The OPEN_SERVICE message

Upon receiving the SERVICE_REQUEST message, the Broker or Server will choose the protocol to be used and establish a message-path to the user via the Internet with an OPEN_SERVICE message.

The OPEN_SERVICE message, see Figure 3C, contains:

(i) the user's address as DISTANT-HOST-ADDRESS

(ii) the user's Internet name

(iii) the originating Router's REQUEST_REFERENCE number

(iv) the transport layer protocol to be used for service delivery

(v) the capacity and switching priority to be reserved by the Routers.

Items (iv) and (v) are valid only if a complete virtual-message-path can be

established and are used only after being transferred to an OPEN_DONE message.

The OPEN_SERVICE messages will be treated as a normal OPEN message by all Routers except the final Router that connects to the user or LAN. This Router uses the REQUEST_REFERENCE to find the session record, verify the USER's INTERNET NAME and pick-up the message-path to the user.

The OPEN_DONE message

OPEN_DONE to the Server

The Router then returns an OPEN_DONE message to the Server. The message repeats the protocol, capacity and priority fields from the OPEN_SERVICE message and is used by all Routers to reserve the necessary capacity. To the Server, the message confirms the protocol to be used and indicates that a complete virtual-message-path has been established.

OPEN_DONE to the user

The same OPEN_DONE message will be sent to the user but with the forward and backward capacity and priority fields reversed (the capacity and priority may be required by a LAN Router).

The message tells the user which transport layer protocol will be used for service delivery and overrides the default old network protocol established by the SERVICE_ACK message. At the end of the transport layer session, the user must revert

to the default.

Control message interface

The user's Internet Router will be required to provide an interface for subsequent control messages as both the user and Server will consider themselves to the session originator. For charging purposes, the session must be considered to be originated by the Server.

The REQUEST_DONE message

Having received OPEN_DONE indicating that the message path is complete, the Server will return a REQUEST_DONE message to the originating Router using the message-path created by the SERVICE_REQUEST; that path will then be closed.

Delivering the service

Using the established message-path, the Server will open a transport layer session with the user to commence service delivery. This will often involve interrogating the user to further identify the service required after which the user may be transferred to another Server.

SERVICE TRANSFER (See Figures 5 & 6)

THE TRANSFER_REQUEST message

A Server transfers a user to another Server by closing the transport layer session and sending a TRANSFER_REQUEST message to the other Server. The

TRANSFER_REQUEST message contains the same information as the original SERVICE_REQUEST message, but indicates that the existing message-path must be diverted.

The message will usually be addressed directly to the other Server, but may be addressed via a Sorter as before, in which case the SPECIAL_SERVICE_ADDRESS field must be updated.

The message packet may include information obtained during the earlier session and indicate which party is expected to pay for the transferred service. All such information is of no consequence to the Internet.

The TRANSFER_REQUEST message will be forwarded to the new Server and a message-path created for the return of the REQUEST_DONE or FAILURE message.

The OPEN_TRANSFER message

The new Server will use a OPEN_TRANSFER message to establish a message-path via the Internet to the user. The message content is the same as an OPEN_SERVICE message and is treated as an ordinary OPEN message by all Routers except the final Router that connects to the user or user's LAN. This router uses the REQUEST_REFERENCE number to find the session record, verify the USER'S INTERNET NAME and complete the virtual-message-path to the user.

OPEN_DONE, REQUEST_DONE and CLOSE_REQUEST messages

Having completed the new message-path, the Router will send an OPEN_DONE message to the new Server and to the user as before, and will send a CLOSE_REQUEST message to the old Server on the old message path. (If the previous session uses old network procedure, no CLOSE_REQUEST message can be sent.)

The previous Server will CLOSE the old message-path when the CLOSE_REQUEST message is received.

Upon receiving the OPEN_DONE message, the user will cancel the default situation (restored when the previous transport layer session was closed) and await the opening of a new transport layer session using the protocol indicated in the OPEN_DONE message.

When the new Server receives the OPEN_DONE message, it will send REQUEST_DONE to the old Server on the TRANSPORT_REQUEST message-path and will commence service delivery.

After receiving REQUEST_DONE, the old Server will close the TRANSFER_REQUEST message-path.

Subsequent transfers

The session transfer activity may be repeated any number of times.

PART 3

ACCOMMODATING EXISTING EQUIPMENT

To interwork with existing equipment, new version hosts and new version Routers must be able to handle the existing procedures and must be able to receive and send old version messages. Control flags indicate the presence of old version messages on host/Router links; on links between Routers, old version messages use a special VCN.

A SIMPLE SESSION IN THE UNKNOWN INTERNET (See Figure 7)

Although capable of old network procedures, new version hosts will never initiate old version sessions. Even when a session is known to involve old version equipment, a new version host will try to establish a virtual-message-path, thereby ensuring as far as possible the continuity of the session. (If only the distant host were old version equipment a virtual-message-path could be established right across the Internet.)

The OPEN message

When a new version host sends an OPEN message into the Internet, a message-path will be established to the distant host or to the point that the path meets old version equipment.

If the path meets old version equipment, the Router at the interface to the old equipment completes the path to the old network route and returns OPEN_OLD to the originating end.

The OPEN_OLD message

The OPEN_OLD message, see Figure 7A, informs the user that the message-path is open but is not complete and that old network procedures must be used. The message includes a field that must be used as the SOURCE_ADDRESS in the IP Headers; it identifies the interface Router and its session-record number. (Similar to the REQUEST_REFERENCE number in SERVICE_REQUEST messages.)

The OPEN_OLD message also indicates nominal capacities and priorities to be reserved by the Routers.

Once an interface to old version equipment has been provided, it is not possible to return to the new version procedures if later equipment has new version capability.

Conducting the session (See Figure 8)

The user will send and receive messages with IP/TCP type headers on the established virtual-message-path. (With the link-header using the SESSION-REFERENCE and the control bits set to 00.) The DESTINATION_ADDRESS in the IP header will be the same as the distant-host-address in the OPEN message, the SOURCE_ADDRESS will be that provided in the OPEN_OLD message.

Forward messages

Upon receiving forward messages from the user, the Router at the interface will pass the messages to the old network route. The messages will continue to their

destination using old network procedures.

Backward messages

Messages returned from the distant end will be addressed to the SOURCE_ADDRESS given in the forward messages, which identifies the interface Router and its session-record number. Upon receiving the returned messages, the interface Router will find the session-record and return the messages, with headers, to the user on the established virtual-message-path.

Closing the session

When the session ends, the originating host will CLOSE the message-path to the interface Router in the normal manner.

A SPECIAL-SERVICE SESSION IN THE UNKNOWN INTERNET

INVOKING THE SPECIAL-SERVICE

When a new version host attempts to OPEN a session with a special-service address, the Internet Router addresses a SERVICE_REQUEST message to the nearest Sorter which re-addresses the message to an appropriate Server.

If an old version host attempts to gain access to such a service, the special-service address will appear in the DESTINATION_ADDRESS of an IP header received by a new or old version Router. A variety of treatments are possible, but are not detailed herein.

SERVICE_REQUEST via old network (See Figure 9)

IP/UDP Header

If the message path from the Router via the Sorter to the chosen Server encounters old version equipment, the Router at the interface will prefix the SERVICE_REQUEST message with an IP/UDP Header and forward it via the old version equipment.

For this purpose, new version Routers will have a ready-made IP/UDP Header. The Router will be required to complete the DESTINATION_ADDRESS, CHECKSUM and LENGTH fields each time the header is used. The ready-made header may also be used to forward TRANSFER_REQUEST messages.

A Sorter will be required to accept IP/UDP messages only when old network equipment exists in the path between the Sorter and the Routers which it serves; or when SERVICE_REQUEST messages are received from Sorters in other networks or other countries. Having received a request message using IP/UDP, the message should be forwarded to the Server in the same manner.

The SERVICE_REQUEST message will be delivered using the IP/UDP protocol to the Server's control port (a standard port number on special-service equipment.)

The ACK_OLD message

Servers do not acknowledge SERVICE_REQUEST messages delivered by IP/UDP. Having forwarded the message, the interface Router will return ACK_OLD to

the originating Router.

The ACK_OLD message has no parameters. The originating Router will CLOSE the partly established REQUEST message-path (used only to return DONE or FAILURE messages from the Server) and await the commencement of service delivery; a time-out and escape procedure being available if no response arises.

SERVICE DELIVERY VIA OLD NETWORK (See Figure 10)

THE OPEN_SERVICE message

Having received the SERVICE_REQUEST message (by whatever means), the SERVER will attempt to open a message-path to the user by sending a OPEN_SERVICE message into the Internet.

If the message-path meets old version equipment, the Router at the interface to the old equipment will complete the path to the old network route and return OPEN_OLD to the Server.

The OPEN_OLD message

The OPEN_OLD message informs the Server that the message-path is not complete and that old network procedure must be used.

The message gives nominal capacity and priority reservations and includes a field that must be used by the Server as the SOURCE_ADDRESS in the IP headers. The

address identifies the interface Router and its session-record.

Upon receiving the OPEN_OLD message, the Server will return REQUEST_DONE to the request message source. (If the request message delivery had encountered old-network equipment, it will not be possible to return a REQUEST_DONE message.)

Conducting the session (See Figure 11)

Forward messages

The Server will commence service delivery using the part established message-path. (i.e. The link header will hold the session_reference number with the control bits set to 00.)

Each message packet will have an old version IP/TCP type header. The DESTINATION_ADDRESS in the header will be the originating Router's REQUEST_REFERENCE number received in the SERVICE_REQUEST/TRANSFER_REQUEST message. The SOURCE_ADDRESS will be that received in the OPEN_OLD message, identifying the interface Router and its session-record.

The interface Router passes messages received from the Server into the old network which forwards the messages to the originating Router as identified by the DESTINATION_ADDRESS.

The originating Router recognises that the DESTINATION_ADDRESS in the forward messages is a REQUEST-REFERENCE number. It finds the session-record and passes the messages to the user on the established message path, albeit only one link. (The link headers hold the session-reference number with the control bits set to 00.)

The user will be in the default situation and will be expecting service delivery using old network protocols. The port and session to which the messages belong will be identified by the session-reference number in the link header; the IP Header in the forward messages will be used only for checksums and to provide the address for returned messages.

Backward messages

To simplify the handling of backward messages, the originating Router will record in its switching table the route from which forward messages are received. The table must be updated each time a forward message is received as the route may change without notice if service delivery is transferred to a Server which also needs to use old network procedure.

Messages returned to the Router from the user will have IP/TCP type headers and will use the established one-link message-path (the link-header holding the session-reference and the control bits set to 00). The DESTINATION_ADDRESS will be the SOURCE_ADDRESS received in the forward messages which identifies the interface Router and its session-record.

The Router will send the messages into the Internet using old-network procedure.

When the interface Router receives the messages it recognises that the DESTINATION_ADDRESS is a session-record and returns the messages to the Server on the established message-path.

Closing the previous message-path (if any)

If the service delivery were the result of a service transfer, the originating Router's records would hold references to the path used for the earlier session. The records will be updated and a CLOSE_REQUEST message sent on the previous message-path.

The previous Server will CLOSE the previous message-path when it receives the CLOSE-REQUEST message.

If the previous session encountered old-network equipment, no CLOSE_REQUEST message could be sent. The previous Server would CLOSE the previous incomplete message-path after receiving REQUEST_DONE from the new Server; or after receiving ACK_OLD in response to its TRANSFER_REQUEST message indicating that REQUEST_DONE would not be received.

Closing the session

When the service-delivery is complete, the final Server will CLOSE the part

established message-path in the normal manner. The user will CLOSE the host/Router link when no more transfers are expected.

MULTI-SESSIONS

A user may establish several simultaneous sub-sessions in the pursuit of a session. No special handling is required in the Internet as the user would be able to relate the different Internet sessions as being part of one master-session.

A multi-session may also be formed by a special-service Server adding other Servers instead of transferring to other Servers; or by a mixture of user and Server created sub-sessions.

A Server adds another Server by sending an ADD_REQUEST message to the new Server containing the same information that would be contained in a TRANSFER_REQUEST message.

The new Server will establish a message-path to the user with an OPEN_ADD message containing the same information that would be contained in an OPEN_TRANSFER message.

The user's Router will return an OPEN_DONE message to the new Server which will send REQUEST_DONE to the Server that initiated the ADD.

The user's Router will also allocate a sub-session number before sending an ADD_DONE message to the user containing similar information to that contained in the OPEN_DONE message.

Upon receiving the ADD_DONE message, the user's host will open a sub-session as indicated by the SESSION_REFERENCE and sub-session number in the link header.

The ADD facility is dependent upon new version equipment. There is no means of separating the different sub-session windows if old version equipment is encountered.

THE FUTURE INTERNET - CHARGING

Basic charges

Internet users will pay a fixed-fee to their Internet Provider and will probably pay an additional usage charge, each session being charged to the session originator.

Session charges will depend upon the time that a session remains open (and upon the number and size of the messages carried). Session charges should be sufficient to deter users from blocking network resources by keeping sessions open unnecessarily.

Special-service charges

Sessions originated by Brokers or Servers in response to service or transfer request messages will be charged to the Broker or Server. Some Service Providers may choose to pay the session charges (like Freefone in the telephone network) while others

may not only pass-on the session charges to the user but levy an additional charge for the actual service delivered (like Premium Rate services).

Collecting Service Provider's charges

To deliver special-services, Brokers and Servers are given the user's Internet name/address. Most simply, the charge for the service should be collected from that name/address.

Collecting service delivery charges on behalf of the Service Providers could be a very attractive and very profitable service provided by the Internet Operators.

Recording the charges levied by Servers for service delivery will be the responsibility of the Service Providers - not a problem for the Internet! (A Broker may elect to pay for a session between a Server and a user - then add commission before charging the user.)

SECURITY

User identity verification

The user-friendliness and commercial security are interdependent and lie in the fact that services are delivered directly to the user who has no knowledge of the service's source or the detail of its invocation. The Server is given the user's identity which is verified by the user's Internet Router from the session records.

Breaching security

The commercial security of the procedure is in part attributable to the fact that services are delivered to a verifiable user name.

This verification is not possible when services are delivered via old version equipment as the DESTINATION_ADDRESS in the IP header is a session-record reference number and the user's identity is not included.

Also, when message paths are established via old version equipment, the user is given a session-record reference number to use as the SOURCE_ADDRESS in IP headers.

Having established a message-path via old version equipment, a knowledgeable and meddlesome user could extricate this session-record reference number and use it to build SERVICE or TRANSFER_REQUEST messages with a bogus user-name.

The user may also cheat the system when services are known to be delivered via old version equipment, by sending REQUEST messages to Servers containing a false user's name and address but with the true address in the REQUEST_REFERENCE field. This method may not be so attractive to a dishonest user as it requires revealing the true address.

Servers must be aware that the user's identity cannot be verified when services

are delivered via old network equipment.



CLAIMS

1. A communications network comprising means for interconnecting a user computer terminal to a further computer terminal, which further computer terminal is one of a plurality of computer terminals connected in the network, wherein a virtual message path is established from the further computer terminal to the user computer terminal in response to an open message sent from the user computer terminal to a user router which sends a service request to the further computer terminal via one or more further routers.

2. A communications network as claimed in Claim 1, wherein the virtual message path is established using network provided references.

3. A communications network as claimed in Claim 1 or 2, wherein a special service request is sent from the user router to a sorter, which sorter, using information from a database held therein, readdresses the special service request to an appropriate further computer terminal connected in the network.

4. A communications network as claimed in any preceding claim, the network being the Internet.

Fig.1.

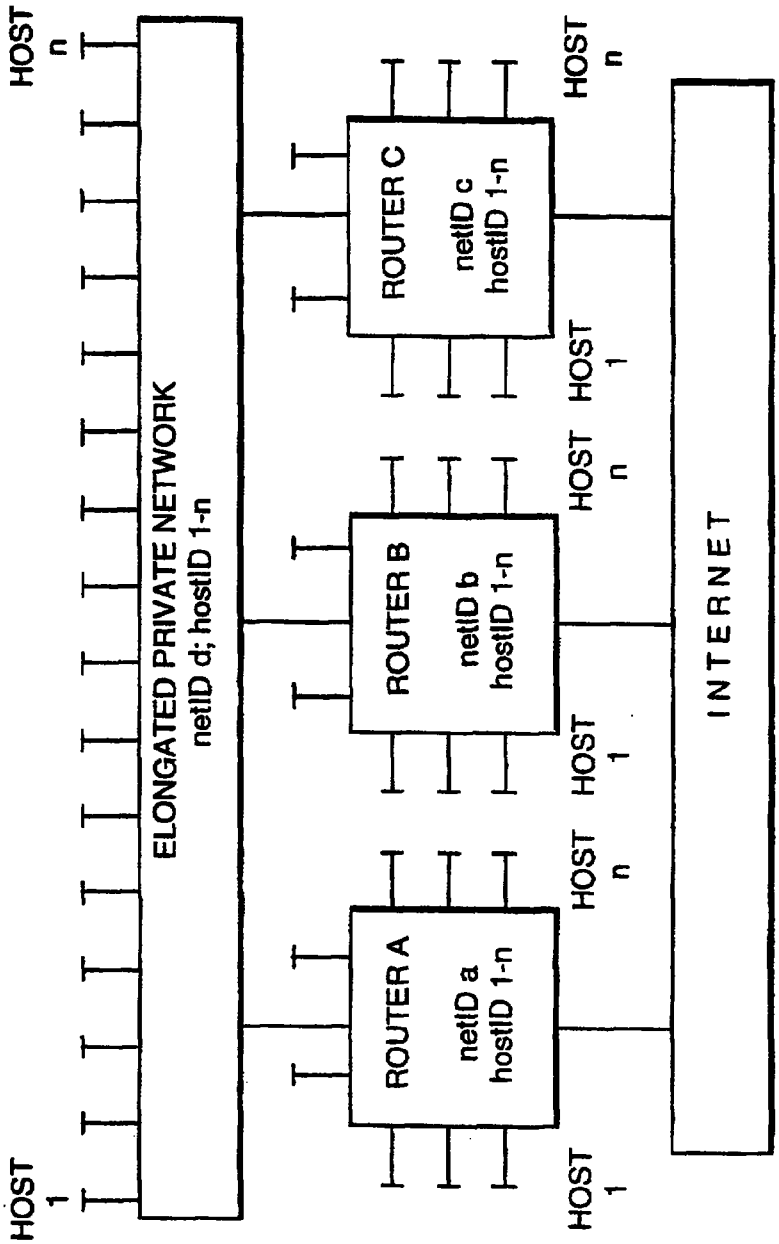

HOST n
HOST 1
ELONGATED PRIVATE NETWORK
netID d; hostID 1-n
ROUTER A
netID a
hostID 1-n
ROUTER B
netID b
hostID 1-n
ROUTER C
netID c
hostID 1-n
HOST n
HOST 1
HOST n
HOST 1
HOST n
HOST 1
INTERNET

Fig.2.

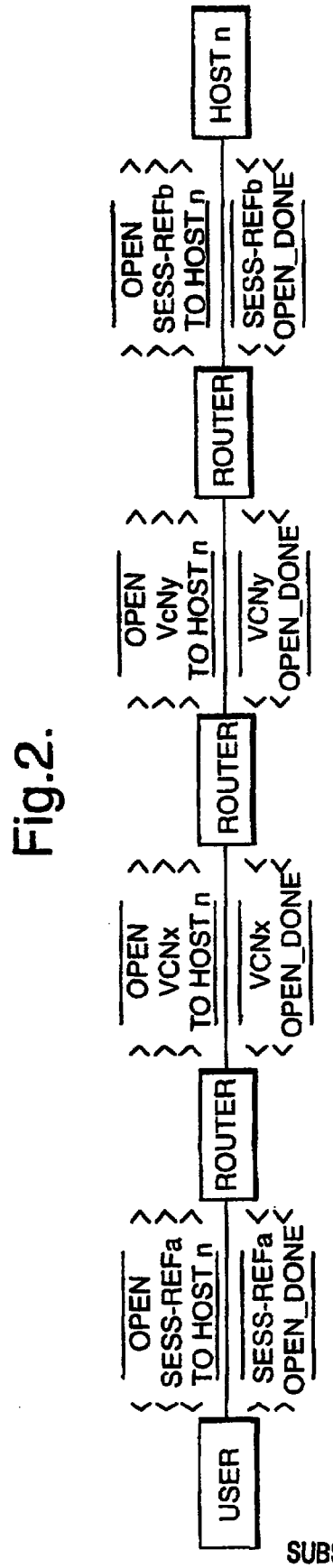


Fig.2A.

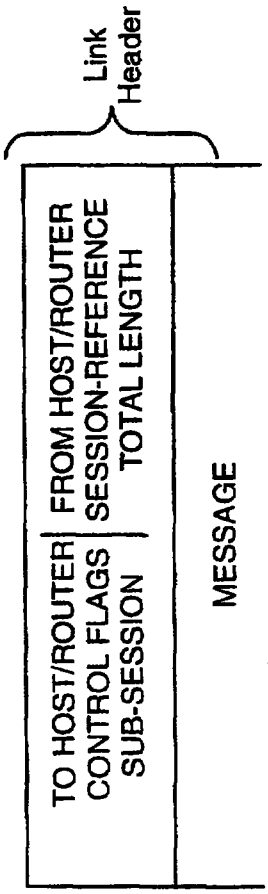


Fig.2B.

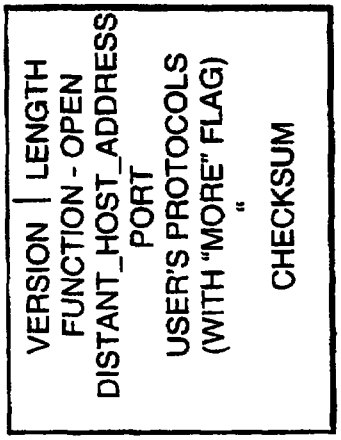


Fig.2C.

VIRTUAL CHANNEL 0000 (CONTROL CHANNEL) TOTAL MESSAGE LENGTH
ALLOCATED VCN (CHANGED BY EACH ROUTER)
OPEN MESSAGE

Fig.2D.

ALLOCATED VCN (CHANGED BY EACH ROUTER) TOTAL MESSAGE LENGTH
MESSAGE PACKET

Fig.3.

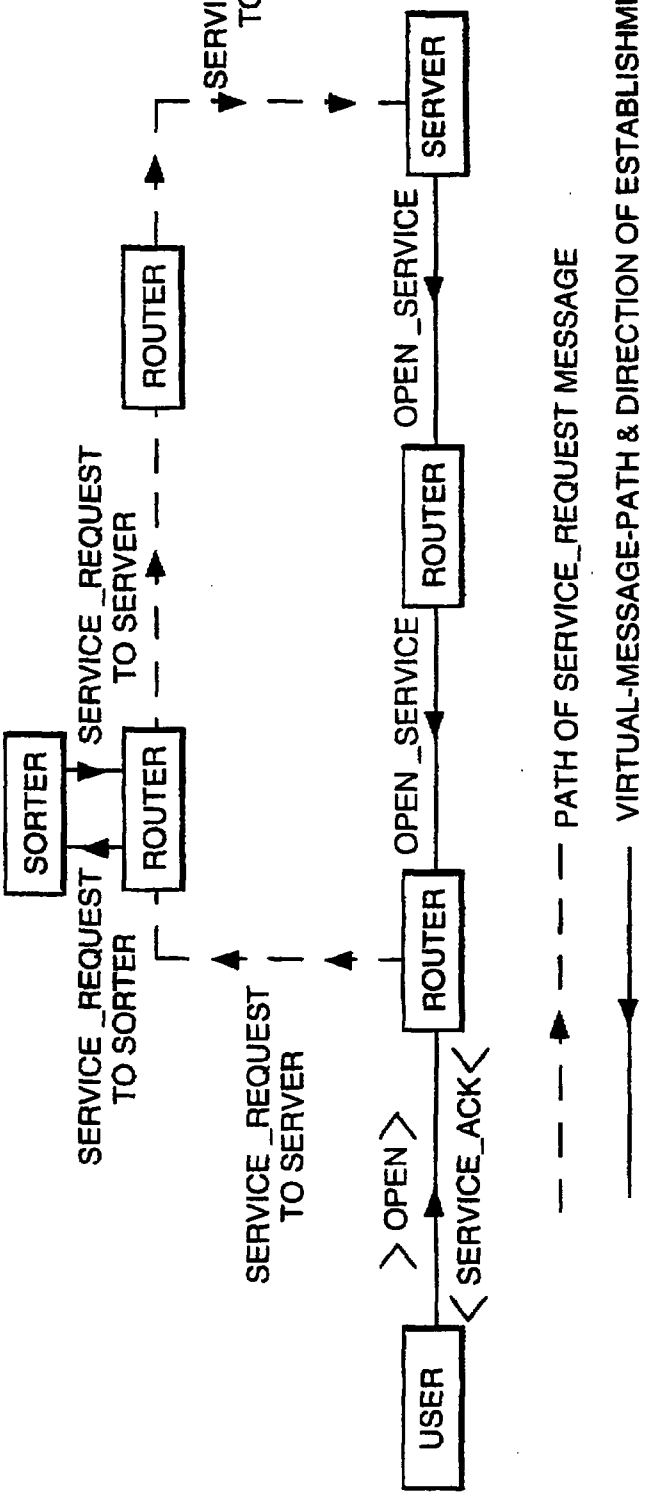


Fig.3A.

VERSION	LENGTH
FUNCTION - SERVICE_ACK	
CHECKSUM	

Fig.3B.

VERSION	LENGTH
FUNCTION- SERVICE_REQUEST	
*SORTER/SERVER ADDRESS	
SPECIAL-SERVICE ADDRESS	
REQUEST REFERENCE NUMBER	
USER'S INTERNET NAME	
USER'S INTERNET ADDRESS	
AVAILABLE PROTOCOLS	
(WITH "MORE" FLAGS)	
"	
"	
CHECKSUM	

Fig.3C.

VERSION	LENGTH
FUNCTION- OPEN_SERVICE	
DISTANT_HOST_ADDRESS	
USER'S INTERNET NAME	
REQUEST_REFERENCE	
CHOSEN PROTOCOL	
FORWARD CAPACITY & PRIORITY	
BACKWARD CAPACITY & PRIORITY	
CHECKSUM	

Fig.7A.

VERSION	LENGTH
FUNCTION - OPEN_OLD	
FORWARD CAPACITY & PRIORITY	
BACKWARD CAPACITY & PRIORITY	
SOURCE _ADDRESS TO USE	
CHECKSUM	

Fig.4.

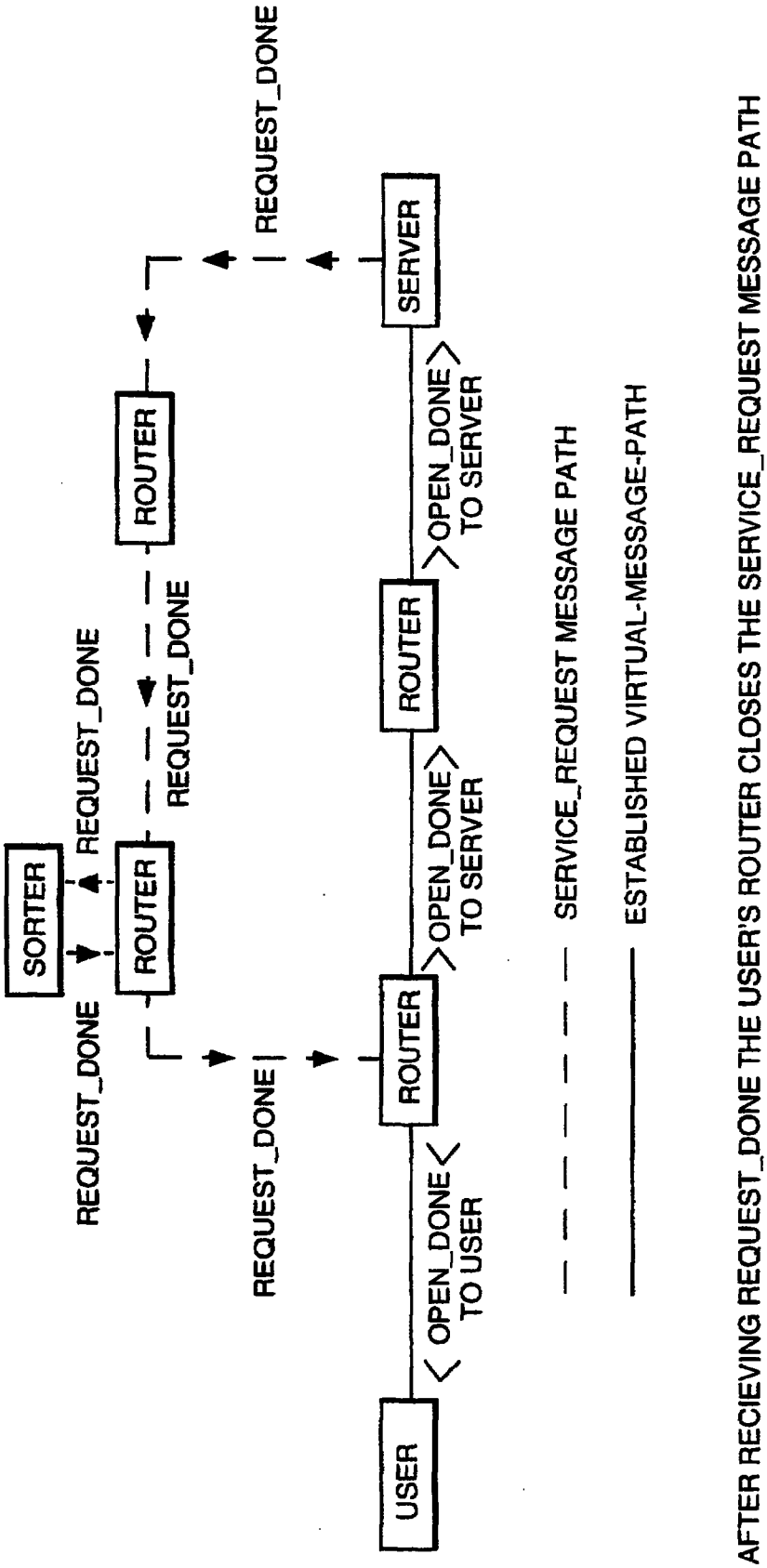

SORTER
ROUTER
ROUTER
ROUTER
ROUTER
SERVER
USER
REQUEST_DONE
REQUEST_DONE
REQUEST_DONE
REQUEST_DONE
REQUEST_DONE
OPEN_DONE TO USER
OPEN_DONE TO SERVER
OPEN_DONE TO SERVER
SERVICE_REQUEST MESSAGE PATH
ESTABLISHED VIRTUAL-MESSAGE-PATH
AFTER RECIEVING REQUEST_DONE THE USER'S ROUTER CLOSES THE SERVICE_REQUEST MESSAGE PATH

Fig.5.

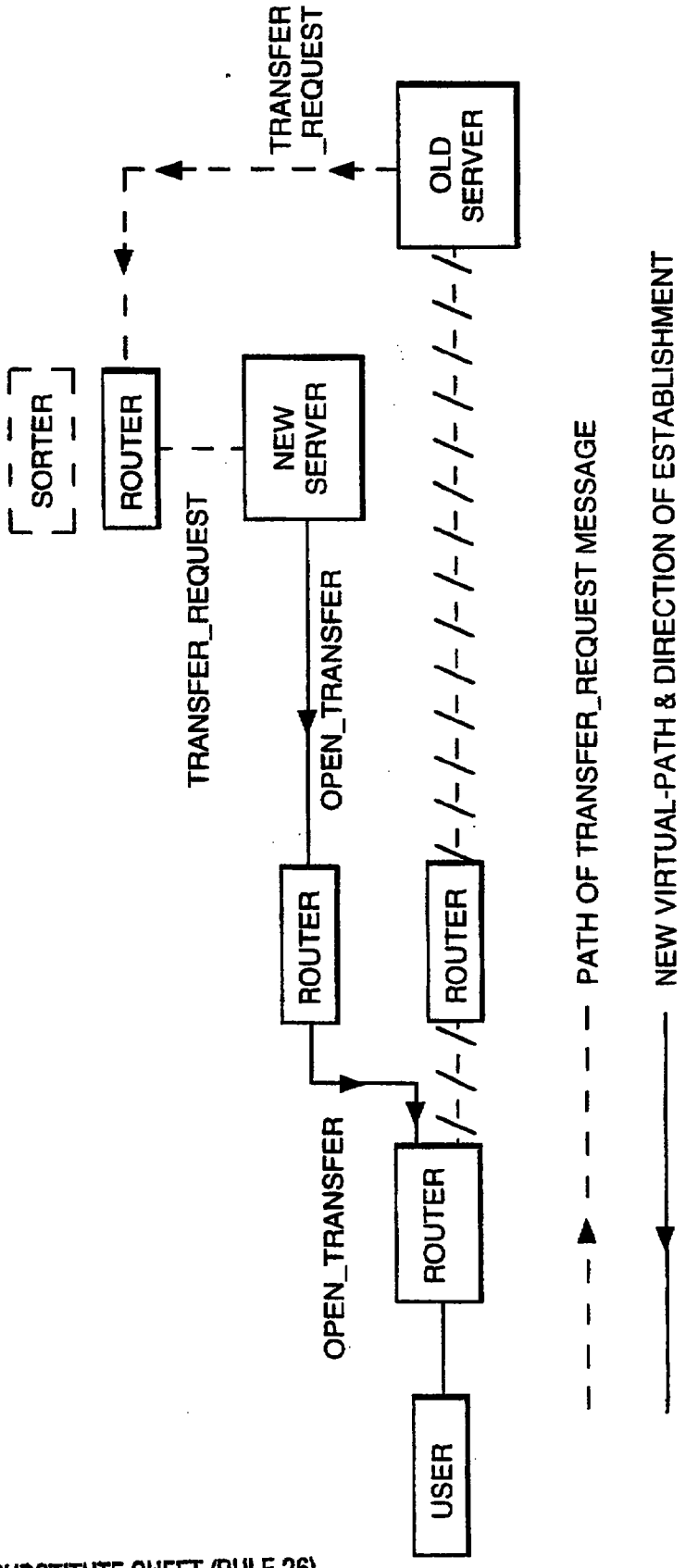

SORTER
ROUTER
TRANSFER_REQUEST
TRANSFER_REQUEST
OLD SERVER
NEW SERVER
OPEN_TRANSFER
ROUTER
ROUTER
OPEN_TRANSFER
ROUTER
USER
PATH OF TRANSFER_REQUEST MESSAGE
NEW VIRTUAL-PATH & DIRECTION OF ESTABLISHMENT
OLD VIRTUAL-PATH

Fig.6.

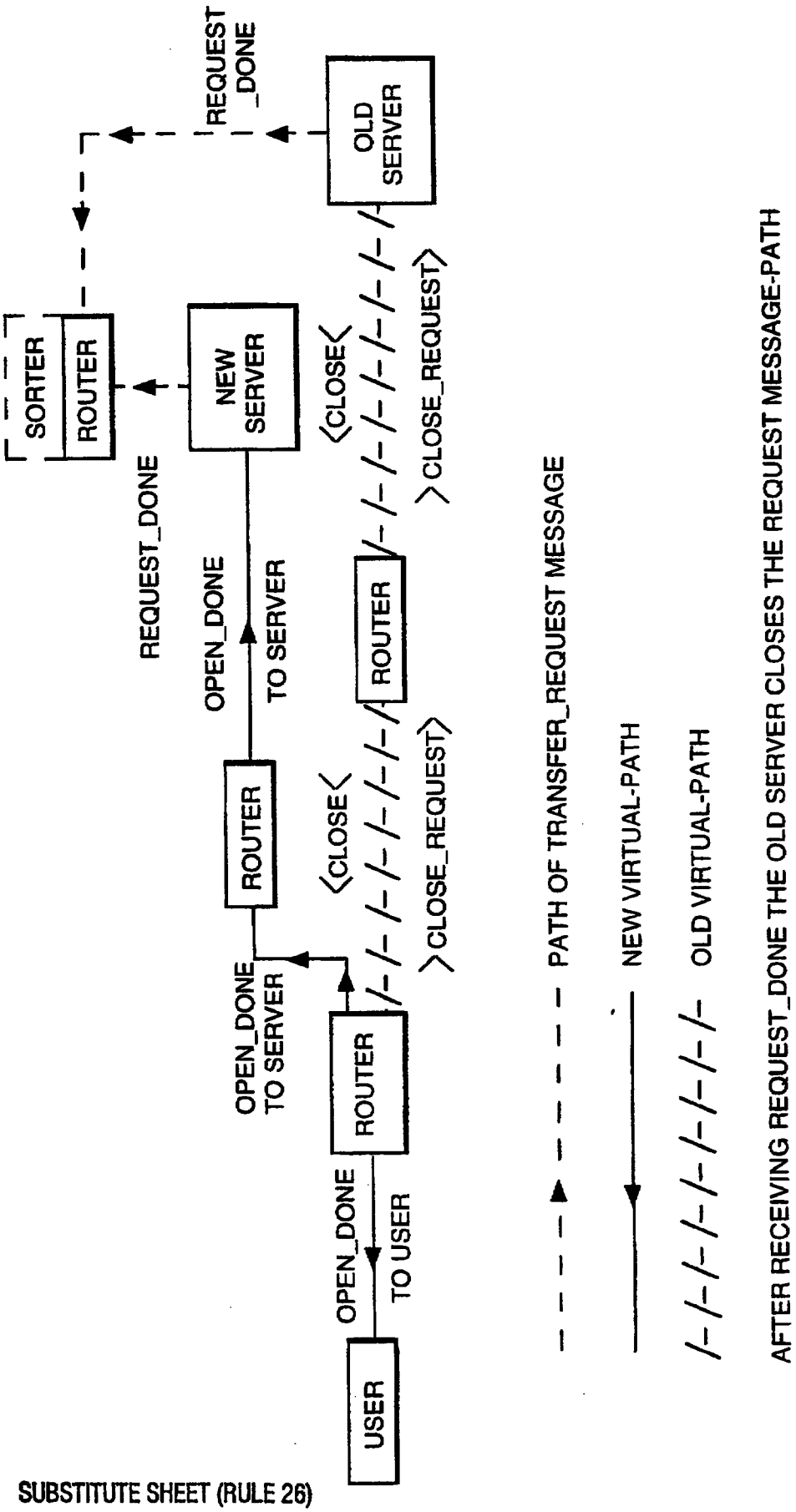

USER
ROUTER
ROUTER
ROUTER
SORTER
ROUTER
NEW SERVER
OLD SERVER
OPEN_DONE TO USER
OPEN_DONE TO SERVER
OPEN_DONE TO SERVER
REQUEST_DONE
REQUEST_DONE
CLOSE
CLOSE_REQUEST
CLOSE
CLOSE_REQUEST
PATH OF TRANSFER_REQUEST MESSAGE
NEW VIRTUAL-PATH
OLD VIRTUAL-PATH
AFTER RECEIVING REQUEST_DONE THE OLD SERVER CLOSES THE REQUEST MESSAGE-PATH

Fig.7.

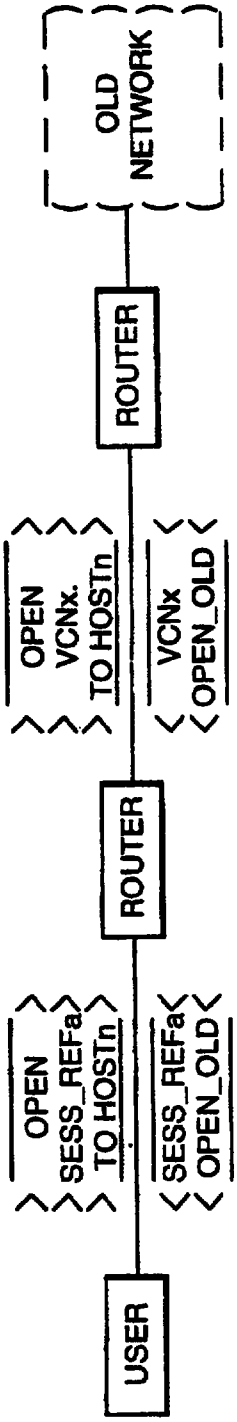
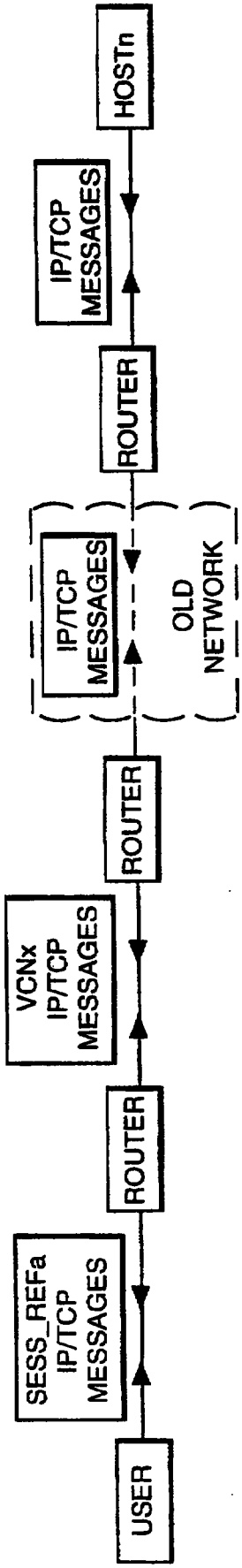

OLD NETWORK
ROUTER
OPEN VCNx. TO HOSTn
VCNx OPEN_OLD
ROUTER
OPEN SESS_REFa TO HOSTn
SESS_REFa OPEN_OLD
USER

Fig.8.


HOSTn
IP/TCP MESSAGES
ROUTER
IP/TCP MESSAGES
OLD NETWORK
ROUTER
VCNx IP/TCP MESSAGES
ROUTER
SESS_REFa IP/TCP MESSAGES
USER

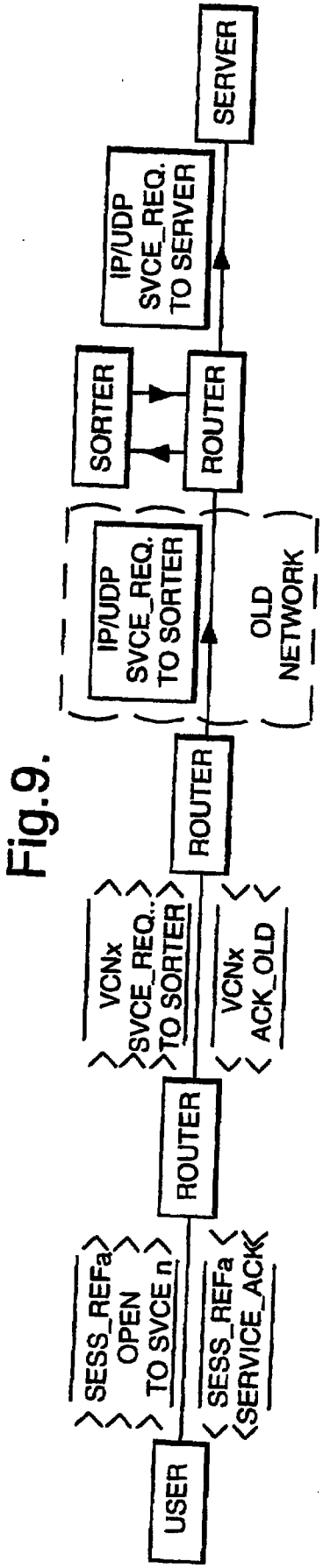


Fig.9.

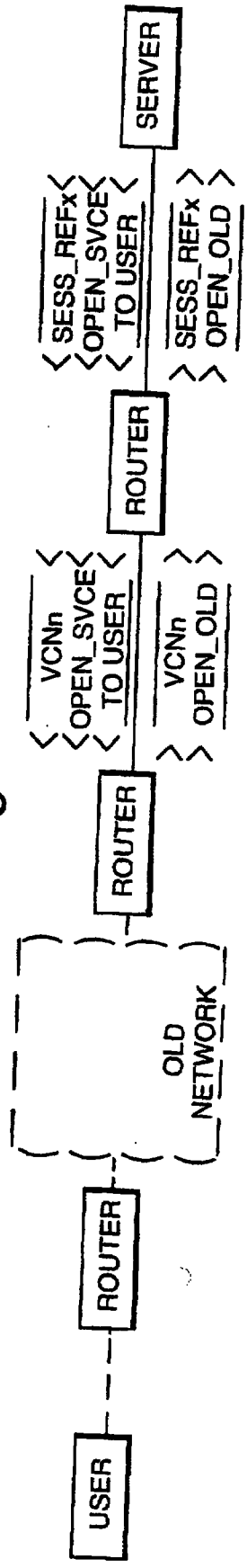


Fig.10.

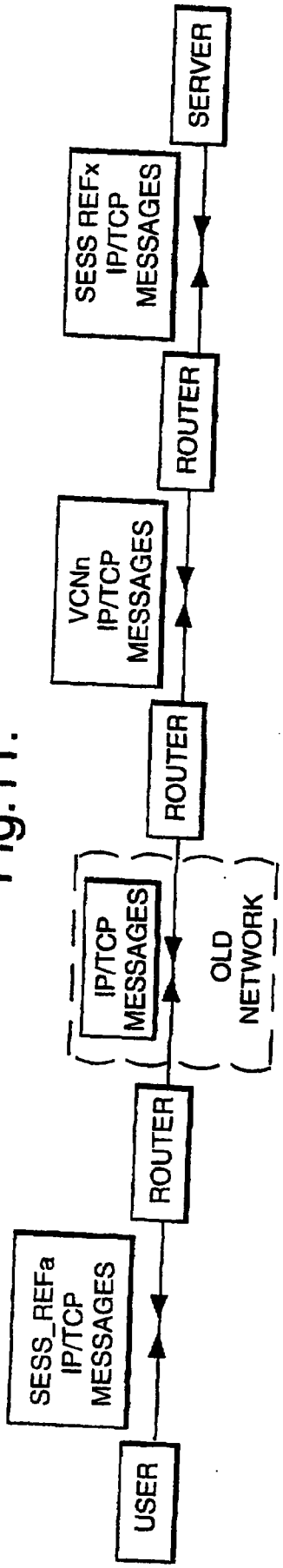


Fig.11.

9805700-3

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06 — A1

(11) International Publication Number: WO 97/44941

(43) International Publication Date: 27 November 1997 (27.11.97)

(21) International Application Number: PCT/GB97/01288

(22) International Filing Date: 12 May 1997 (12.05.97)

(30) Priority Data:
9610319.7 — 17 May 1996 (17.05.96) — GB

(71) Applicant *(for all designated States except US)*: GPT LIMITED [GB/GB]; New Century Park, P.O. Box 53, Coventry CV3 1HJ (GB). sel PCT/18/3a.

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: WILLIAMS, Philip, John [GB/GB]; 9 Hulse Road, Brislington, Bristol BS4 5AN (GB).

(74) Agent: BRANFIELD, Henry, Anthony; GEC Patent Dept., Waterhouse Lane, Chelmsford, Essex CM1 2QX (GB).

(81) Designated States: AU, NO, SG, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CONNECTION ORIENTED COMMUNICATIONS NETWORK

(57) Abstract

A communications network has means for interconnecting a user computer terminal to a further computer terminal, which further computer terminal is one of a plurality of computer terminals connected in the network. To achieve this a virtual message path is established from the further computer terminal to the user computer terminal in response to an open message sent form the user computer terminal to a user router which sends a service request to the further computer terminal via one or more further routers. Typically the communications network will be the Internet or a similar service.