Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2563354 C 2010/08/17

(11)(21) 2 563 354

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2005/04/25
(87) Date publication PCT/PCT Publication Date: 2005/11/03
(45) Date de délivrance/Issue Date: 2010/08/17
(85) Entrée phase nationale/National Entry: 2006/10/11
(86) N° demande PCT/PCT Application No.: US 2005/014093
(87) N° publication PCT/PCT Publication No.: 2005/102016
(30) Priorité/Priority: 2004/04/26 (US60/565,490)

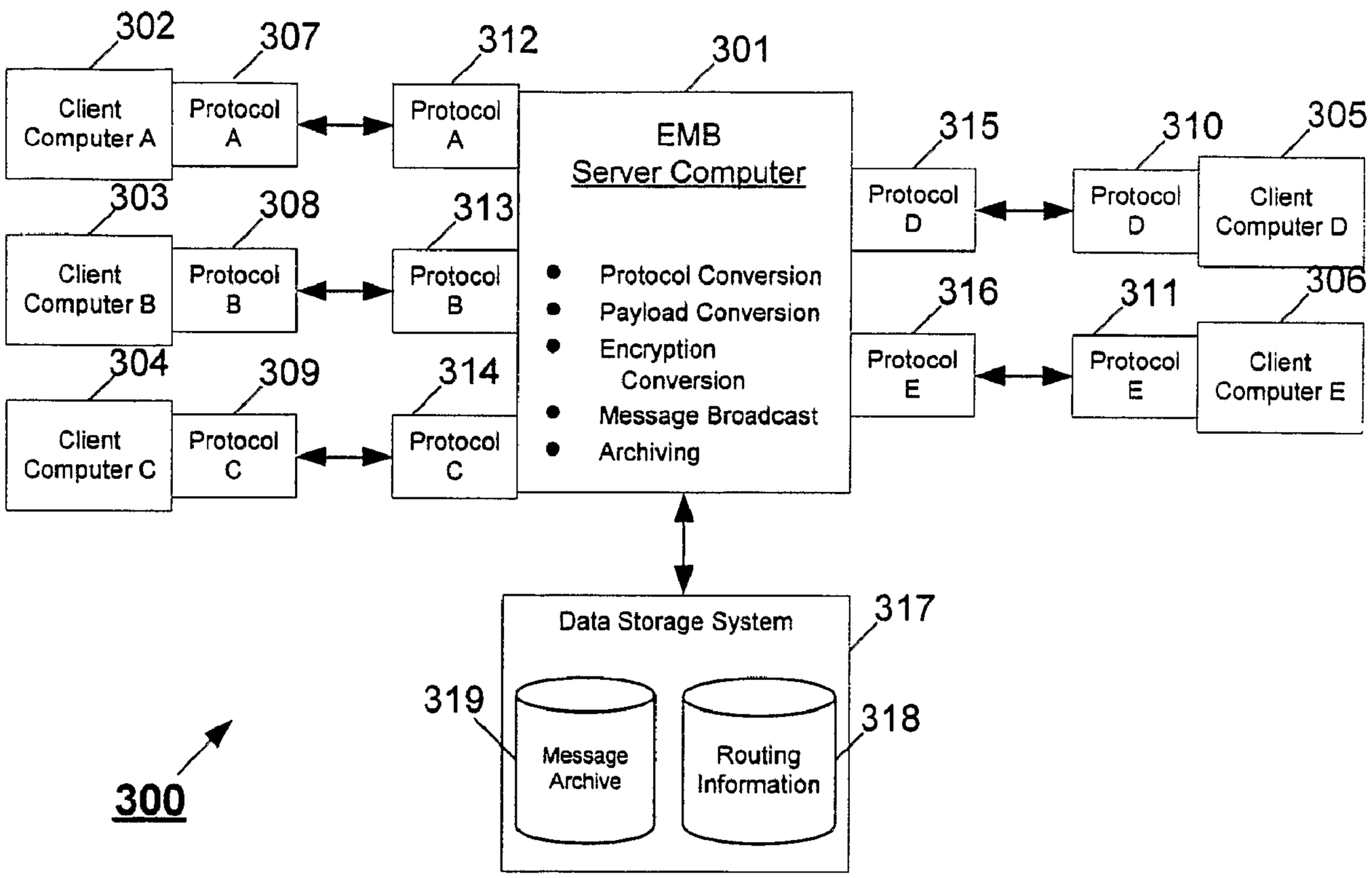
(51) Cl.Int./Int.Cl. *H04L 12/54* (2006.01)

(72) Inventeurs/Inventors:
SETHI, VINCENT, GB;
VASKAS, JOSEPH A., US;
CONNELLY, THOMAS J., US;
WOS, ROSMARIE, US;
BARLOW, ATHENA, US;
SHABASH, MARINA, US;
NARAYANAN, CHANDRAMOULI, US

(73) Propriétaire/Owner:
JP MORGAN CHASE BANK, US

(74) Agent: DIMOCK STRATTON LLP

(54) Titre : SYSTEME ET PROCEDE D'ACHEMINEMENT DE MESSAGES
(54) Title: SYSTEM AND METHOD FOR ROUTING MESSAGES



(57) Abrégé/Abstract:
A hub-and-spoke communication arrangement is provided, in which the "hub" includes a server computer system. The "spokes" are other computers that act as message originators and/or destinations. All internal-to-external messages, and vice versa, are routed through the server computer system to reduce the number of proprietary connections needed between the internal and external entities. In addition, the server computer system provides protocol conversion, message payload conversion, encryption conversion, message broadcast, and/or message archival functionality, so that the "spoke" computers need not be concerned with providing such functionality on their own.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 November 2005 (03.11.2005)

PCT

(10) International Publication Number
WO 2005/102016 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/014093

(22) International Filing Date: 25 April 2005 (25.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/565,490 26 April 2004 (26.04.2004) US

(71) Applicant *(for all designated States except US)*: **JP MORGAN CHASE BANK** [US/US]; 270 Park Avenue, New York, NY 10172 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SETHI, Vincent** [GB/GB]; 28 Yewberry Way, Chandlers Ford, Southampton SO53 4PE (GB). **VASKAS, Joseph, A.** [US/US]; 3947 Berger Avenue, Bethpage New York, NY 11714 (US). **CONNELLY, Thomas, J.** [US/US]; 3654 Carrollton Avenue, Wantagh, NY 11793 (US). **WOS, Rosmarie** [US/US]; 55 Rolling Hill Drive, Chatham, NJ 07928 (US). **BARLOW, Athena** [US/US]; 33-1109 Hudson Street, Jersey City, NJ 07302 (US). **SHABASH, Marina** [US/US]; 240 Muriel Avenue, North Plainfield, NJ 07060 (US). **NARAYANAN, Chandramouli** [IN/US]; 234 The Promenade, Edgewater, NJ 07020 (US).

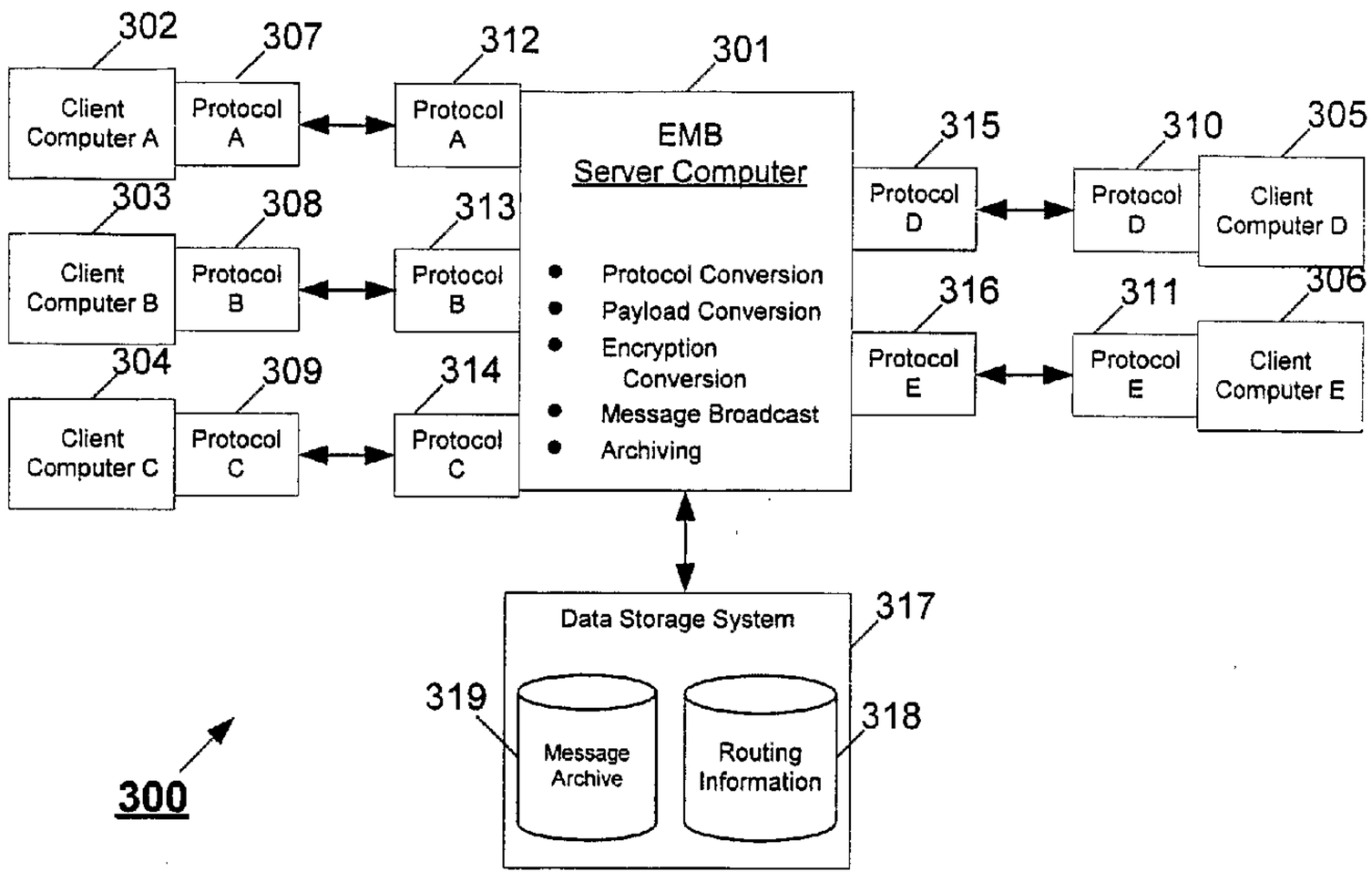
(74) Agent: **PETRUZZELLI, Justin, D. Esq.**; Lowenstein Sandler PC, 65 Livingston Avenue, Roseland, NJ 07068 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ROUTING MESSAGES



(57) Abstract: A hub-and-spoke communication arrangement is provided, in which the "hub" includes a server computer system. The "spokes" are other computers that act as message originators and/or destinations. All internal-to-external messages, and vice versa, are routed through the server computer system to reduce the number of proprietary connections needed between the internal and external entities. In addition, the server computer system provides protocol conversion, message payload conversion, encryption conversion, message broadcast, and/or message archival functionality, so that the "spoke" computers need not be concerned with providing such functionality on their own.

WO 2005/102016 A2

WO 2005/102016 A2

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR ROUTING MESSAGES

Field of the Invention

The present invention relates to efficiently routing messages. In particular, this invention pertains to routing messages while handling protocol conversions, encryption conversions, message payload conversions, and archiving, so that message originators need not be concerned with the protocol, encryption method, and message payload format used by their destination(s).

Background of the Invention

With reference to FIG. 1, organizations often are comprised of multiple lines of businesses ("LOBs") 101, 102, 103. Commonly, these LOBs need to transmit digital information to one or more external entities 104, for example, to conduct business. For instance, in the securities-trading industry, LOBs need to transmit information to the Depository Trust and Clearing Corporation (DTCC), an external entity, pertaining to the trades they have conducted for settlement of the trades. In many cases, communication between the LOBs 101, 102, 103 and

an external entity 104 occurs over proprietary connections 105, such as leased lines. The LOBs 101, 102, 103 are charged a fee for using the proprietary connections 105.

In conventional arrangements, because the LOBs 101, 102, 103 often are unaware of what other LOBs are doing, each LOB 101, 102, 103 would establish its own proprietary connection 105 with the external entity 104. However, because fees are associated with each proprietary connection 105, such conventional arrangements are fiscally inefficient. Accordingly, a way to reduce the number of proprietary connections 105 is needed in the art.

Summary of the Invention

This problem is addressed and a technical solution is achieved in the art by a system and a method for routing messages according to the present invention. In an embodiment of the present invention, a hub-and-spoke communication arrangement is provided, in which the "hub" includes a server computer system, and the "spokes" are other computers that act as message originators and/or destinations. All internal-to-external messages, and vice versa, are routed through the "hub," such that the server computer system acts as a funnel through which all messages pass. Therefore, a fewer number of proprietary connections between the "hub" and the external entities are required.

The present invention also provides an all-inclusive routing functionality that limits the amount of logic required by the "spoke" computers. In particular, various embodiments of the present invention provide protocol conversion, message payload conversion, encryption conversion, message broadcast, and/or message archival functionality, so that the "spoke" computers need not be concerned with providing such functionality on their own.

For instance, according to an embodiment of the present invention, a server computer system, which may include one or more computers, is programmed to receive a message via a protocol. The server computer system determines a destination for the message and what protocol is needed to communicate with the destination. Thereafter, the server computer system transmits the message to the destination via the protocol required by the destination. The protocols may be, without limitation, HTTP, SOAP, MQ, TCP/IP, SNA, GPRS ("General Packet Radio Service"), etc. The message may be an IBM Websphere™ MQ message, a SonicMQ™ message, and a Tibco™ EMS message, for example.

According to another embodiment of the present invention, the message has a data payload in a first format, and the server computer system determines whether the first format of the data payload is to be converted to a second format. If so, the server computer system converts the data payload from the first format to the second format, and transmits the message to the destination in the second format. The first and/or second format(s) may be, without limitation, a Microsoft Word™ format, a Microsoft Excel™ format, a Microsoft Powerpoint™ format, a WordPerfect™ format, a Portable Document Format ("PDF") format, a text-based format, an XML or XML-based format, an ebXML format, a SWIFT format, a FIX format, an ATM format, a CHIP format, an ACH format, an EDI format, an image file format (JPEG, BMP, TIF, etc.), or a video file format (MOV, MPG, AVI, etc.).

According to a further embodiment of the present invention, the server computer system includes encryption conversion functionality. For instance, the server computer system determines whether the message is to be encrypted and what encryption process is to be used prior to transmission of the message to the destination. If the message is to be encrypted, the message is encrypted according to the pertinent encryption process. If the message was received

by the server computer system in an encrypted format, the message may be decrypted prior to encrypting the message according to the pertinent encryption process and prior to transmission to the destination. Encryption processes may include, without limitation, SSL, MQ Secure, etc.

According to still another embodiment of the present invention, message-broadcast functionality is provided by the server computer system. In particular, the message identifies a plurality of destinations, and the server computer system determines the protocol(s), payload format(s), and encryption format(s) required by each of the destinations. The server computer system then performs any required protocol conversions, payload conversions, and encryption conversions prior to sending the message to its destinations.

According to yet another embodiment of the present invention, message archival functionality is provided by the server computer system. In this instance, the message may include information specifying that the message is to be archived or "persistent."

Brief Description of the Drawings

The present invention will be more readily understood from the detailed description of preferred embodiments presented below considered in conjunction with the attached drawings, of which:

FIG. 1 illustrates a conventional communication arrangement;

FIG. 2 illustrates a communication arrangement, according to an embodiment of the present invention;

FIG. 3 illustrates a system for routing messages, according to an embodiment of the present invention;

FIG. 4 illustrates a method for routing messages, according to an embodiment of the present invention;

FIG. 5 illustrates an example of a message being routed through a system, according to an embodiment of the present invention; and

FIG. 6 illustrates a system for routing messages, according to an embodiment of the present invention, according to an embodiment of the present invention.

It is to be understood that the attached drawings are for purposes of illustrating the concepts of the invention and may not be to scale.

Detailed Description of the Invention

With reference to FIG. 2, the present invention provides a hub-and-spoke communication arrangement, in which the "hub" includes a server computer system 201, which may comprise one or more server computers. The "spokes" are other computers 202, 203, 204, 205 that act as message originators and/or destinations. In the embodiment illustrated in FIG. 2, computers 202, 203, 204 are computers that belong to internal lines of business "LOB1," "LOB2," and "LOB3," respectively. Also in the embodiment of FIG. 2, the computer 205 belongs to an external entity. All internal-to-external messages, and vice versa, are routed through the "hub," or server computer system 201. In other words, the server computer system 201 acts as a funnel through which all messages pass. Therefore, a fewer number of proprietary

connections 105 between the "hub" and the external entity/ies are required. As shown in FIG. 2, as few as a single proprietary connection 105 may be used by the lines of business 202, 203, 204.

In addition to reducing the number of proprietary connections 105 needed, the present invention also provides an all-inclusive routing functionality that limits the amount of logic required by the "spoke" computers. In particular, various embodiments of the present invention provide protocol conversion, message payload conversion, encryption conversion, message broadcast, and/or message archival functionality, so that the "spoke" computers need not be concerned with providing such functionality on their own.

FIG. 3 illustrates a system 300 for routing messages, according to an embodiment of the present invention. An Enterprise Messaging Bus ("EMB") server computer 301 is an implementation of the server computer system 201 illustrated in FIG. 2, according to an aspect of the present embodiment. The EMB server computer 301 routes messages to a plurality of client computers communicatively connected to the EMB server computer 301: a "client computer A" 302, a "client computer B" 303, a "client computer C" 304, a "client computer D" 305, and a "client computer E" 306. Although only client computers are shown in FIG. 3, one skilled in the art will appreciate that server computers may be included as message originators and/or message destinations from the perspective of the EMB server computer 301. Further, although only five client computers 302 to 306 are shown in FIG. 3, one skilled in the art will appreciate that any number of client computers may be used. The client computers 302 to 306 may belong to internal or external entities. The messages transmitted between the client computers 302 to 306 may be, without limitation, IBM Websphere MQ messages, SonicMQ messages, and Tibco EMS messages, for example. One skilled in the art will appreciate, however, that the present invention is not limited to particular message types. In the case where MQ messages are

transmitted, the EMB server computer 301 may operate an MQ server application so that the individual client computers 302 to 306 do not have to operate their own MQ server applications, thereby simplifying processing for the client computers 302 to 306 and reducing their costs.

The term "computer" is intended to include any data processing device, such as a desktop computer, a laptop computer, a mainframe computer, a personal digital assistant, a Blackberry, and/or any other device for processing data, whether implemented with electrical and/or magnetic and/or optical and/or biological components, or otherwise.

In the embodiment of FIG. 3, each client computer 302 to 306 communicates with the EMB server computer 301 using its own preferred protocol. For example, client computer A 302 communicates using protocol A 307, client computer B 303 communicates using protocol B 308, client computer C 304 communicates using protocol C 309, client computer D 305 communicates using protocol D 310, and client computer E 306 communicates using protocol E 311. Although each client computer 302 to 306 is shown as communicating using a different protocol, some or all of the client computers 302 to 306 may communicate using the same protocol. The protocols may be, without limitation, HTTP, SOAP, MQ, TCP/IP, SNA, GPRS ("General Packet Radio Service"), etc. One skilled in the art will appreciate, however, that the present invention is not limited to any particular protocol.

The EMB server computer 301 communicates using any of the protocols required by the client computers 302 to 306. For example, because the client computer A 302 communicates using protocol A 307, the EMB server computer 301 communicate with the client computer A 302 using protocol A 312, the same protocol as protocol A 307. Correspondingly, the EMB server computer 301 communicates with the client computer B 303 using protocol B 313 to match protocol B 308. Similarly, the EMB server computer 301 communicates with the

client computer C 304 using protocol C 314, with the client computer D 305 using protocol D 315, and with the client computer E 306 using protocol E 316.

To facilitate the routing of messages between the client computers 302 to 306, the EMB server computer 301 manages and references data stored in a data storage system 317, which is communicatively connected to the EMB server computer 301. The phrase "communicatively connected" is intended to include any type of connection, whether wired, wireless, or both, between devices and/or programs in which data may be communicated. Further, the phrase "communicatively connected" is intended to include a connection between devices and/or programs within a single computer, a connection between devices and/or programs located in different computers, or a connection between devices not located in computers at all. In this regard, although the data storage system 317 is shown separately from the EMB server computer 301, one skilled in the art will appreciate that the data storage system 317 may be stored completely or partially within the EMB server computer 301.

The data storage system 317 stores, among other things, routing information 318. The routing information 318 includes information specifying the protocol(s) used by each of the client computers 302 to 306. When the EMB server computer 301 receives a message, it accesses the routing information 318 to determine what protocol to use to send the message to the message's destination. Such determination is referred to herein as "protocol conversion," whereby the EMB server computer 301 receives a message according to a first protocol, determines a second protocol used by a destination computer using the routing information 318, and transmits the message to the destination computer using the second protocol. By storing the routing information 318 in the data storage system 317, the client computers 302 to 306 do not have to be concerned with what protocols are used by the other client computers.

In addition to performing protocol conversions, the EMB server computer 301 is configured to perform message payload conversions, according to an embodiment of the present invention. A message, according to an aspect of the present embodiment, has administrative information, such as destination information, and a payload, which is the actual substantive data to be transmitted. For example, if a portable document format ("PDF") file, which is known in the art, is to be transmitted to the client computer E 306, the message's administrative information specifies that the client computer E 306 is the destination, and the payload is the PDF file.

The administrative information in the message also may specify that the payload is to be converted from one format to another prior to being sent to the destination. For example, a message transmitting a Microsoft Word™ document to the client computer E 306, may specify in its administrative information that the Word document is to be converted to the PDF format prior to being transmitted to the client computer E 306. In this scenario, the EMB server computer 301, upon reading the administrative information included in the message, performs payload conversion on the message's payload by converting the Word document to a document in the PDF format prior to transmitting the message to the client computer E 306. Payload conversions may also include, without limitation, a Microsoft Word™ format, a Microsoft Exce™l format, a Microsoft Powerpoint™ format, a WordPerfect ™format, a Portable Document Format ("PDF") format, a text-based format, an XML or XML-based format, an ebXML format, a SWIFT format, a FIX format, an ATM format, a CHIP format, an ACH format, an EDI format, an image file format (JPEG, BMP, TIF, etc.), or a video file format (MOV, MPG, AVI, etc.). One skilled in the art will appreciate, however, that payload conversions involving other formats are included within the scope of the invention.

According to an embodiment of the present invention, the routing information 318 includes payload conversion information in addition to or in lieu of the administrative information in the messages. In particular, the routing information 318 may specify a default payload conversion format for one or more of the client computers 302 to 306. For example, the routing information may specify that, by default, any message with a payload having a Microsoft Word™ format going to the client computer E 306 is to be converted to the PDF format. If, at the same time, the administrative information in an incoming message specifies that the payload is not to be converted or is to be converted to a format other than the PDF format, the EMB server computer 301 adheres to the instructions in the administrative information in the message over the default instructions in the routing information 318.

According to an embodiment of the present invention, the EMB server computer 301 is configured to perform encryption conversions. The phrase "encryption conversion" is intended to include the process of encrypting an unencrypted message, decrypting an encrypted message, and/or decrypting an encrypted message and encrypting the decrypted message using the same or a different encryption technique. The routing information 318 may specify whether messages are to be encrypted, what types of messages require encryption, and what encryption technique(s) is/are to be used when sending messages to particular client computers. For example, the routing information 318 may specify that all messages transmitted to the client computer E 306 are to be encrypted using MQ Secure, which is known in the art. Another example is that the routing information 318 may specify that only messages transmitted to the client computer D 305 originating from the client computer C are to be encrypted using Secure Socket Layer ("SSL") encryption. Yet another example is that the routing information 318 may specify that all messages beginning with the word "confidential," when transmitted to the client

computer C 304, are to be encrypted using SSL encryption. When the EMB server computer 301 receives a message, it accesses the routing information 318 to determine whether and how to encrypt the message before transmitting the message to its destination(s).

By performing message encryption with the EMB server computer 301, only the EMB server computer 301 needs to operate software and storage capacity required to perform such encryptions. To elaborate, the EMB server computer 301 is configured to store a repository of encryption software that is available for all of the client computers 302 to 306 to use without those computers having to store their own repositories of encryption software. This arrangement reduces the amount of software and storage capacity required by the client computers 302 to 306 and, consequently, reduces costs and may reduce licensing fees associated with such encryption software. For example, if the client computer A 302 requires that all messages transmitted to it be encrypted according to a proprietary encryption technique, only the EMB server 301 needs to use the proprietary encryption technique. If the client computer E 306 wants to send a message to the client computer A 302, the client computer E 306 transmits the message to the EMB server computer 301 using a no-cost encryption technique (or without any encryption). Upon receipt, the EMB server computer 301 decrypts the message using the no-cost encryption technique, if necessary, and then encrypts the message using the proprietary encryption technique before forwarding the message to the client computer A 302. That is, only a single copy of the software for the proprietary encryption technique is required.

According to an embodiment of the present invention, the administrative information in a message may specify that the message is to be a broadcast message. A broadcast, or multi-cast, message is a message that is sent to a plurality of client computers without having to specifically identify every destination computer. The routing information 318

may include information specifying groups of client computers, and the administrative information in the message need only specify a group name to send the message to the client computers in the group. For example, the EMB server computer 301 may receive a message specifying that the destination of the message is "all users." In such a circumstance, the EMB server computer 301 accesses the routing information 318 to determine the addresses of all of the client computers 302-306, and transmits the message to all client computers, with the exception of the originating client computer, if desired.

According to an embodiment of the present invention, the EMB server computer 301 performs message archiving. To implement such functionality, the EMB server computer searches for an indication in the administrative information in an incoming message that the message is to be archived. According to an aspect of this embodiment, the administrative information indicates that the message is to be a persistent message. Upon receipt of a message including such an indication, the EMB server computer 301 stores the message in a message archive 319 within the data storage system 317. An advantage of this arrangement is that a client computer may instruct the EMB server computer 301 to resend an archived message to the same or a different destination without having to retransmit the message to the EMB server computer 301.

According to another embodiment of the present invention, the EMB Server 301 is configured to compile messaging statistics used for billing, resource planning, marketing, and/or general reporting purposes, according to the system and method described in U.S. Patent Application Publication No. 2006/0026019 A1, titled "System and Method for Measuring Communication-System Infrastructure Usage," by Vincent Sethi, Philip J. DiStefano, and Thomas J. Connelly.

FIG. 4 illustrates a method for routing messages, according to an embodiment of the present invention. FIG. 4 will be described in conjunction with FIG. 5, which illustrates an example of a message routed through a system, according to an embodiment of the present invention. At step S401, the EMB server computer 501 receives a message for distribution. For example, the message may be received from the client computer A 502 via the TCP/IP protocol 507, 512. Optionally, the message may be encrypted according to SSL encryption. The message's administrative information may specify that the message originates from the client computer A 502, that the message is to be persistent, and that the destination for the message is the client computer E 506. The message's payload may be in Word™ format, which also may be specified by the message's administrative information. The message's administrative information may further specify that the payload format is to be converted into the PDF format. In summary, the message's administrative information may specify the information shown in Table I. Note that the information shown in Table I is used for illustration purposes only. One skilled in the art will appreciate that the message's administrative information may include less information, different types of information, and/or may specify information in different formats.

Message's Administrative Information				
Message Originator	**Destination(s)**	**Current Payload Format**	**Desired Payload Format**	**Persistent?**
Client Computer A 502	Client Computer E 506	Word	PDF	Yes

TABLE I

At step S402, the EMB server computer 501 accesses the routing information 518 to determine the characteristics of the destination computer(s). In this example, the routing information 518 may include the information shown in Table II.

Subset of Routing Information 518		
Destination	**Protocol**	**Encryption Technique (if any)**
Client Computer A 502	SNA	MQ Secure

TABLE II

The information shown in Table II is used for illustration purposes only. One skilled in the art will appreciate that the routing information 518 may include different types of information and/or may specify information in different formats for each destination computer. For example, the routing information 518 may further include a preferred message payload format, which may be overridden based upon a format specified in a message's administrative information. Also, the routing information 518 may specify different encryption techniques depending upon characteristics of the message, such as the type of message payload, the name of the message, and/or the originator of the message. Further, the routing information 518 may specify different preferred payload formats depending upon characteristics of the message. Further still, the routing information 518 may specify that particular payload formats are not acceptable and that such messages are to be rejected.

At step S403, the EMB server computer 501 converts the message's payload format, if necessary, based upon the message's administrative information. In this example, the message's administrative information in Table I specifies that the message's payload is currently in Word format and that the message's payload is to be converted to the PDF format. Accordingly, the EMB server computer 301 converts the message's payload format from Word format to the PDF format, at step S403.

At step S404, the EMB server computer 501 decrypts and/or encrypts the message, if necessary, based upon the received routing information 518. In this example, the routing information 518 shown in Table II specifies that messages transmitted to the client

computer E 506 are to be encrypted according to the MQ Secure encryption program. Accordingly, the EMB server computer 301 runs the MQ Secure encryption program to encrypt the message at step S404.

At step S405, the EMB server computer 501 archives the message, if necessary, based upon the message's administrative information. In this example, the message's administrative information in Table I specifies that the message is to be persistent. Accordingly, the EMB server computer 501 stores the message in the message archive 519, at step S405.

At step S406, the EMB server computer 501 transmits the message using the protocol required by the destination(s), as specified by the routing information 518. In this example, the routing information in Table II indicates that the client computer E 506 uses the SNA protocol, which is known in the art. Accordingly, the EMB server computer 501 transmits the message using the SNA protocol 511, 516 to the client computer E 506, at step S406.

Although FIG. 4 illustrates a particular sequence of steps, one skilled in the art will appreciate that the invention is not limited to this particular sequence of steps and that the steps in FIG. 4 may occur in a different order. For example, the archiving step S405 may occur any time after receipt of the message at step S401. Further, the payload conversion step S403 may occur prior to accessing the routing information 518 at step S402. In addition, the present invention is not limited to the occurrence of all of the steps shown in FIG. 4. In particular, steps S403, S404, and S405 are optional.

FIG. 6 illustrates an EMB server computer system 601, according to an embodiment of the present invention. The EMB server computer system 601 includes redundancy with respect to EMB server applications 602, 603. The EMB server applications 602, 603 are similar, if not identical, applications that control the EMB server computer system

601 to behave as described above with reference to the server computer system 201, the EMB server computer 301, and/or the EMB server computer 501. The EMB server applications 602, 603 each may be located on one or more computers. The EMB server application 602 may be designated as a primary application that controls the EMB server computer system 601 until it fails. If the EMB server application 602 fails, the EMB server application 603 takes over controlling the EMB server computer system 601.

The EMB server computer system 601 also includes redundancy provided with synchronous mirroring, which is known in the art, with respect to data storage systems 604, 605. One skilled in the art, however, will appreciate that redundancy may be provided with solutions other than synchronous mirroring. The data storage systems 604, 605 are similar, if not identical, data storage systems storing the data described with respect to the data storage system 317. The data storage systems 604, 605 are preferably stored at different locations. The data storage system 604 may be designated as a primary data storage system that provides data to the EMB server application 602 or the EMB server application 603, whichever is currently controlling the functionality of the EMB server computer system 601. If the data storage system 604 fails, the data storage system 605 takes over. Although only two identical EMB server applications 602, 603 and only two identical data storage systems 604, 605 are shown in FIG. 6, one skilled in the art will appreciate that more EMB server applications 602, 603 and/or data storage systems 604, 605 may be provided.

It is to be understood that the exemplary embodiments are merely illustrative of the present invention and that many variations of the above-described embodiments can be devised by one skilled in the art without departing from the scope of the invention. It is therefore

intended that all such variations be included within the scope of the following claims and their equivalents.

Claims

1. A computer-implemented method for routing messages, comprising the steps of:

receiving a message, encrypted according to a first encryption process, via a first protocol, the message having a data payload in a first format;

determining a destination for the message;

determining a second protocol for the destination;

determining whether the first format of the data payload is to be converted to a second format;

converting the data payload from the first format to the second format, if it is determined that the first format of the data payload is to be converted to the second format; and

transmitting the message to the destination via the second protocol

wherein the message is transmitted in the first format if the data payload was not converted from the first format to the second format, and

wherein the message is transmitted in the second format to the destination, if the data payload was converted from the first format to the second format;

determining whether the message is to be encrypted prior to being transmitted to the destination;

decrypting the message, if it is determined that the message is not to be encrypted prior to being transmitted to the destination, wherein the decrypted message is transmitted to the destination;

determining whether the message is to be encrypted according to a second encryption process prior to being transmitted to the destination, if it is determined that the message is to be encrypted prior to being transmitted to the destination; and

decrypting the message and encrypting the message according to the second encryption process, if it is determined that the message is to be encrypted according to the second encryption process prior to being transmitted to the destination,

wherein the message encrypted according to the second encryption process is transmitted to the destination.

2. The method of claim 1, further comprising the steps of:

determining whether the message is to be archived; and

archiving the message, if it is determined that the message is to be archived.

3. The method of any one of claims 1 or 2, wherein the first protocol and the second protocol are a same protocol.

4. The method of any one of claims 1 to 3, wherein the destination is an intermediate destination.

5. The method of any one of claims 1 to 4, wherein the first format or the second format or both the first format and the second format are a Microsoft Word ™ format, a Microsoft Excel ™ format, a Microsoft Powerpoint ™ format, a WordPerfect ™ format, a Portable Document Format ("PDF") format, a text-based format, an XML-based format, an ebXML format, a SWIFT format, a FIX format, an ATM format, a CHIP format, an ACH format, an EDI format, an image file format, or a video file format.

6. A computer-accessible memory storing computer code for implementing a method for routing messages, wherein the computer code comprises:

code for receiving a message, encrypted according to a first encryption process, via a first protocol, the message having a data payload in a first format;

code for determining a destination for the message;

code for determining a second protocol for the destination;

code for determining whether the first format of the data payload is to be converted to a second format;

code for converting the data payload from the first format to the second format, if determined that the first format of the data payload is to be converted to the second format; and

code for transmitting the message to the destination via the second protocol, wherein the message is transmitted in the first format if the data payload was not converted from the first format to the second format, and

wherein the message is transmitted in the second format to the destination if the data payload was converted from the first format to the second format;

code for determining whether the message is to be encrypted prior to being transmitted to the destination;

code for decrypting the message, if it is determined that the message is not to be encrypted prior to being transmitted to the destination, wherein the decrypted message is transmitted to the destination;

code for determining whether the message is to be encrypted according to a second encryption process prior to being transmitted to the destination, if it is determined that the message is to be encrypted prior to being transmitted to the destination; and

code for decrypting the message and encrypting the message according to the second encryption process, if it is determined that the message is to be encrypted according to the second encryption process prior to being transmitted to the destination, wherein the message encrypted according to the second encryption process is transmitted to the destination.

7. The computer-accessible memory of claim 6, wherein the computer code further comprises:

code for determining whether the message is to be archived; and

code for archiving the message, if it is determined that the message is to be archived.

8. The computer-accessible memory of any one of claims 6 or 7, wherein the first format or the second format or both the first format and the second format are a Microsoft Word ™ format, a Microsoft Excel ™ format, a Microsoft Powerpoint ™ format, a WordPerfect ™ format, a Portable Document Format ("PDF") format, a text-based format, an XML-based format, an ebXML format, a SWIFT format, a FIX format, an ATM format, a CHIP format, an ACH format, an EDI format, an image file format, or a video file format.

9. A system for routing messages, the system comprising:

a first client computer configured to execute a client messaging program that instructs the first client computer to transmit a message via a first protocol;

a second client computer; and a server computer communicatively connected to the first client computer and the second client computer, wherein the server computer is configured to execute a server messaging program that instructs the server computer to at least:

receive the message from the first client computer via the first protocol,

wherein the message includes information that specifies the second client computer as a destination for the message;

determine a second protocol for the second client computer; and

transmit the message to the second client computer via the second protocol;

wherein the first client computer is programmed at least to encrypt the message according to a free-of-charge encryption process prior to transmission, and the server messaging program further instructs the server computer to at least:

decrypt the message according to the free-of-charge encryption process; and

encrypt the message according to a proprietary encryption process, wherein the message encrypted according to the proprietary encryption process is transmitted to the second client computer via the second protocol.

10. The system of claim 9, further comprising a data storage system communicatively connected to the server computer, wherein the server computer determines the second protocol based at least upon information stored in the data storage system.

11. The system of any one of claims 9 or 10, wherein the client messaging program is an MQ client program, the server messaging program is an MQ server program, and the message is an MQ message.

12. The system of any one of claims 9 to 11, further comprising a data storage system communicatively connected to the server computer, wherein the server computer further is

programmed to determine the proprietary encryption process based at least upon information stored in the data storage system.

13. The system of any one of claims 9 to 12, wherein the free-of-charge encryption process performs Secure Socket Layer ("SSL") encryption.

14. The system of any one of claims 9 to 13, wherein the proprietary encryption process performs MQ Secure encryption.

15. A computer-based method for routing messages, comprising the steps of:

receiving an MQ message, encrypted according to a first encryption process, via a first protocol, wherein the message has a data payload in a first format; determining a destination for the message;

determining a second protocol for the destination;

determining whether the first format of the data payload is to be converted to a second format;

converting the data payload from the first format to the second format, if it is determined that the first format of the data payload is to be converted to the second format, wherein the first format or the second format or both the first format and the second format are a Microsoft Word ™ format, a Microsoft Excel ™ format, a Microsoft Powerpoint ™ format, a WordPerfect ™ format, a Portable Document Format ("PDF") format, a text-based format, an XML-based format, an ebXML format, a SWIFT format, a FIX format, an ATM format, a CHIP format, an ACH format, an EDI format, an image file format, or a video file format;

determining whether the message is to be encrypted prior to being transmitted to the destination;

decrypting the message, if it is determined that the message is not to be encrypted prior to being transmitted to the destination, wherein the decrypted message is transmitted to the destination;

determining whether the message is to be encrypted according to a second encryption process prior to being transmitted to the destination, if it is determined that the message is to be encrypted prior to being transmitted to the destination;

encrypting the message and encrypting the message according to the second encryption process, if it is determined that the message is to be encrypted according to the second encryption process prior to being transmitted to the destination;

determining whether the message is to be archived by reading the message for an indication that the message is to be persistent; archiving the message, if it is determined that the message is to be archived; and

transmitting the message, encrypted according to the second encryption process, to the destination via the second protocol, wherein the message is transmitted in the first format if the data payload was not converted from the first format to the second format, and wherein the message is transmitted in the second format to the destination if the data payload was converted from the first format to the second format.

Fig. 1

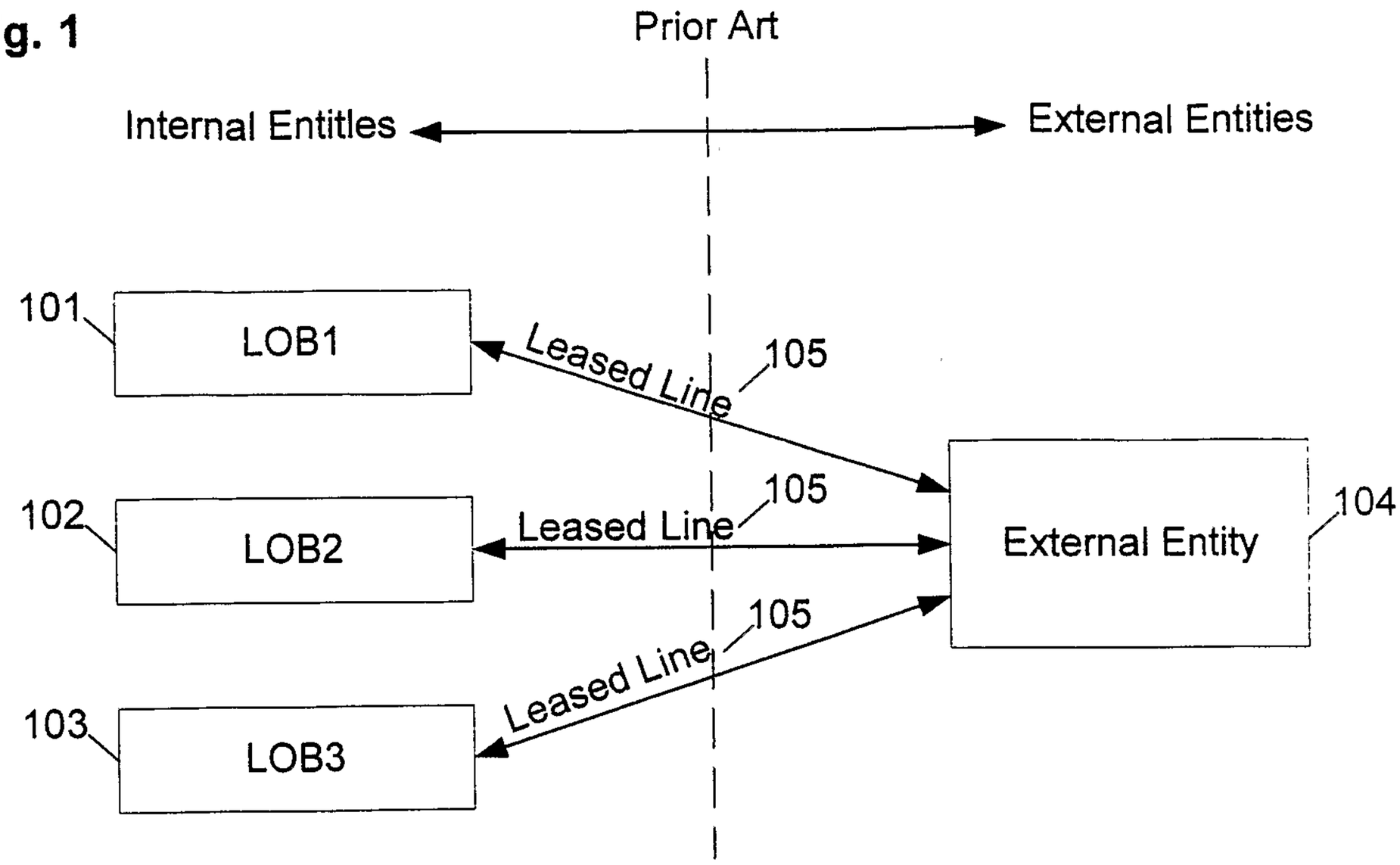

Prior Art
Internal Entitles
External Entities
101
LOB1
Leased Line
105
102
LOB2
Leased Line
105
External Entity
104
103
LOB3
Leased Line
105

Fig. 2

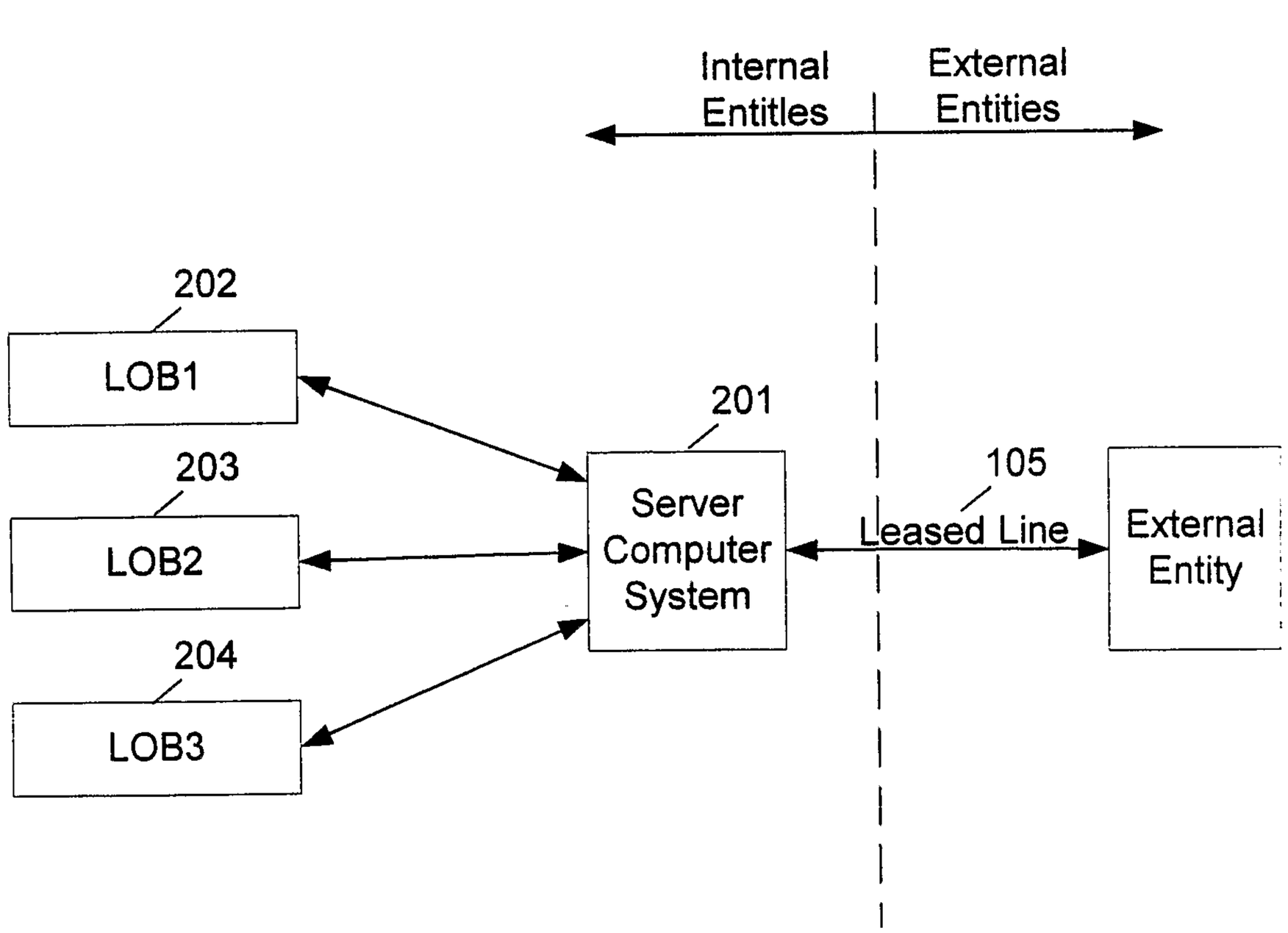

Internal Entitles
External Entities
202
LOB1
201
203
LOB2
Server Computer System
105
Leased Line
External Entity
204
LOB3

Fig. 3

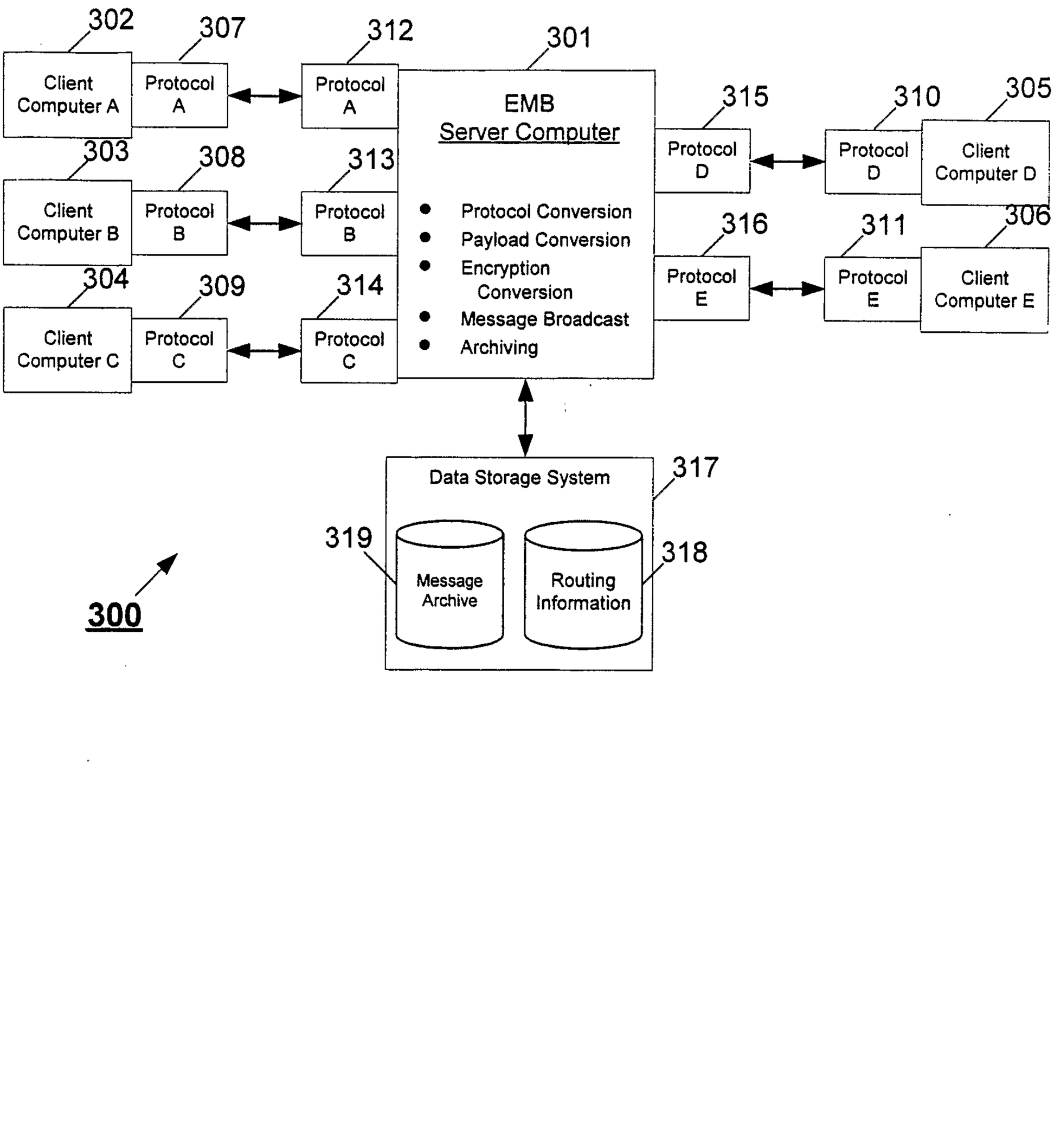
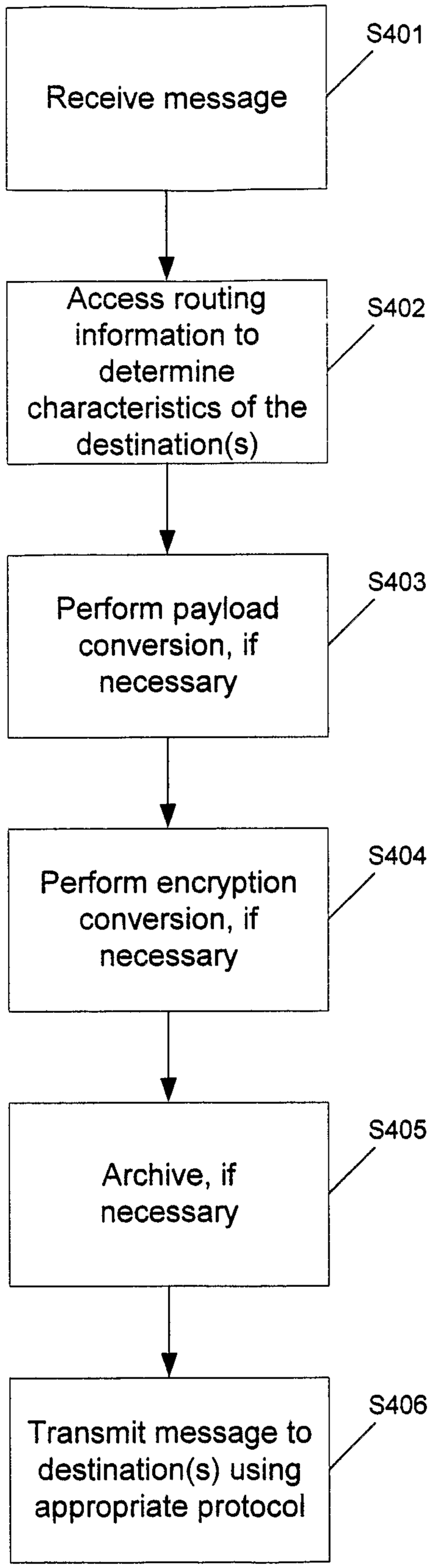

302
307
312
301
Client Computer A
Protocol A
Protocol A
EMB Server Computer
315
310
305
Protocol D
Protocol D
Client Computer D
303
308
313
Client Computer B
Protocol B
Protocol B
Protocol Conversion
Payload Conversion
Encryption Conversion
Message Broadcast
Archiving
316
311
306
Protocol E
Protocol E
Client Computer E
304
309
314
Client Computer C
Protocol C
Protocol C
Data Storage System
317
319
318
Message Archive
Routing Information
300

Fig. 4


Receive message
S401
Access routing information to determine characteristics of the destination(s)
S402
Perform payload conversion, if necessary
S403
Perform encryption conversion, if necessary
S404
Archive, if necessary
S405
Transmit message to destination(s) using appropriate protocol
S406

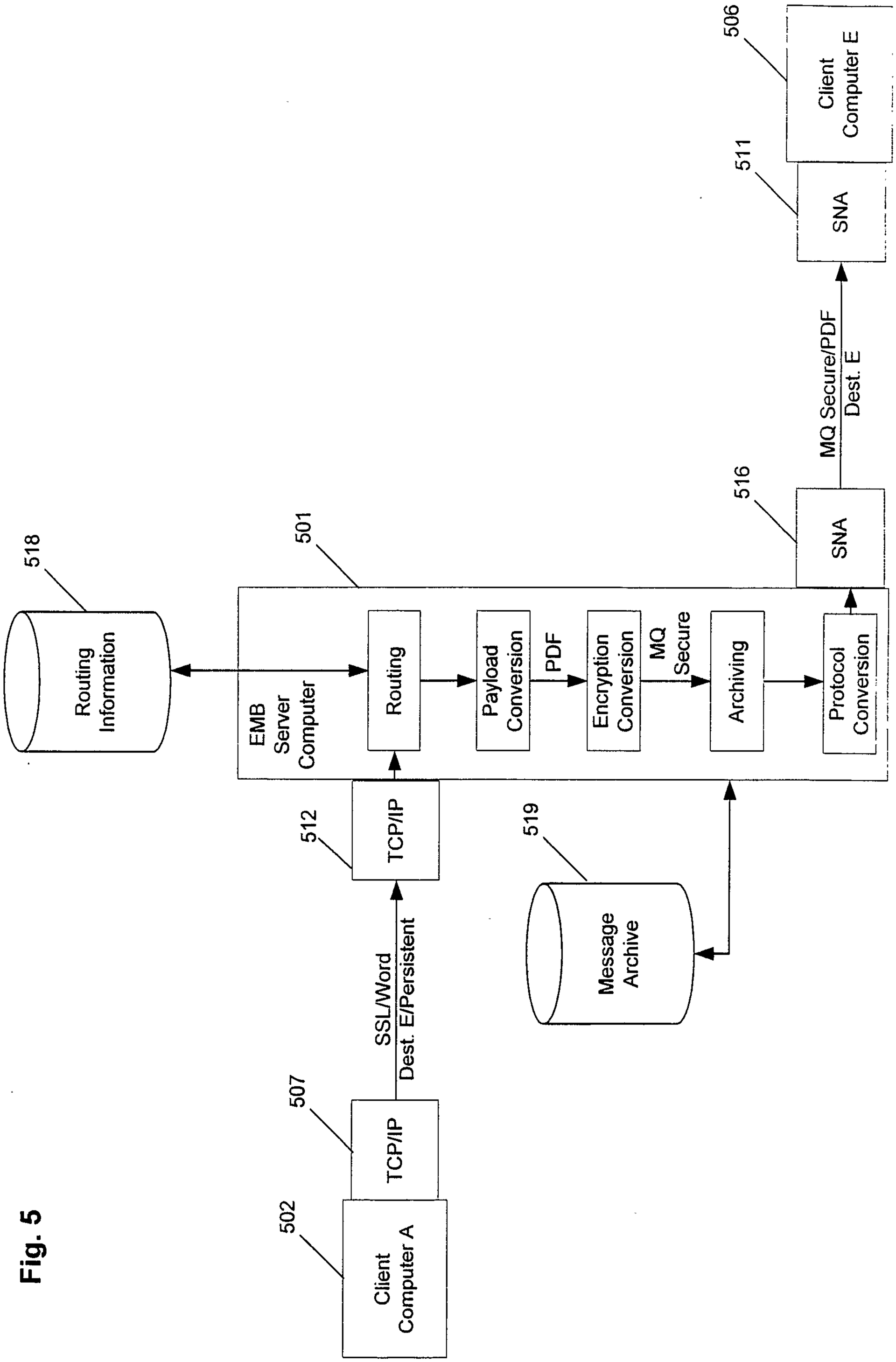
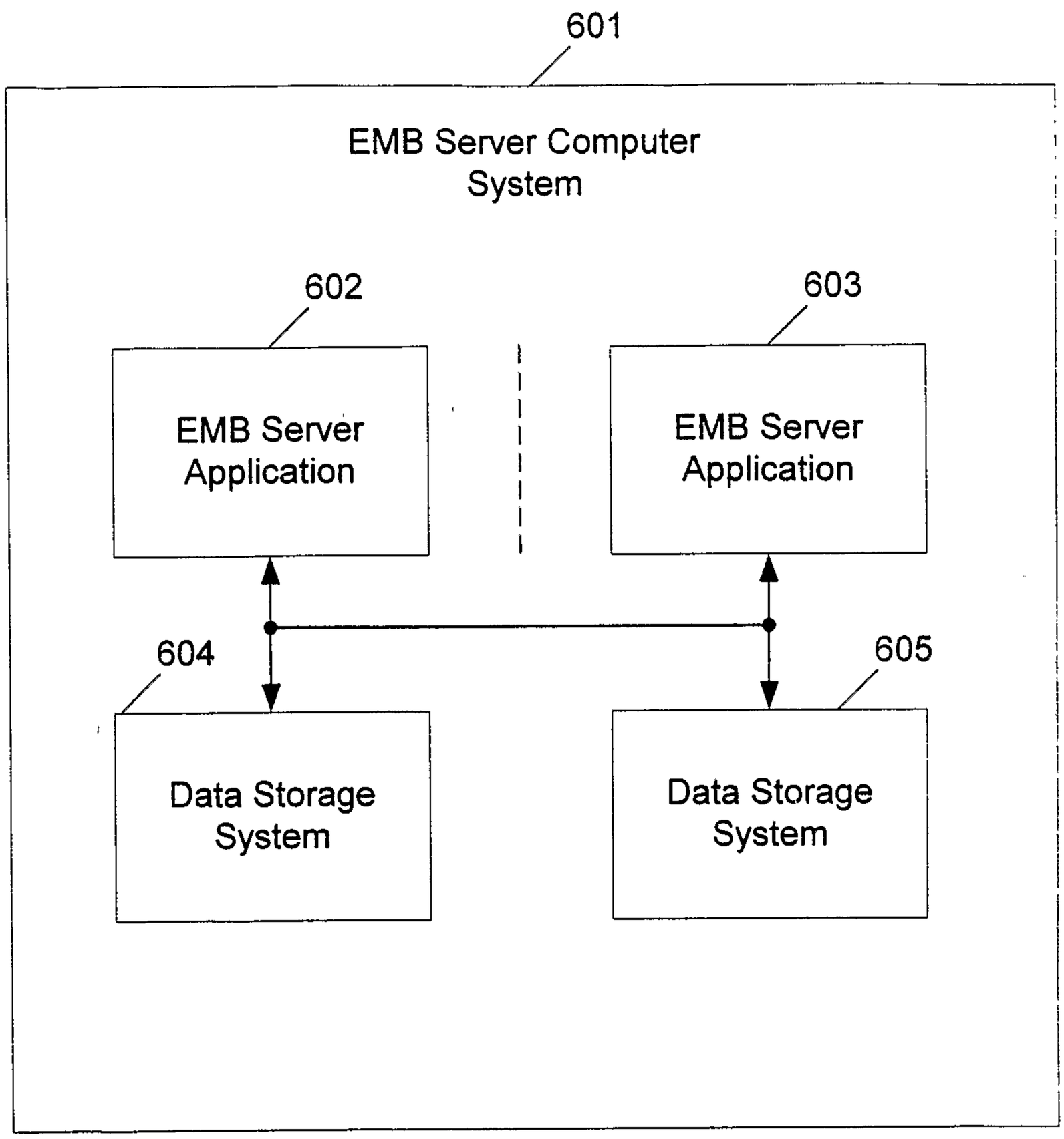
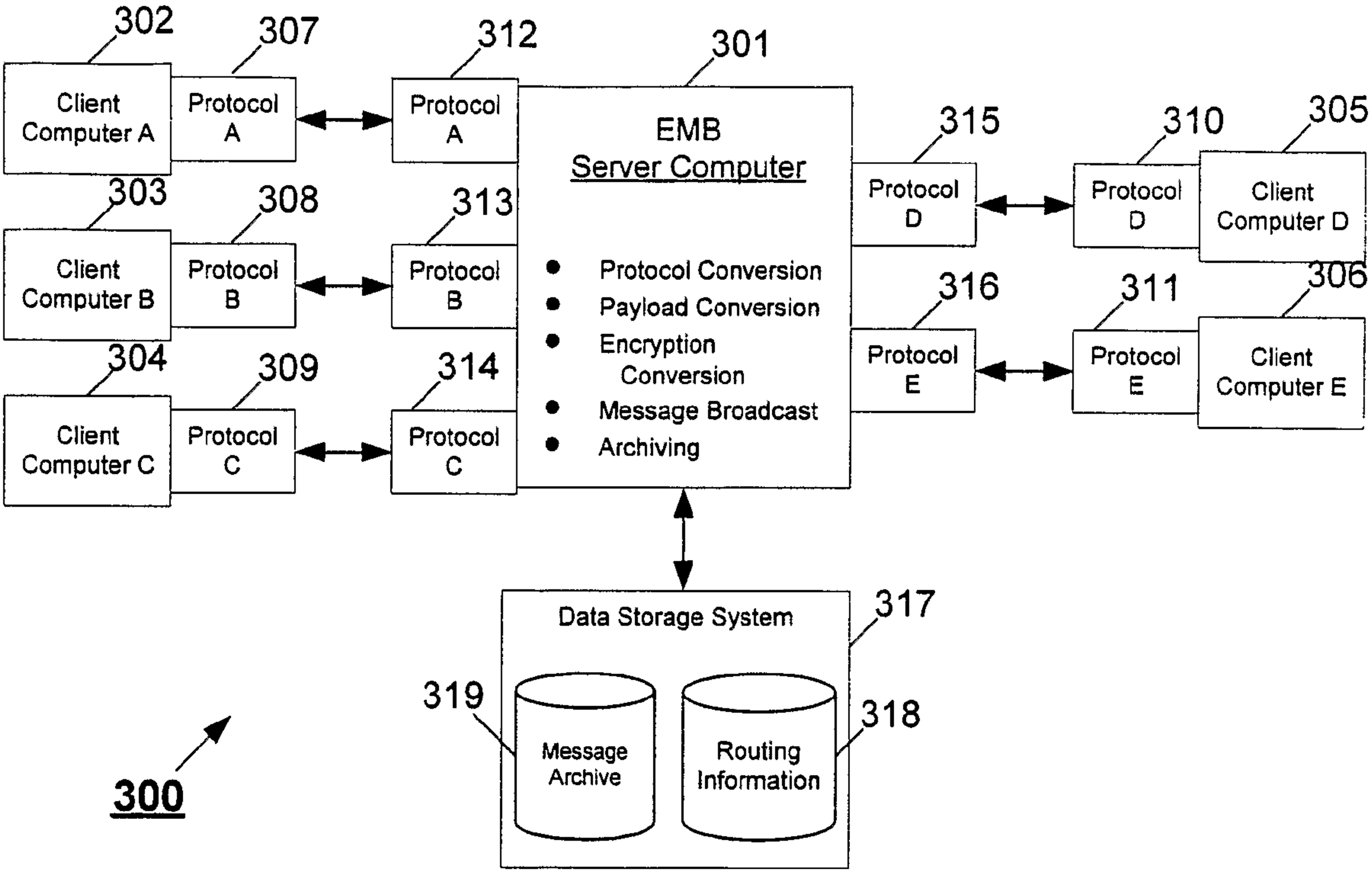

506
Client Computer E
511
SNA
MQ Secure/PDF
Dest. E
516
SNA
518
Routing Information
501
EMB Server Computer
Routing
Payload Conversion
PDF
Encryption Conversion
MQ Secure
Archiving
Protocol Conversion
512
TCP/IP
519
Message Archive
SSL/Word
Dest. E/Persistent
507
TCP/IP
502
Client Computer A

Fig. 5

Fig. 6


601
EMB Server Computer System
602
603
EMB Server Application
EMB Server Application
604
605
Data Storage System
Data Storage System


302
307
312
301
Client Computer A
Protocol A
Protocol A
EMB
Server Computer
315
310
305
Protocol D
Protocol D
Client Computer D
303
308
313
Client Computer B
Protocol B
Protocol B
Protocol Conversion
Payload Conversion
Encryption Conversion
Message Broadcast
Archiving
316
311
306
Protocol E
Protocol E
Client Computer E
304
309
314
Client Computer C
Protocol C
Protocol C
Data Storage System
317
319
318
Message Archive
Routing Information
300