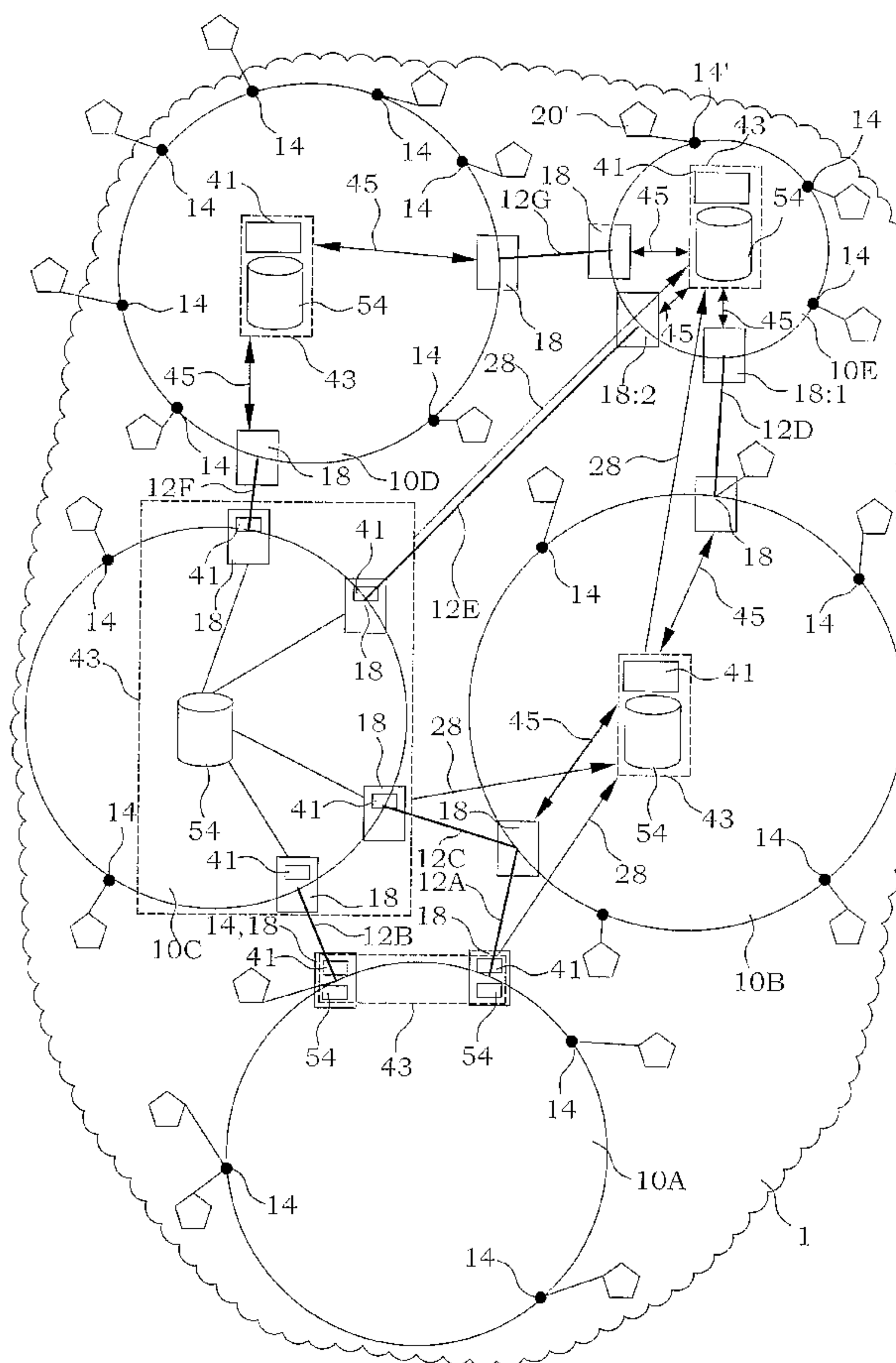




(86) Date de dépôt PCT/PCT Filing Date: 2004/06/30
(87) Date publication PCT/PCT Publication Date: 2006/01/12
(85) Entrée phase nationale/National Entry: 2006/11/06
(86) N° demande PCT/PCT Application No.: SE 2004/001065
(87) N° publication PCT/PCT Publication No.: 2006/004461

(51) Cl.Int./Int.Cl. **H04L 12/46** (2006.01),
H04L 12/24 (2006.01)
(71) Demandeur/Applicant:
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL), SE
(72) Inventeurs/Inventors:
FLINTA, CHRISTOFER, SE;
MANGS, JAN-ERIK, SE;
WESTBERG, LARS, SE
(74) Agent: BEAUCHESNE, NICOLAESCU

(54) Titre : PROCÉDE ET SYSTÈME DE CONFIGURATION DE RESEAU PRIVE VIRTUEL A DOMAINES MULTIPLES
(54) Title: METHOD AND SYSTEM FOR MULTI-DOMAIN VIRTUAL PRIVATE NETWORK CONFIGURATION



(57) **Abrégé/Abstract:**

Information about virtual private networks -VPNs- in each domain (10A-E) of a multi-domain communications system (1) is provided. By comparing a request (31) for a configuration of a VPN with the provided information of other connected domains, a



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

match can be found. VPN configuration can then be performed based on the outcome of the match. The provided domain VPN information is in one embodiment spread to other domains under constrictions put by SLAs between domain operators. The spreading of VPN information can be performed regularly or triggered by an external event. In another embodiment, the VPN configuration request is instead spread to different domains.

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

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
12 January 2006 (12.01.2006)

PCT

(10) International Publication Number
WO 2006/004461 A1(51) International Patent Classification⁷: **H04L 12/46,**
12/24(21) International Application Number:
PCT/SE2004/001065

(22) International Filing Date: 30 June 2004 (30.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **TELEFONAKTIEBOLAGET LM ERICSSON (publ)**
[SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FLINTA, Christofer** [SE/SE]; Sköldgatan 4, S-118 63 Stockholm (SE). **MÅNGS, Jan-Erik** [SE/SE]; Björnstigen 36, S-170 72 Solna (SE). **WESTBERG, Lars** [SE/SE]; Långtora, S-745 96 Enköping (SE).(74) Agent: **AROS PATENT AB**; P.O. Box 1544, S-751 45 Uppsala (SE).

(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, 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, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

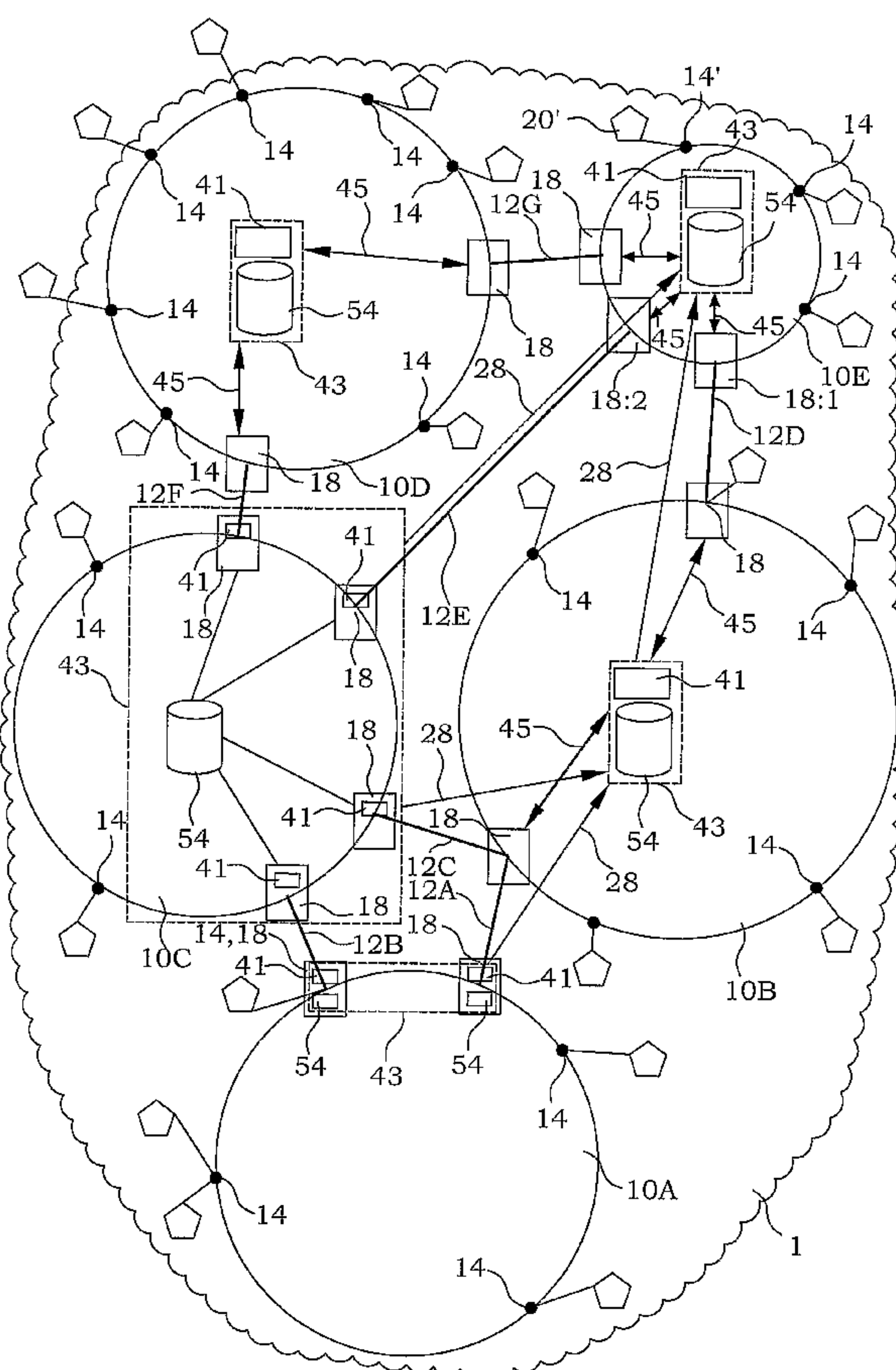
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, 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:

— with international search 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.

(54) Title: METHOD AND SYSTEM FOR MULTI-DOMAIN VIRTUAL PRIVATE NETWORK CONFIGURATION



(57) Abstract: Information about virtual private networks -VPNs - in each domain (10A-E) of a multi-domain communications system (1) is provided. By comparing a request (31) for a configuration of a VPN with the provided information of other connected domains, a match can be found. VPN configuration can then be performed based on the outcome of the match. The provided domain VPN information is in one embodiment spread to other domains under constrictions put by SLAs between domain operators. The spreading of VPN information can be performed regularly or triggered by an external event. In another embodiment, the VPN configuration request is instead spread to different domains.

WO 2006/004461 A1

Method and system for multi-domain virtual private network configuration

TECHNICAL FIELD

5

The present invention relates in general to virtual private networks in communications systems and in particular to configuration of virtual private networks in multi-domain communications systems.

10

BACKGROUND

15

20

25

A Virtual Private Network (VPN) utilises a public or private communications network to conduct private communications. Traditionally, a company or other customer that wanted to build a wide-area network had to provide for its own dedicated lines between each node to provide the connectivity. Such solutions are, however, generally expensive and inflexible. During the last years, the concept of VPNs has evolved rapidly. VPNs offer a solution, where a communications network is shared between many customers, but where the communication of each customer is virtually separated. VPN technology is often based on the idea of tunnelling. Network tunnelling involves establishing and maintaining a logical network connection. On this connection, packets are encapsulated within some other base or carrier protocol. They are then transmitted between VPN client and server and eventually de-encapsulated on the receiver side. Authentication and encryption assists in providing security.

30

A tendency is that the number of network nodes that form a VPN grows fast, which results in large complex network structures and topology. This is caused, partly because of the increasing traffic on VPNs and partly on that the VPNs are requested to cover larger and larger geographical areas. Communication networks providing VPNs having nodes at all continents are present today. However, the more nodes and the more traffic that is to be transmitted, the more complex the configuration of VPNs becomes.

Conventionally, a VPN is created according to an agreement between a network operator and a customer. The location of the nodes, the quality of service and other conditions are agreed on and a programmer at the operator sets up the configuration manually or by consulting configuration aid tools. When having more and more complex communications networks, such configuration becomes more and more complex and time consuming. Furthermore, when a customer wants to modify its VPN, the entire procedure has to be repeated.

When setting up VPNs in a network, different technologies can also be used. Each technology has its own benefits and drawbacks and its own way of configuring the VPNs. There is no general VPN architecture that is independent of VPN technology.

SUMMARY

A general problem of prior-art solutions is thus that communications networks providing virtual private networks having a large geographical coverage and/or having large traffic become very complex. A further problem is that configuration of new VPNs or modifications of already existing VPNs become complex and time consuming. A further problem is that communication resources of network operators covering smaller geographical areas cannot be generally utilised for wide-area VPNs.

A general object of the present invention is thus to improve methods for configuration of VPNs as well as providing systems and devices suitable therefore. A further object of the present invention is to provide methods for configuring VPNs utilising more than one network domain. Another further object of the present invention is to provide methods for configuring of VPNs that are basically independent on the actual VPN technology used. Yet a further object of the present invention is to provide a method for automatic configuration of a VPN.

The above objects are achieved by methods and devices according to the enclosed patent claims. In general words, information about VPNs in a domain is provided. By comparing a request for a configuration of a VPN with the provided information of other connected domains a match can be found. The re-configuration can then be performed based on the outcome of the match. The provision of domain VPN information can be performed in different ways, e.g. collection of data in a centralised or distributed manner, or by retrieving stored data. A distributed VPN control node is in particular embodiments localised to border nodes of a domain. The domain VPN information is in particular embodiments collected from the edge nodes of the domain. This can be performed by passively extracting broadcasted information from the edge nodes, by requesting domain VPN information from the edge nodes or a combination thereof. The collection can be triggered by an external event, such as a VPN configuration request. The provided domain VPN information is in one embodiment spread to other domains under constrictions put by SLAs between domain operators. In another embodiment, the VPN configuration request is instead spread to different domains. The matching can thus be performed at various distances from the originally requesting domain.

One important advantage with the present invention is that it provides a simple and stable platform on which operators of different domains can co-operate. The domain VPN information is made available for supporting VPN configuration in essentially all domains of a multi-domain system. However, at the same time, in one embodiment, the actual information is spread over the multi-domain system constricted by different agreements between the operators.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further objects and advantages thereof, may best be understood by making reference to the following description taken together with the accompanying drawings, in which:

FIG. 1 is a schematic illustration of a multi-domain communications network providing virtual private networks;

FIG. 2A is a schematic illustration of VPN information collection according to an embodiment of the present invention;

FIGS. 2B-D are schematic illustrations of VPN information collection according to other embodiments of the present invention;

FIGS. 3A-D are embodiments according to the present invention of VPN control node configurations within a domain;

FIG. 4 is a schematic illustration of VPN information forwarding and connect requests according to an embodiment of the present invention;

FIG. 5 is a schematic illustration of VPN information forwarding and connect requests according to another embodiment of the present invention;

FIG. 6A is a block scheme of an embodiment of a general VPN control node according to the present invention;

FIG. 6B is a block scheme of another embodiment of a VPN control node according to the present invention;

FIG. 7 is a schematic illustration of VPN configuration according to one embodiment of the present invention; and

FIG. 8 is a flow diagram illustrating the main steps of an embodiment of a method according to the present invention.

DETAILED DESCRIPTION

An embodiment of a general VPN provider architecture 1 is illustrated in Fig. 1. In this VPN Provider Architecture, there are five VPN Provider Domains 10A-E present, which are attached to each other by interdomain data connections 12A-G. One operator may control one or more of these domains 10A-E, or they can all be controlled by separate operators. The relation between the domains 10A-E, i.e. the control of the interdomain data connections 12A-G are typically regulated according to agreements between

the involved operators, e.g. a VPN Service Level Agreement (SLA). Each VPN provider domain 10A comprises VPN edge nodes 14 and core nodes 16, which can be VPN aware or VPN unaware, of which only a few are provided with reference numbers. The VPN edge nodes 14 are nodes through which customer sites 20 of different customers are connected to different VPN's in the architecture 1. VPN unaware nodes 16 are just intermediate nodes within a domain and is only used for forwarding messages and data between VPN edge nodes 14. The customers are unaware of which VPN unaware nodes that are used for the communication. The only important matter is the starting and ending VPN edge node 14. A VPN connected in a domain can thus be represented by a direct line between VPN edge nodes 14, even if the actual communication may take place via one or several VPN unaware nodes 16. In the remaining part of the present disclosure, the existence of VPN unaware nodes will in general be neglected, since the basic procedural steps according to the present invention are not directly dependent on the existence of any VPN unaware nodes 16 or not. In the practical implementation, it is, however, likely that VPN unaware nodes 16 are used for providing the actual connectivity.

The VPN provider domains 10A-E are connected in a data plane via VPN border nodes 18, i.e. the interdomain data connections 12A-G start and end in a VPN border node 18. The VPN border node 18 may or may not at the same time also act as a VPN edge node 14. A customer site 20 is connected to one of the VPN edge nodes 14. Customer sites 20 of the same customer may then be connected through the VPN provider domains 10A-E by a VPN 22A-C. One customer may have customer sites 20 connected to different VPN's 22A-C. Also, more than one customer site 20 can be connected to the same VPN edge node 14, but will be unaware of the existence of the other customer site 20 as well as of the VPN to which the other customer site 20 is connected.

In the present embodiment, three VPN's 22A-C are illustrated. However, anyone skilled in the art realises that the number of VPN's in a real system

typically is much higher. A first VPN 22A, illustrated by broken lines, is extended over three domains 10A, 10C, 10D and connects customer sites 20 in all of these domains. A second VPN 22B, illustrated by dotted lines, is extended over all domains 10A-E of the present embodiment. Finally, a third
5 VPN 22C, illustrated by a dash-dotted line, connects customer sites 20 only within the domain 10B. Each customer site 20 is unaware of the existence of customer sites 20 of other customers as well as of the existence of any VPN's except the one it is connected to. In such a manner, the privacy character of the VPN's is preserved, although they all share the same basic
10 communications resources. This is the scenario in which the present invention preferably operates.

Now, consider that a new customer site 20' is connected to a VPN edge node 14' in domain 10E. If the customer site 20' wants to be connected to VPN
15 22B, the procedures are probably relatively simple, since the VPN 22B already is present within domain 10E. Manual or automatic VPN reconfiguration procedures according to prior art may be employed, as well as mixes therebetween. However, if the new customer site 20' wants to connect to VPN 22A or 22C, the situation becomes more difficult. In prior
20 art, there are no general interdomain VPN configuration procedures.

One basic idea of the present invention is based on three part activities. One part concerns provision of domain VPN information, comprising in its most basic version VPN identity of VPNs available in the respective domain. Another
25 part concerns searching for a specific VPN to connect to. This is in other words a matching between a requested VPN and provided domain VPN information. In some embodiments, this matching procedure comprises transferring of domain VPN information or information derived therefrom to other domains. In other embodiments, a request for a certain VPN is instead transferred
30 between domains. The final part concerns the actual re-configuring of a VPN. The fundamentally new ideas of the present invention are mainly involved in the two first stages.

Fig. 2A illustrates an embodiment of an initial phase of providing domain VPN information. Each VPN edge node 14 has stored information reflecting its own present VPN configuration regarding at least which VPN's that have connected customer sites at that particular VPN edge node 14. In particular
5 embodiments, the VPN edge node 14 has information also about which customers that are connected to the VPN edge node 14 and associations between the present VPN's and customer sites 20. In some embodiments, information, such as VPN address space and address type (local or global), VPN quality of service classes, specified by requirements such as bandwidth,
10 delay and jitter, and/or VPN set-up, i.e. use of tunnels or filters is provided. Also information such as encryption properties, transparency layer properties, tunnelling properties and topology properties can be included. Furthermore, the VPN border nodes 18 have stored information about the identity of the VPN provider domain it belongs to.

15 According to one embodiment of the present invention, the domain VPN information stored in each VPN edge node 14, or at least parts thereof, is collected by each border node 18 in the same domain 10A-E. This is visualised in Fig. 2A as arrows, of which some are provided with reference number 24. In
20 such a way, the collective domain node information for the own domain is available in each VPN border node 18 of each domain 10A-E. One alternative for the communication is to use a communication protocol similar to BGP (Border Gateway Protocol), spreading the information all over the domain without any particular knowledge about where the need for information is. The
25 border nodes may then pick up all necessary information. This is an example of a push mechanism for distributing domain VPN information.

Fig. 2B illustrates another embodiment for providing domain VPN information, now concentrated to one domain 10C. If the VPN border nodes
30 18 has stored information about which edge nodes 14 that are present in the same domain 10C, the VPN border node 18 can simply request 23 any VPN edge node 14 to return its domain node information 24. In the most simple form of requesting information, the request itself could be a question if the

VPN edge node 14 is associated to a certain VPN or not, e.g. received by the domain interconnection 12F. An acknowledgement message will in such a case not comprise any information as such, but will implicitly transfer information of this particular VPN at that particular VPN edge node. This is
5 an example of a pull mechanism for distributing domain VPN information.

The domain node information can also be collected with different timing. One alternative is to continuously or at least regularly collect such information to the border nodes in order to assure that the available information always is
10 updated. In such embodiments, the information is preferably stored in the border nodes or in any other node where it is retrievable from the border node, see embodiments described further below. Another alternative is that the information collection is triggered by some event. This event could e.g. be a broadcasting message from an edge node that there is a change of some
15 kind or, as being described above, a request for finding a particular VPN. If all edge nodes have knowledge about which border nodes that are available in the domain, the information could also be sent directly to all border nodes when such a change occurs. In case the information is searched as triggered by a request to find a certain VPN, the collected information may be
20 restricted to that VPN and may not even necessarily be stored for later use.

Fig. 2C illustrates an embodiment, where the domain VPN information is collected in a centralised manner. A storage 54 is provided to store all domain VPN information 24 provided by the different edge nodes 14. Any
25 functionalities using such domain VPN information can retrieve this information from the central storage 54.

Fig. 2D illustrates another embodiment based on a centralised collection of domain VPN data. Here, a request 23 or other external signal can initialise
30 the provision of VPN data 24 to the storage 54. This request 23 does not necessarily have to come from the storage itself 54.

As an alternative to collect domain VPN information among the domain nodes, the domain VPN information may instead be provided by retrieving data from a data storage. This stored data could e.g. be the result of a previous collection of data according to the procedures above, or could be provided from elsewhere.

In the previously described embodiment, the provision of data within a domain is executed by the border nodes or a node in direct association therewith. Such a situation is also illustrated in Fig. 3A. Here, one domain 10A in a multidomain system is illustrated more in detail. The border nodes 18 are responsible for the data traffic to and from other domains by the data connections 12A and 12B. The border nodes 18 comprise in this particular embodiment means 41 for collecting domain VPN information, in the form of e.g. software functionality in the processors of the border node 18. The domain VPN information can be stored in a storage 54. A VPN control node 43 for handling domain VPN information regarding the domain as a whole is thus in this particular embodiment implemented as a distribution of local means 41 at every border node 18.

In Fig. 3B, another particular embodiment is illustrated. Here, the border nodes 18 still comprise functionality entities 41 involved with domain VPN information. However, a distributed VPN control node 43 comprises in this particular embodiment means 41 for providing domain VPN information situated in or in connection with the border nodes 18 and a central database 54. In the central database 54, the actual updated and preferably also historical VPN information is stored.

In Fig. 3C, yet another particular embodiment is illustrated. Here, the VPN control node 43 is centralised and comprises the means 41 for providing domain VPN information and the central database 54 basically provided at the same location. The border nodes 18 are in this particular embodiment merely used for handling communications 45 between the VPN control node and neighbouring domains. Functionalities in the border nodes 18 regarding

control signalling associated with the actual data traffic can in such a way be utilised also to signal control messages concerning VPN configuration.

In Fig. 3D, an embodiment having a VPN control node 43 that is virtually separated from the border nodes in the system is illustrated. The VPN control node 43 is in such an embodiment connected to VPN control nodes in other domains by dedicated VPN control signal connections 47, creating a high-level network of its own.

In a particular embodiment of the present invention, the provided domain VPN information can be transferred within the system, i.e. between the different domains. This is illustrated in Fig. 4. The first step is provision of VPN information within each domain. This is performed by a VPN control node 43 in each domain. However, the configuration of the VPN control nodes 43 may differ between the different domains. In Fig. 4 it is indicated that domain 10A has a VPN control node 43 similar to the example shown in Fig. 3A, domain 10C has a VPN control node 43 similar to the example shown in Fig. 3B and domains 10B, 10D and 10E have VPN control nodes 43 similar to the example shown in Fig. 3C. According to each SLA regulating the traffic between the different domains, at least a part of the available domain VPN information in each VPN control node 43 is in this embodiment transferred to the counteracting VPN control node in the neighbouring domains. Arrows 28 illustrate this interdomain transfer of information. The SLA may comprise agreements about how much of the available information that should be made available for the neighbouring domain. In a general case, the VPN control node processes available intradomain VPN information into compiled or processed VPN information that is suitable to forward to neighbouring domains. If the domains are closely related, e.g. belonging to the same operator, the SLA could involve a total transparency in exchanging domain VPN information. In other cases, the processed information 28 that is transferred between the VPN control nodes 43 may be compiled VPN information, only revealing very basic fact about the individual domain VPNs. The minimum information that has to be

sent over the interdomain connections 12A-G in the present embodiment is the identities of the VPN's that are available somewhere beyond the border node that sends the information.

5 The information 28 sent on the interdomain connections 12A-G causes an update of the total available VPN information situation at the receiving VPN control node. This VPN control node now also has information e.g. of what VPN's that are available via the interdomain connections. If more thorough information is available, the VPN control node may also determine e.g. edge
10 node identities at which these different VPN's are available, VPN quality of service etc. The so achieved VPN information is now a property of the neighbour domain and can, if allowed by the SLA, be used for activities in that domain. The information stored in the storage 54 of the VPN control node 43 could be identical to the information received from the neighbouring
15 domain or a processed version thereof, adding, removing or modifying the received information. For instance, the information could be labelled with an indication from what domain it originated from.

This information distribution may continue in many successive steps, in
20 some cases applying further modification of the information before forwarded to another domain, in analogy with the first transfer. Eventually, all VPN control nodes in the entire VPN provider architecture 1 has at least a processed version of all domain VPN information available in the system. At each VPN control node, the information may be processed according to the
25 SLA that is valid for the associated interdomain connection to be used.

In an alternative embodiment, information distribution between domains can be performed in a broadcast push manner. The domain VPN information is then sent directly to one, several or all of the other VPN control nodes in the
30 other domains in the total system, not restricted to the neighbouring domains. This means that the domain VPN information is not forwarded in a chain as in the other embodiment, but merely broadcasted through the

system. The availability of such direct request forwarding can be regulated by domain SLAs.

5 The exchange of domain VPN information can be performed with different timing. One alternative is to continuously or at least regularly exchange such information in order to assure that the available information always is updated. In such embodiments, the information is preferably stored in the VPN control nodes or in any other node, where it is retrievable by the VPN control node. In other words, this alternative is a typical push mechanism
10 for data distribution.

Another alternative is that the information exchange is triggered by some event. This event could e.g. be that a change of some kind has occurred in a domain or, as being described below, a request for finding a particular VPN
15 is issued. In other words, this alternative can be described as a triggered push mechanism for data distribution.

In case the information is exchanged as triggered by a request to find a certain VPN, the exchanged information may be restricted to that VPN and
20 may not even necessarily be stored for later use. This is an example of a pull mechanism for data distribution.

Now, consider the connection of a new customer site 20' to an edge node 14' intended to be connected to a certain VPN. In a particular embodiment, the
25 connection will initiate a "plug-and-play" procedure that automatically will find the appropriate VPN and at least suggest how to arrange the revised VPN configuration. The control node 43 identifies that a new customer site 20' is connected and investigates which VPN it is intended for.

30 When a VPN control node 43 initiates a VPN connection request, it compares the requested VPN to the stored information about VPN's that is available through its interdomain connections. If there is a match, information about the existence of the match and preferably also about in which domain the

VPN exists and through which interdomain connections the VPN is reachable is available. In one embodiment, the path to reach an edge node connected to the requested VPN, if it is available, is returned to the requesting VPN control node. In Fig. 4, the requested VPN is the VPN 22A of Fig. 1. VPN control node 43 of domain 10E has information about that VPN 22A is available through border node 18:1 according to two different paths. One alternative to reach VPN 22A is over interdomain connection 12D, through domain 10B and over interdomain connection 12A. The VPN 22A is then present within domain 10A. Another alternative to reach VPN 22A is over interdomain connection 12D, through domain 10B and over interdomain connection 12C. The VPN 22A is then present within domain 10C. However, the VPN control node 43 of domain 10E has also information about VPN 22A via another border node 18. Here, the requested VPN 22A is reachable over interdomain connection 12E, since VPN 22A is available in domain 10C. Finally, the requested VPN 22A is reachable over interdomain connection 12G, since VPN 22A is available also in domain 10D.

The VPN control node 43 has all necessary information for finding the requested VPN. In this example, the route over interdomain connection 12E seems most simple to use, but e.g. available quality of service levels may change such decisions.

In this particular embodiment, the provided domain VPN information is spread to all VPN control nodes 43 of the entire system 1. In such a way, a request for finding a suitable VPN can be put directly to a VPN control node 43 of the "home" domain. The provision and exchanging of VPN information can as indicated before be performed continuously, regularly or even triggered by the request itself.

Another particular embodiment of the present invention is illustrated in Fig. 5. Here, the initial intradomain VPN information provision is performed just as before. In this particular embodiment, however, the domain VPN information is not brought forward to any neighbouring domain, even in a

processed form. This means that the VPN control nodes 43 now only have information about its own domain VPN's. When the VPN control node 43 initiates a connect request of the VPN control node 43 of its own domain 10E, it does only have the information about VPNs in the own domain readily available in its own databases. However, the VPN control node 43 knows what domains it is connected to and forwards instead the request over the interdomain connection 12A-G to the neighbouring domains. This is illustrated by the arrows 32. A VPN control node 43 receiving such request over an interdomain connection investigates its own databases to see if there are any data of interest. If not, a new forwarding over an interdomain connection will take place until information about the requested VPN is achieved. This information will then be brought back to the VPN control node of the original domain 10E.

This particular embodiment has the advantage that not the entire system 1 has to be updated in every single VPN control node 43. However, instead the finding of the VPN will be somewhat more complicated.

In an alternative embodiment, the VPN connection request is sent directly to one, several or all of the other VPN control nodes in the other domains in the total system, not restricted to the neighbouring domains. This means that the request is not forwarded in a chain as in the other embodiment, but merely broadcasted through the system. The availability of such direct request forwarding can be regulated by domain SLAs.

Fig. 6A illustrates a block scheme of a particular embodiment of a relatively general VPN control node 43 according to the present invention. The VPN control node 43 comprises means 52 for providing domain VPN information. This information may be provided by other nodes in the domain by connections 62. A main control communication interface 40 is provided for communication with other domains. This interface 40 may be arranged in combination with the intra-domain connections 62. A matching unit 49 investigating if an identity of a requested VPN matches with domain VPN

information is provided. The VPN request can be received from another domain, from another node of the own domain or a VPN connect request can be initiated within the VPN control node. An external VPN handling section 44 is responsible for handling interdomain VPN configuration. An internal VPN handling section 41 has functionalities for configuring internal connections within the own domain.

Fig. 6B illustrates a block scheme of another particular embodiment of a VPN control node 43 according to the present invention. Domain VPN information regarding the own domain is provided by an internal VPN handling section 41. The internal domain VPN information is in this particular embodiment stored in a data memory 52. This information is in this particular embodiment provided, as illustrated by the arrow 62, by communication with other nodes within the domain. In other embodiments, this information can be obtained in other ways. The internal domain VPN information is also forwarded to a total VPN information database 54 in an external VPN handling section 44. The internal VPN handling section 41 also comprises an internal configuration machine 46, having functionalities for configuring internal connections within the own domain. The internal VPN handling section 41 is provided with internal domain VPN information, as well as information from the database 54. Communications regarding internal domain matters are thus performed over a connection 42 between the internal VPN handling section 41 and the external VPN handling section 44.

The VPN control node 43 has a main control communication interface 40 with other domains over an interdomain connection. Domain VPN information from other domains are received by the interface 40, and an input processing unit 56 extracts useful information from the received data and stores this external information in an input database 58. In this input database 58, additional information as from which domain the external data was received is also stored. The input database 58 updates the total VPN information database 54 when appropriate. The external VPN handling

section 44 also comprises an external configuration machine 60, having functionalities for configuring parts of interdomain connections that are relevant for the domain. This functionality will be described more in detail below.

5

The external VPN handling section 44 also provides information to other domains. Domain VPN information, associated with the own domain and/or with other domains is extracted from the database 54 and provided to an output data processing unit 50. The retrieved information is processed according to SLAs associated with the different neighbour domains and stored in an output database 48. The SLAs thereby determines what information is allowed to be spread to the different neighbouring domains. Domain operators having a close relationship may allow for more transparent exchange of information, whereas domains belonging to non-related operators may apply a more restrictive information exchange. Information about VPN's is transmitted on the interface 40, when suitable.

A matching unit 49 investigating if an identity of a requested VPN matches with domain VPN information is provided. The VPN request can be received from another domain, from another node of the own domain or a VPN connect request can be initiated within the VPN control node itself. When a match between a requested VPN and the VPN information of the VPN control nodes is achieved, a re-configuration of an inter-domain VPN has to be performed. The implementation can be performed in many different ways, using typical procedures known as such in prior art. One exemplifying embodiment will be described below, which assumes that all VPN information is spread across the whole system, i.e. similar to what is illustrated in Fig. 4.

After matching of the VPN connection request for a user, the assumption is that all VPN control nodes in all domains has a VPN database of where to find VPNs in the system. In each domain database, there is "nexthop" information for each VPN ID not presently in the domain, which points out the neighbour domain ID where this VPN ID can be found. In the neighbour

domain, there is either a VPN already configured for this VPN ID, or new "nexthop" information where to find the VPN ID. The different databases in the domains can thus be interpreted as "VPN routing tables", that shows how to find ways to already configured VPNs. For each "nexthop" information there may be different policy rules associated. Depending on the policy rules, the VPN control node in each domain can choose to set up VPN connections to one or several of the "nexthop" domains.

An example, illustrated in Fig. 7, shows how the configuration of an interdomain VPN can be automated. A new customer site 20' in the domain 10E shall be connected to VPN 22A. It is assumed that VPN tunnels are used for VPN connections both inside domains and between domains. The following steps are taken.

The VPN control node in domain 10E gets a request, in some way, from the customer to connect to VPN 22A. Since the VPN database of domain 10E shows that the VPN 22A is not present in domain 10E, the VPN control node in domain 10E cannot connect customer site 20' directly to the VPN 22A inside domain 10E. However, a match is found between the connect request and VPN information originated from other domains. The database shows that VPN 22A can be found at "nexthop" 10B, 10C and 10D, presently configured and running in domain 10A, 10C and 10D.

The VPN control node in domain 10E chooses to set up the VPN via the "nexthop" 10B only. It sets up a VPN tunnel 71 for VPN 22A from the edge node 14' where the customer site 20' is connected, to the border node 18:1, which is connected to domain 10B via link 12D. The VPN control node in domain 10E initiates communication with the VPN control node in domain 10B and sets up a VPN tunnel 72 for VPN 22A over the link 12D to border node 18:2. Since VPN 22A is not present in domain 10B, the VPN control node in domain 10B checks its VPN database and sees that VPN 22A can be found at "nexthop" 10A and 10C.

The VPN control node in domain 10B chooses to set up the VPN via the "nexthop" 10A only. It sets up a VPN transit tunnel 73 for VPN 22A from the border node 18:2, which is connected to domain 10B via link 12D, to the border node 18:3, which is connected to domain 10A via link 12A. The VPN control node in domain 10B initiates communication with the control node in domain 10A and sets up a VPN tunnel 74 over the link 12A to border node 18:4. Since VPN 22A is present in domain 10A, the control node in domain 10A can set up an internal tunnel 75 from the border node, which is connected to domain 10B via link 12A, to the border node 18:5, which is connected to the VPN 22A.

After each step, the updated VPN databases will be available for the next round of collecting VPN information.

The basic steps of an embodiment of a method according to the present invention are illustrated in Fig. 8. The procedure starts in step 200. In step 210, a connect request is initiated. This request concerns connecting a first edge node in a first domain to a VPN not presently available in the first domain. In step 212, domain node information is collected. In step 214, an identity of the first VPN is matched to VPN identities of collected node information. Based on the outcome of the matching step, the first VPN is configured to comprise the first edge node, in step 216. The procedure ends in step 299.

The embodiments described above are to be understood as a few illustrative examples of the present invention. It will be understood by those skilled in the art that various modifications, combinations and changes may be made to the embodiments without departing from the scope of the present invention. In particular, different part solutions in the different embodiments can be combined in other configurations, where technically possible. In particular, any combination of pull/push, inter-/intra-domain, broadcast/neighbour communication and information/request is possible to apply. The scope of the present invention is, however, defined by the appended claims.

CLAIMS

1. Method for configuration of a multi-domain virtual private network (22A-C) - VPN - within a communications network (1), the communications network (1) having at least two domains (10A-E) interconnected to each other, and whereby customers are connected to VPNs (22A-C) at edge nodes (14; 14') of the at least two domains (10A-E), comprising the steps of:

initiating a connect request for connecting a first edge node (14') in a first domain (10E) to a first VPN (22A) not presently available in the first domain (10E);

providing (24; 62) domain VPN information within the at least two domains;

the domain VPN information comprising at least VPN identity of VPNs available in respective domain;

matching an identity of the first VPN (22A) with VPN identities of a second domain of the at least two domains different from the first domain (10E); and

configuring the first VPN (22A) to comprise the first edge node (14') based on the outcome of the matching step.

2. Method according to claim 1, **characterised in that** the step of matching in turn comprises the steps of:

sending (32) an information request about existence of the first VPN (22A) from the first domain (10E) to an adjacent domain (10B-D); and

comparing the information request with provided domain VPN information in a domain different from the first domain (10E).

3. Method according to claim 1, **characterised in that** the step of matching in turn comprises the steps of:

sending (32) an information request about existence of the first VPN (22A) from the first domain (10E) to one, several or all domains (10B-D); and

comparing the information request with provided domain VPN information in a domain different from the first domain (10E).

4. Method according to claim 2 or 3, **characterised in that** the step of matching in turn comprises the steps of:

5 returning an acknowledgement to the first domain (10E) if a match is found.

5. Method according to claim 2 or 4, **characterised in that** the step of matching further comprises the step of:

10 forwarding the information request about existence of the first VPN to further adjacent domain if no match is found.

6. Method according to any of the claims 2 to 5, **characterised in that** the acknowledgement additionally comprises data representing at least one of:

15 domain ID of domain in which the first VPN (22A) is available;

edge node ID of edge node (14) in which the first VPN (22A) is available;

information about which domains that has to be transited to reach the domain in which the first VPN (22A) is available; and

20 routing information to the edge node in which the first VPN (22A) is available.

7. Method according to claim 1, **characterised in that** the step of matching in turn comprises the steps of:

processing the domain VPN information into processed VPN information comprising at least one VPN identity;

25 transferring (28) the processed VPN information between adjacent domains;

comparing the identity of the first VPN (22A) with the transferred processed VPN information.

30 8. Method according to claim 1, **characterised in that** the step of matching in turn comprises the steps of:

processing the domain VPN information into processed VPN information comprising at least one VPN identity;

transferring (28) the processed VPN information to one, several or all domains;

comparing the identity of the first VPN (22A) with the transferred processed VPN information.

5

9. Method according to claim 7 or 8, **characterised in that** the step of matching comprises the further step of further processing the transferred processed VPN information before the comparing step.

10

10. Method according to claim 7 or 9, **characterised in that** the processed VPN information to be transferred to other domains additionally comprises processed VPN information received from adjacent domains.

15

11. Method according to claim 10, **characterised in that** the step of processing comprises addition of transit information regarding the processed VPN information transferred from other domains or information derived therefrom.

20

12. Method according to any of the claims 7 to 11, **characterised in that** the processed VPN information additionally comprises at least one of:

domain ID of domains (10A-E) in which different VPNs (22A-C) are available;

edge node ID of edge nodes (14, 14') at which different VPNs (22A-C) are available;

25

information about which domains (10A-E) that has to be transited to reach the domain (10A-E) in which different VPNs (22A-C) are available; and

routing information to the edge node (14, 14') at which different VPNs (22A-C) are available.

30

13. Method according to any of the claims 7 to 12, **characterised in that** the step of transferring of processed VPN information is performed on a regular basis.

14. Method according to any of the claims 7 to 12, **characterised in that** the step of transferring of processed VPN information is performed as a response on changes of domain VPN information.

5 15. Method according to any of the claims 7 or 14, **characterised in that** the step of transferring of processed VPN information is performed as a response of the connect request.

10 16. Method according to any of the claims 1 to 15, **characterised in that** the domain VPN information further comprises customer identities of customers connected to the respective edge nodes (14, 14') and associated VPN (22A-C).

15 17. Method according to any of the claims 1 to 16, **characterised in that** the domain VPN information further comprises properties of the VPNs (22A-C).

18. Method according to claim 17, **characterised in that** the properties of the VPNs comprise at least one of:

20 quality of service properties;
encryption properties;
transparency layer properties;
tunnelling properties; and
topology properties.

25 19. Method according to any of the claims 1 to 18, **characterised in that** the step of providing domain VPN information in turn comprises collecting of domain VPN data from edge nodes within the same domains.

30 20. Method according to claim 19, **characterised in that** the collecting of domain VPN data is performed in a centralised manner in at least one domain.

21. Method according to claim 19, **characterised in that** the collecting of domain VPN data is performed in a distributed manner in at least one domain.

22. Method according to any of the claims 19 to 21, **characterised in that** the collecting of domain VPN data is performed by a push mechanism.

23. Method according to any of the claims 19 to 21, **characterised in that** the collecting of domain VPN data is performed by a pull mechanism.

24. Communications network (1), comprising:
at least two network domains (10A-E) being interconnected by connections (12A-G) between border nodes (18);

means for operating virtual private networks (22A-C) - VPNs - within the communications network (1);

edge nodes (14, 14') connected by the VPNs (22A-C), whereby customer sites (20) of the VPNs (22A-C) are connected at the edge nodes (14, 14');

means for initiating a connect request for connecting a first edge node (14') in a first domain (10E) to a first VPN (22A) not presently available in the first domain (10E);

VPN control nodes (43) in each of the at least two network domains (10A-E) comprising means (41) for providing domain VPN information;

the domain VPN information comprising at least VPN identity of VPNs available in the domain (10A-E);

means for matching an identity of the first VPN with VPN identities of a second domain (10A-D) of the at least two domains (10A-E) different from the first domain (10E); and

means for configuring the first VPN (22A) to comprise the first edge node (14') based on the output of the means for matching.

25. Communications network according to claim 24, **characterised in that** the VPN control node (43) is a centralised node in at least one domain (10A-E).

26. Communications network according to claim 24 or 25, **characterised in that** the VPN control node (43) is a distributed node in at least one domain (10A-E).

5 27. Communications network according to claim 26, **characterised in that** at least a part of the distributed VPN control node (43) is in logical connection with a border node (18), whereby communication between the distributed VPN control node (43) and domains connected through the border node (18) takes place via the border node (18).

10 28. Communications network according to any of the claims 24 to 27, **characterised in that** the VPN control node (43) comprises a storage (54) for VPN information.

15 29. Communications network according to any of the claims 24 to 28, **characterised in that** the means for matching is distributed in all domains (10A-E), which distributed parts in turn comprise:

request handling means for sending and receiving information requests about existence of a particular VPN to and from an adjacent domain; and

20 means for comparing received information requests with provided domain VPN information of its own domain;

whereby the request handling means is further arranged for returning an acknowledgement if a match is found.

25 30. Communications network according to any of the claims 24 to 28, **characterised in that** the means for matching is distributed in all domains (10A-E), which distributed parts in turn comprise:

request handling means for sending and receiving information requests about existence of a particular VPN to and from one, several or all domains; and

30 means for comparing received information requests with provided domain VPN information of its own domain;

whereby the request handling means is further arranged for returning an acknowledgement if a match is found.

31. Communications network according to claim 29 or 30, **characterised in that** the request handling means is further arranged to forward an information request to further adjacent domains if no match is found.

32. Communications network according to any of the claims 24 to 28, **characterised in that** the VPN control node (43) further comprises:

first processor (50) for processing the domain VPN information into processed VPN information, connected to the storage (54); and

means for transferring the processed VPN information to other domains, connected to the first processor (50).

33. Communications network according to claim 32, **characterised in that** the VPN control node (43) further comprises:

means for receiving processed VPN information from other domains;

second processor (56) for processing the received processed VPN information, connected to the means for receiving and the storage (54),

whereby the processed received VPN information can be stored in the storage (54).

34. Communications network according to any of the claims 24 to 33, **characterised in that** the VPN control nodes (43) in at one network domain (10A-E) comprises means (41) for collecting domain VPN information from edge nodes in the same domain.

35. VPN control node (43) in a first domain of a communications network (1) having at least two domains (10A-E) and supporting multi-domain virtual private networks (22A-C) - VPNs, customers being connected to the VPNs (22A-C) at edge nodes (14, 14') of the at least two domains (10A-E), the VPN control node (43) comprising:

means (52, 62) for providing domain VPN information;

the domain VPN information comprising at least VPN identity of VPNs available within the first domain; and

means for matching an identity of a requested first VPN with the VPN identities.

5

36. VPN control node according to claim 35, **characterised by** further comprising a configuring machine (46) for VPN connections within the first domain.

10

37. VPN control node according to claim 35 or 36, **characterised by** further comprising a configuring machine (60) for inter-domain VPN connections involving the first domain.

15

38. VPN control node according to any of the claims 35 to 37, **characterised in that** the control node (43) is a centralised node.

39. VPN control node according to claim 38, **characterised by** means for communicating with VPN control nodes in other domains via border nodes.

20

40. VPN control node according to claim 38, **characterised by** means for communicating by dedicated VPN control signal connections (47) with VPN control nodes in other domains.

25

41. VPN control node according to any of the claims 35 to 37, **characterised in that** the control node (43) is a distributed node.

30

42. VPN control node according to claim 41, **characterised in that** at least a part of the distributed control node (43) is in logical connection with a border node (18), through which data communication to neighbouring domains takes place.

43. Control node according to any of the claims 35 to 42, **characterised in that** the control node (43) comprises a storage (54) for VPN information.

44. Control node according to claim 43, **characterised in that** the storage (54) for VPN information is centralised.

5 45. Control node according to claim 43, **characterised in that** the storage (54) for VPN information is distributed.

10 46. VPN control node according to any of the claims 35 to 45, **characterised by** means for communicating domain VPN information to and from other domains.

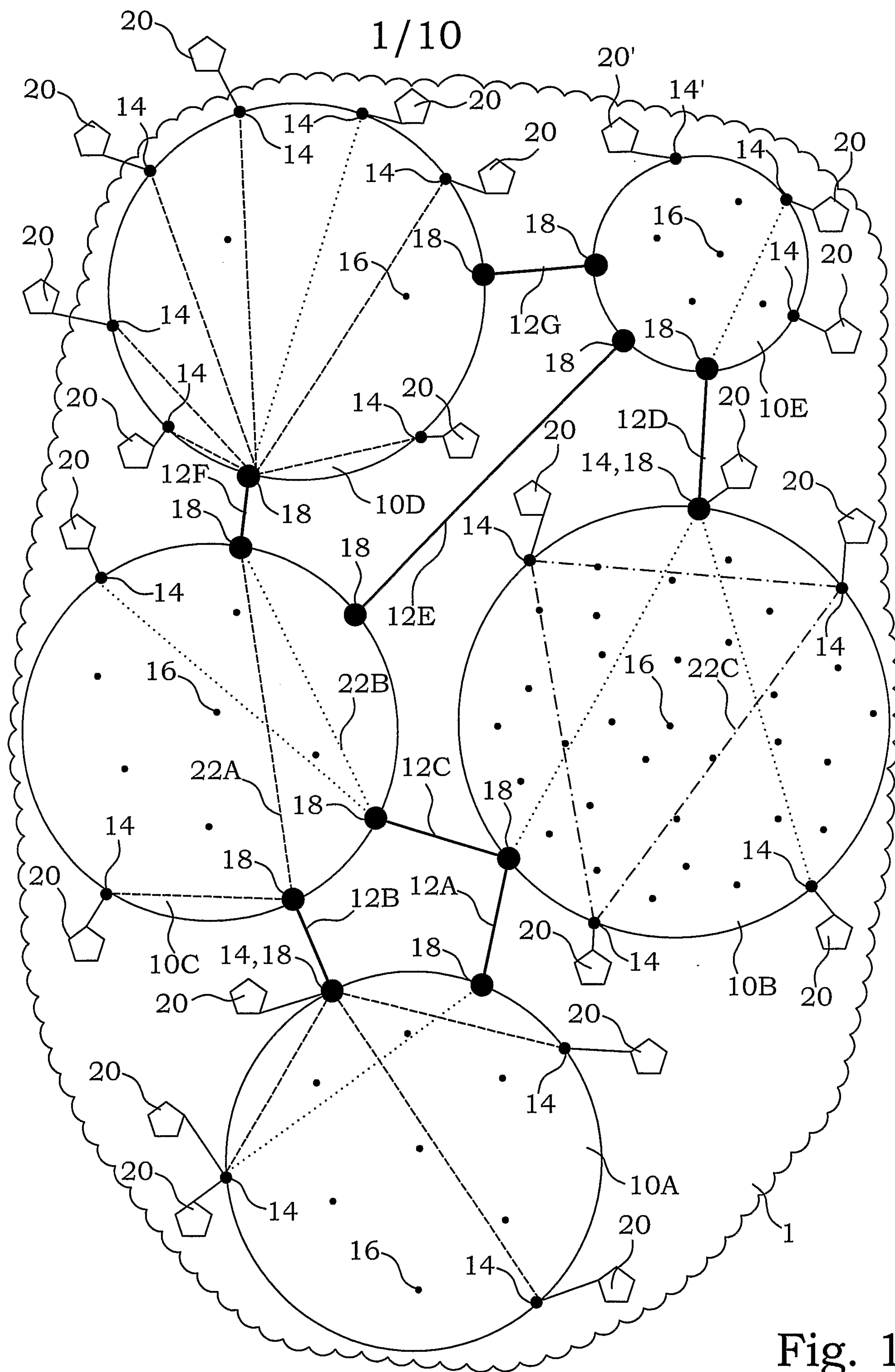
15 47. VPN control node according to any of the claims 35 to 45, **characterised by** means for receiving a VPN request, whereby the means for matching comprises means for sending an acknowledgement if a match is found.

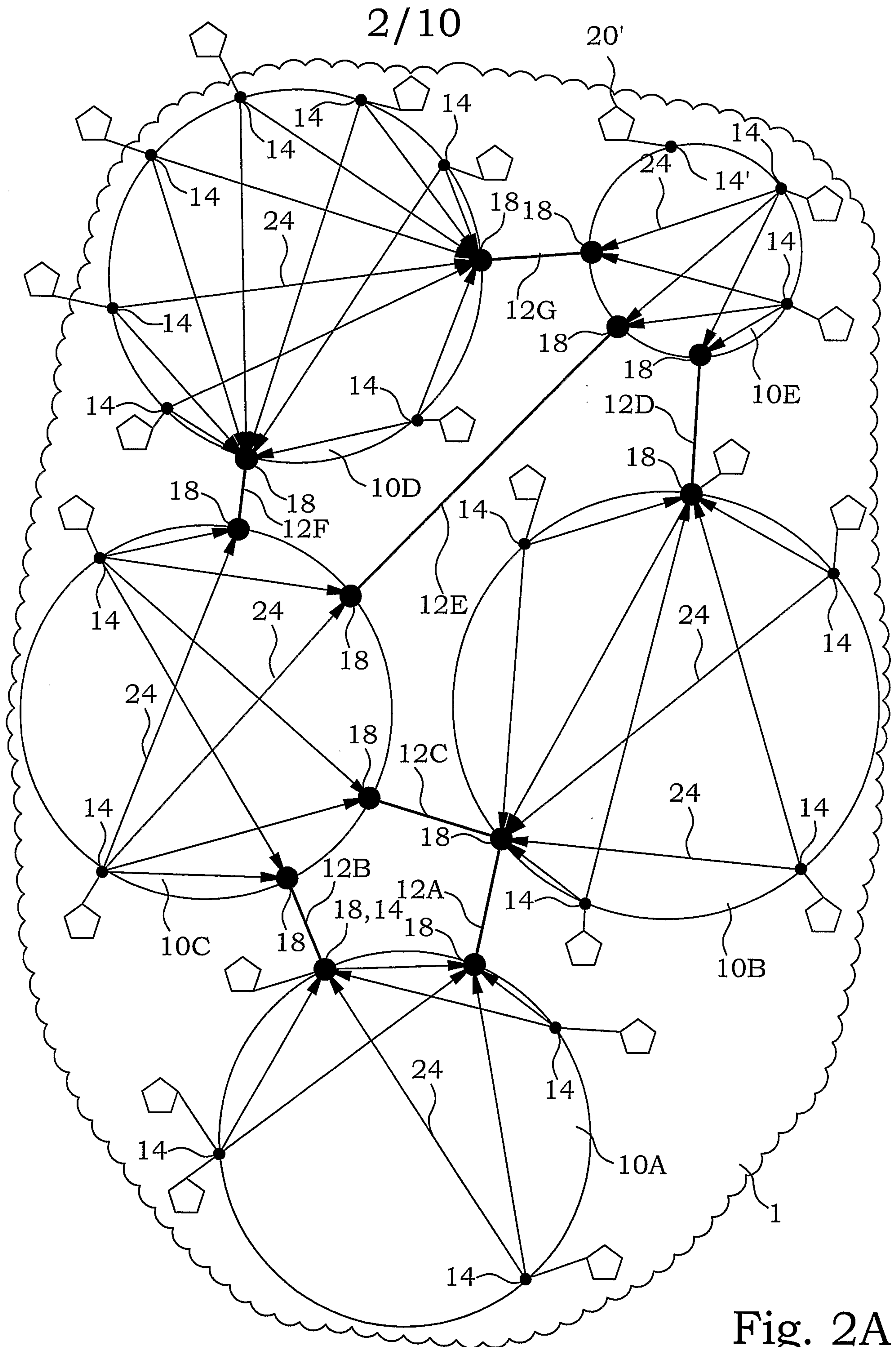
20 48. VPN control node according to claim 47, **characterised by** means for forwarding a VPN request to other domains if no match is found by the means for matching.

49. Control node according to any of the claims 35 to 45, **characterised by** means (41) for collecting domain VPN information from edge nodes in the same domain.

25 50. Method according to claim 49, **characterised in that** the means (41) for collecting domain VPN information is arranged to operate according to a push mechanism.

30 51. Method according to claim 49 **characterised in that** the means (41) for collecting domain VPN information is arranged to operate according to a pull mechanism.





3/10

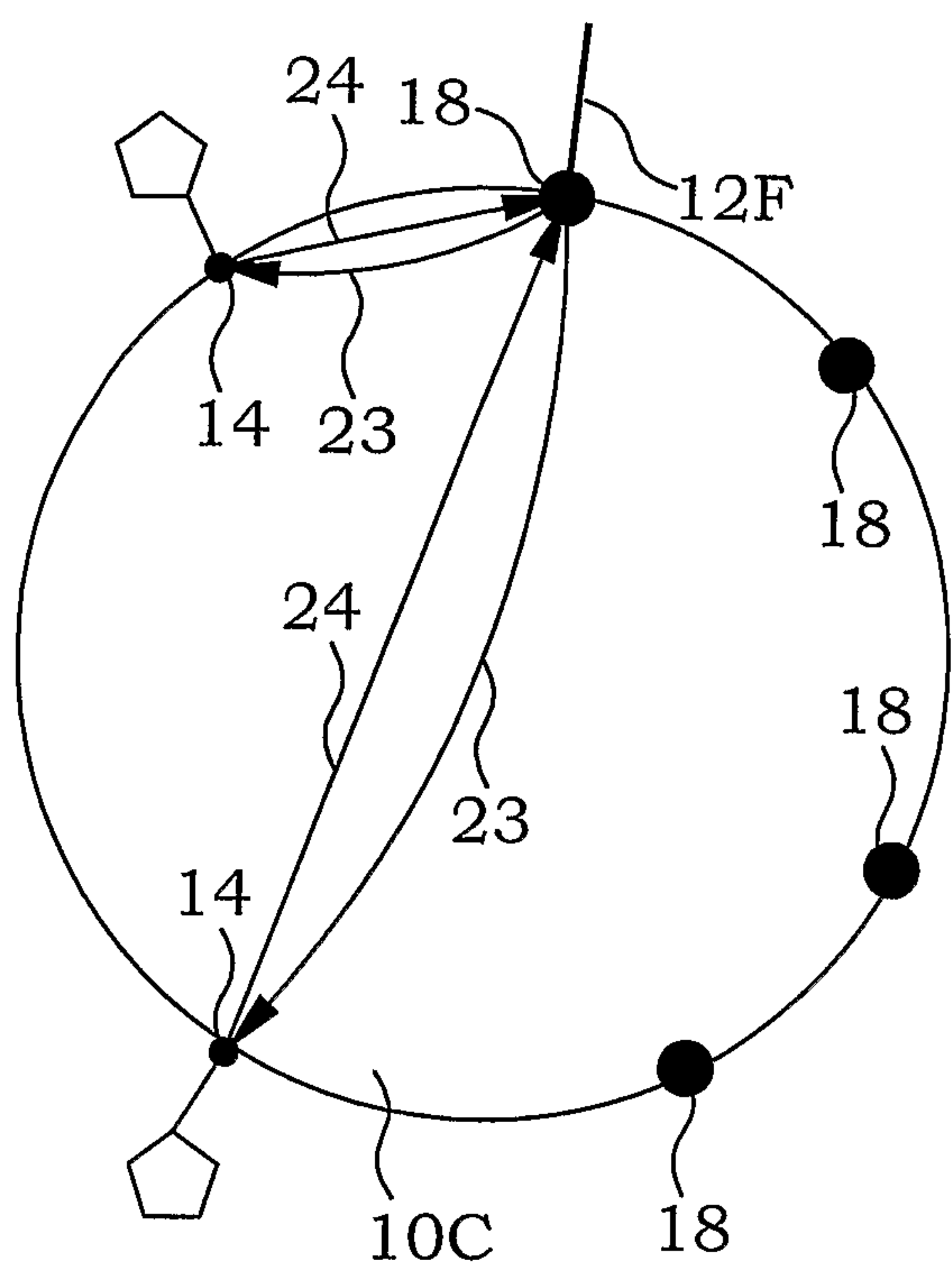


Fig. 2B

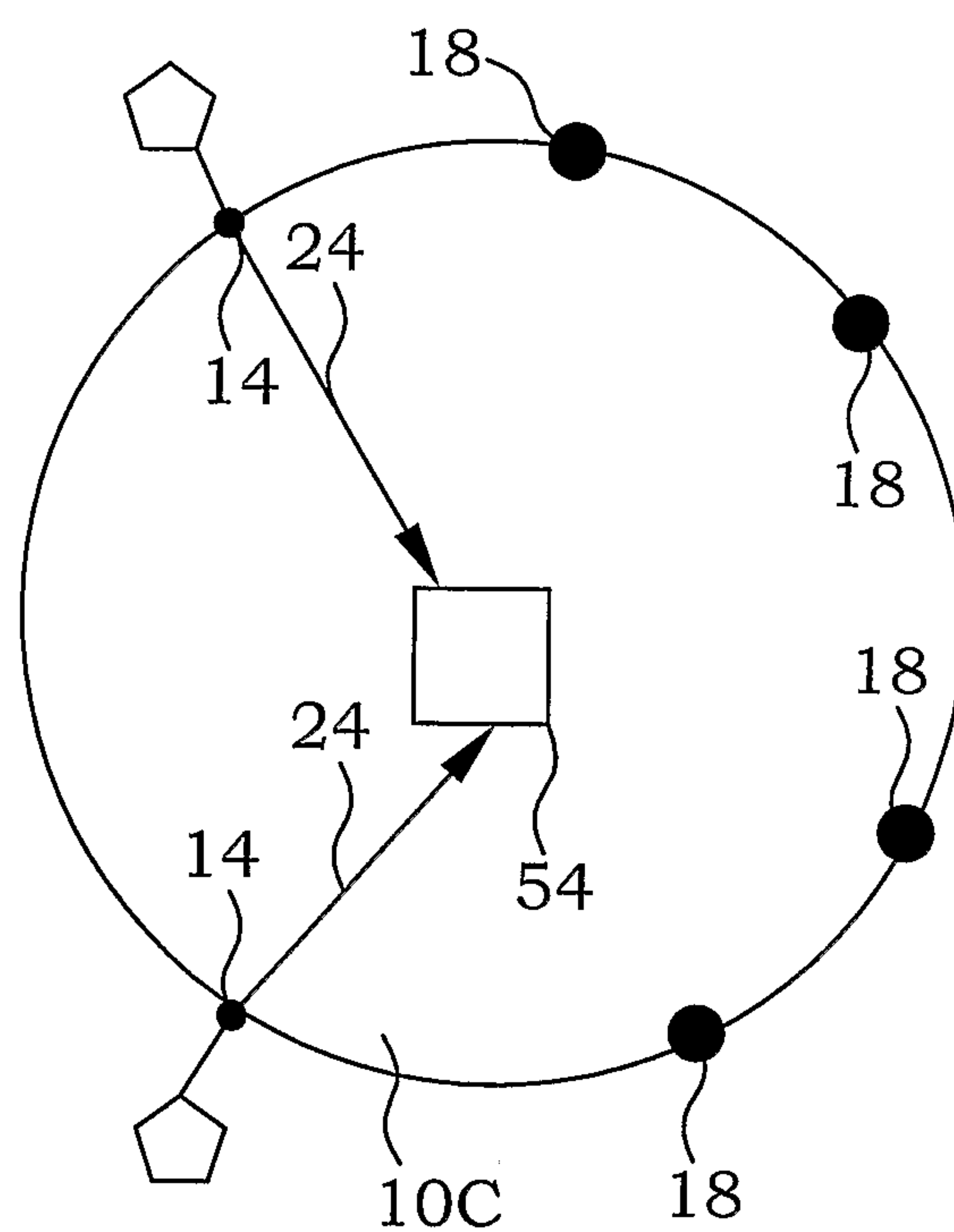


Fig. 2C

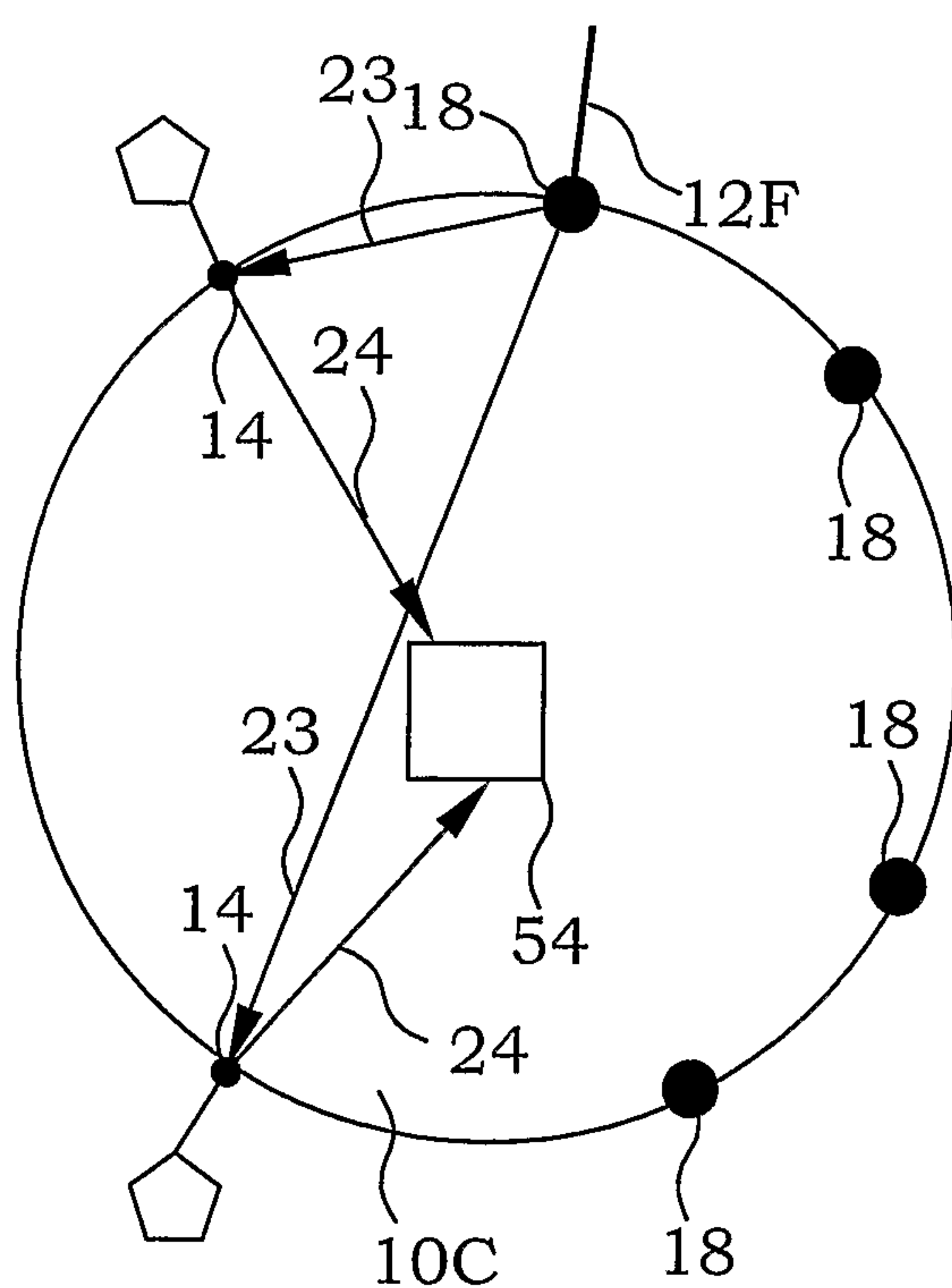
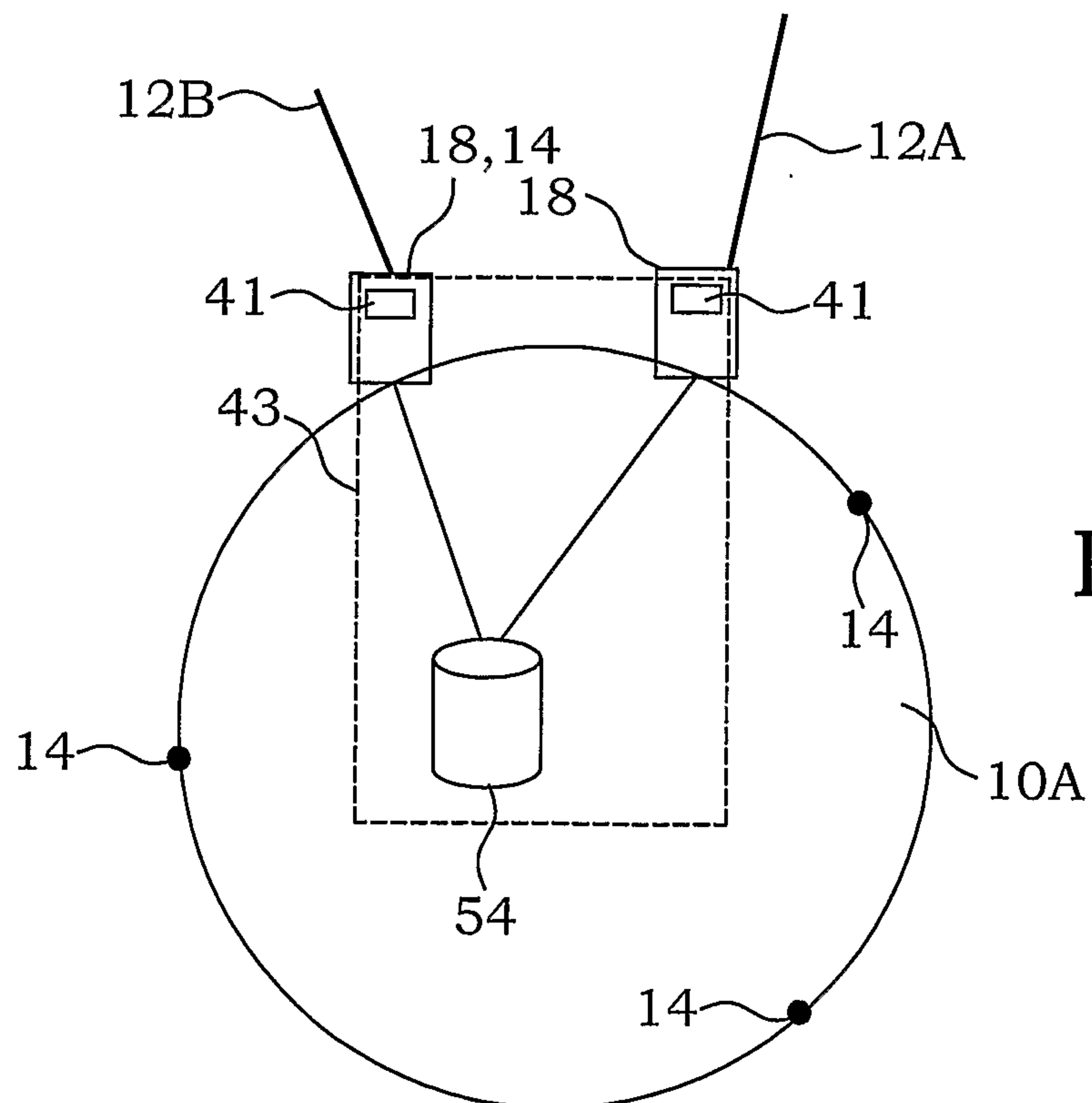
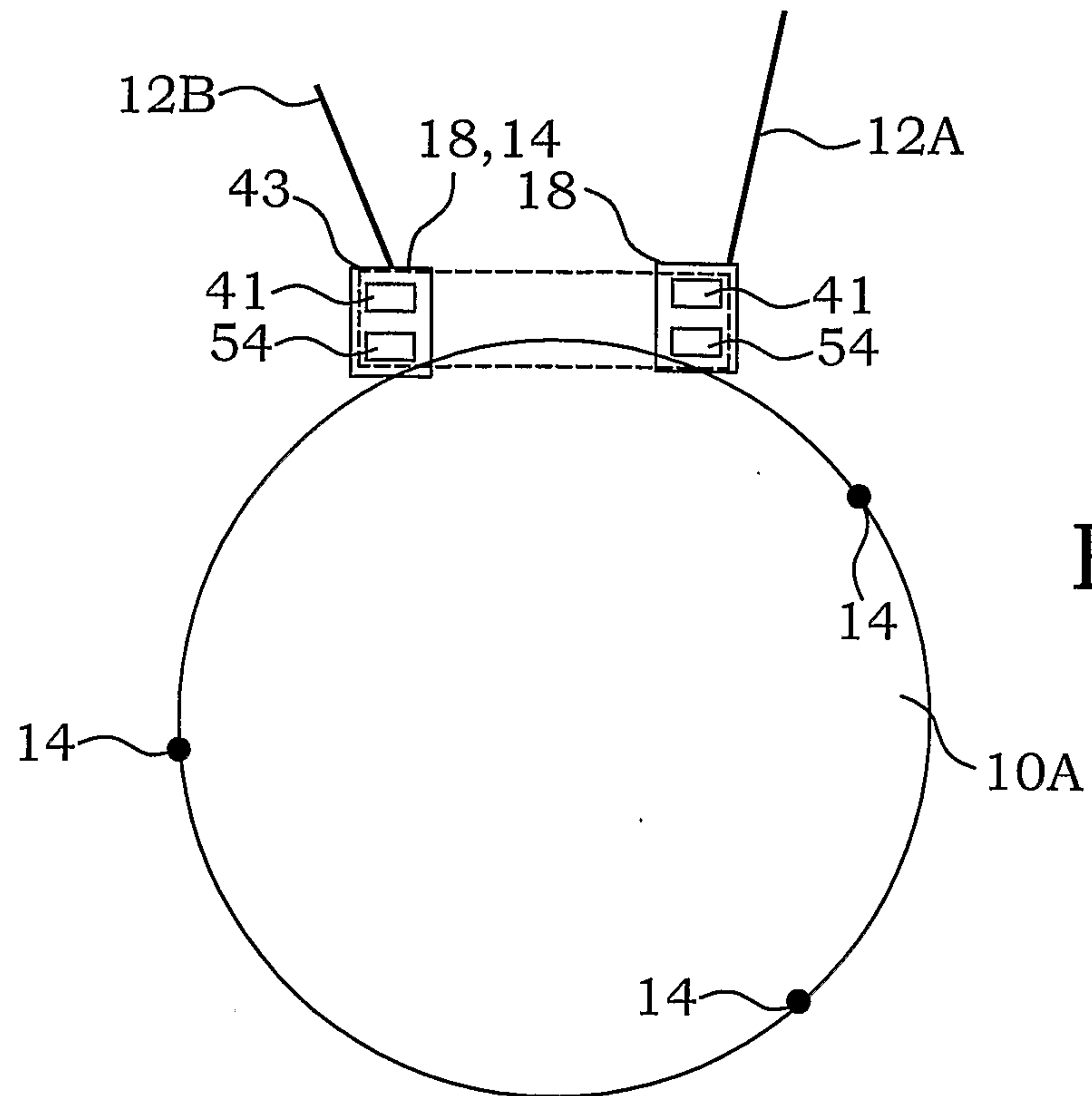


Fig. 2D

4/10



5/10

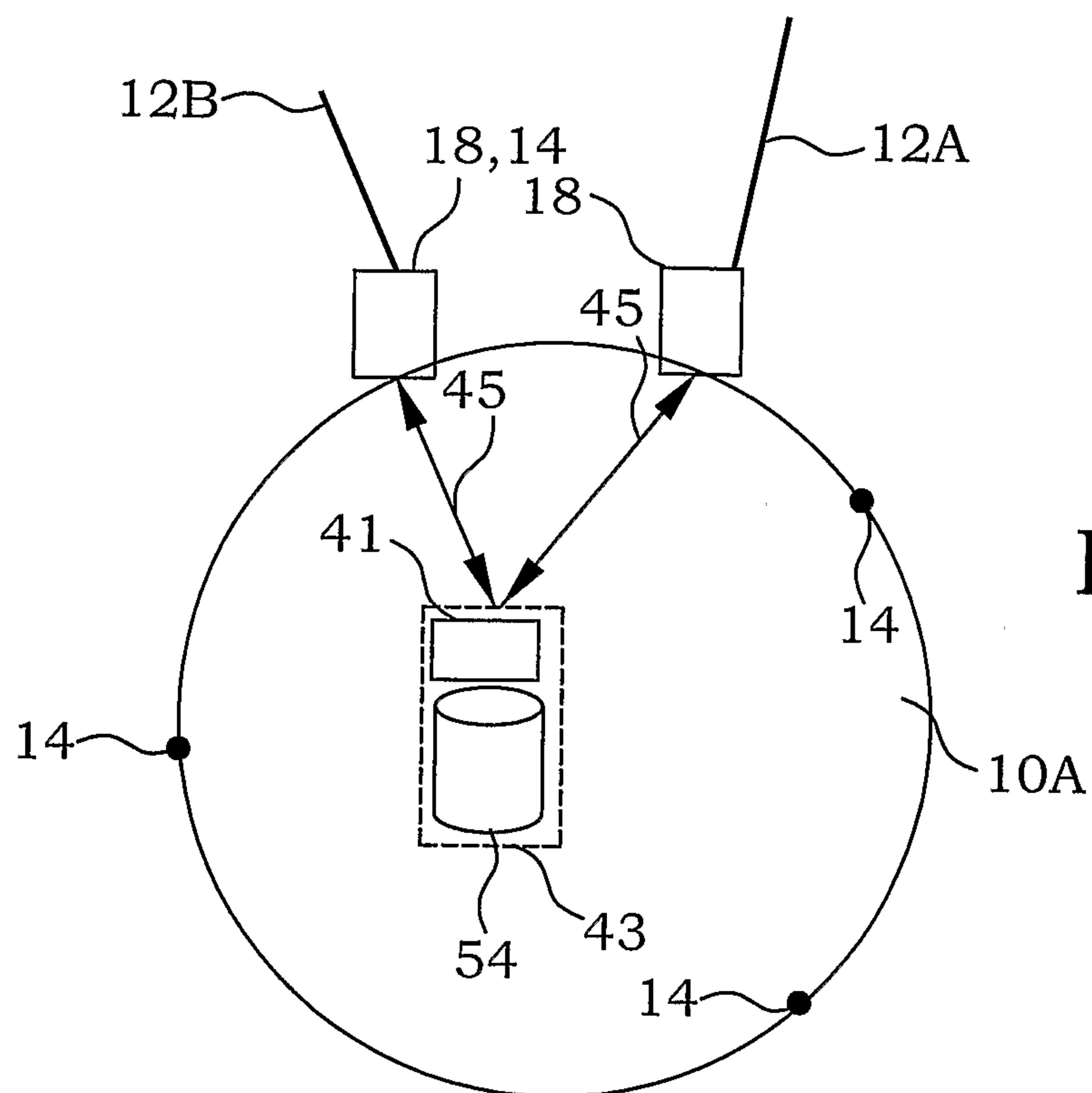


Fig. 3C

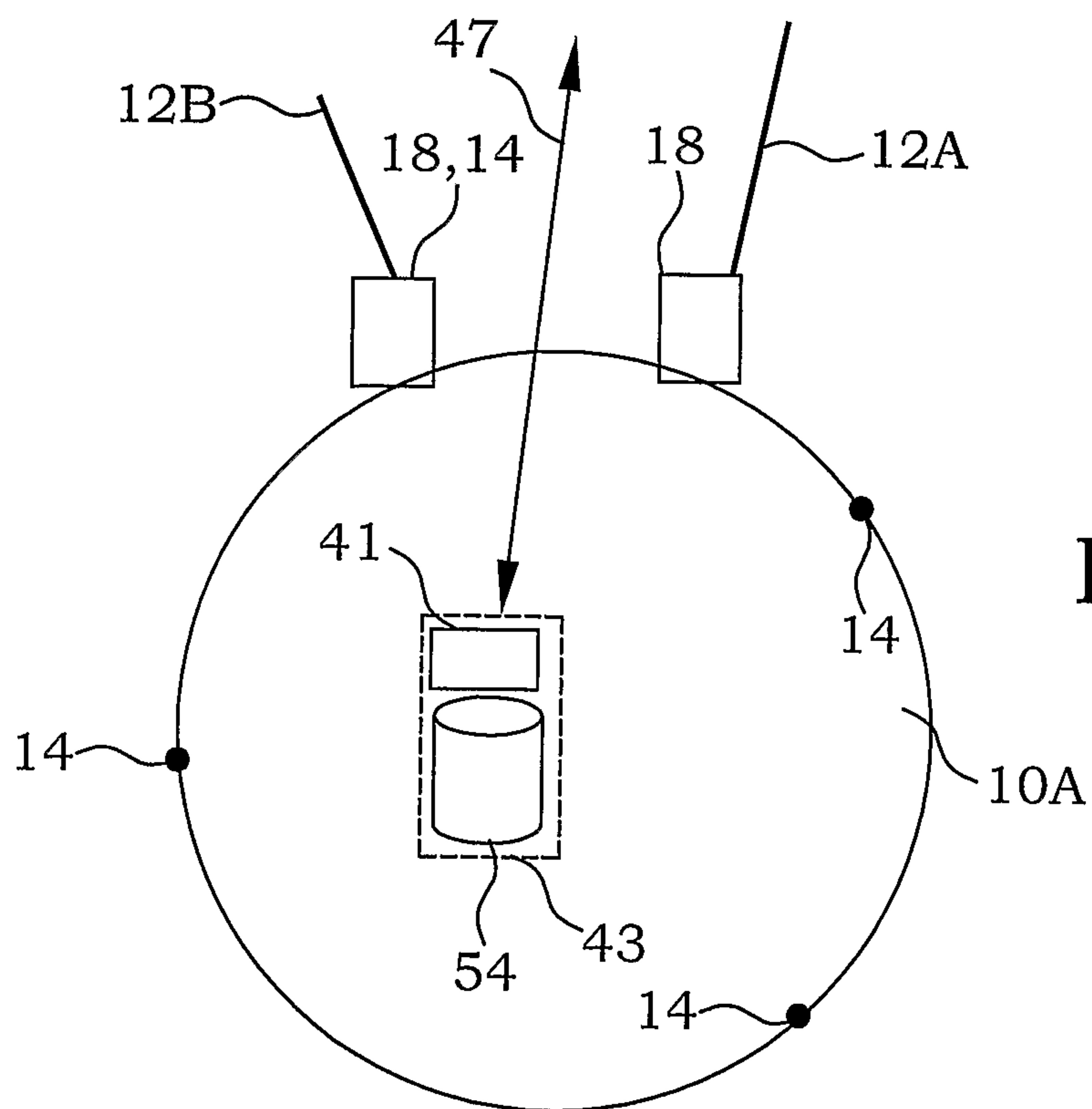


Fig. 3D

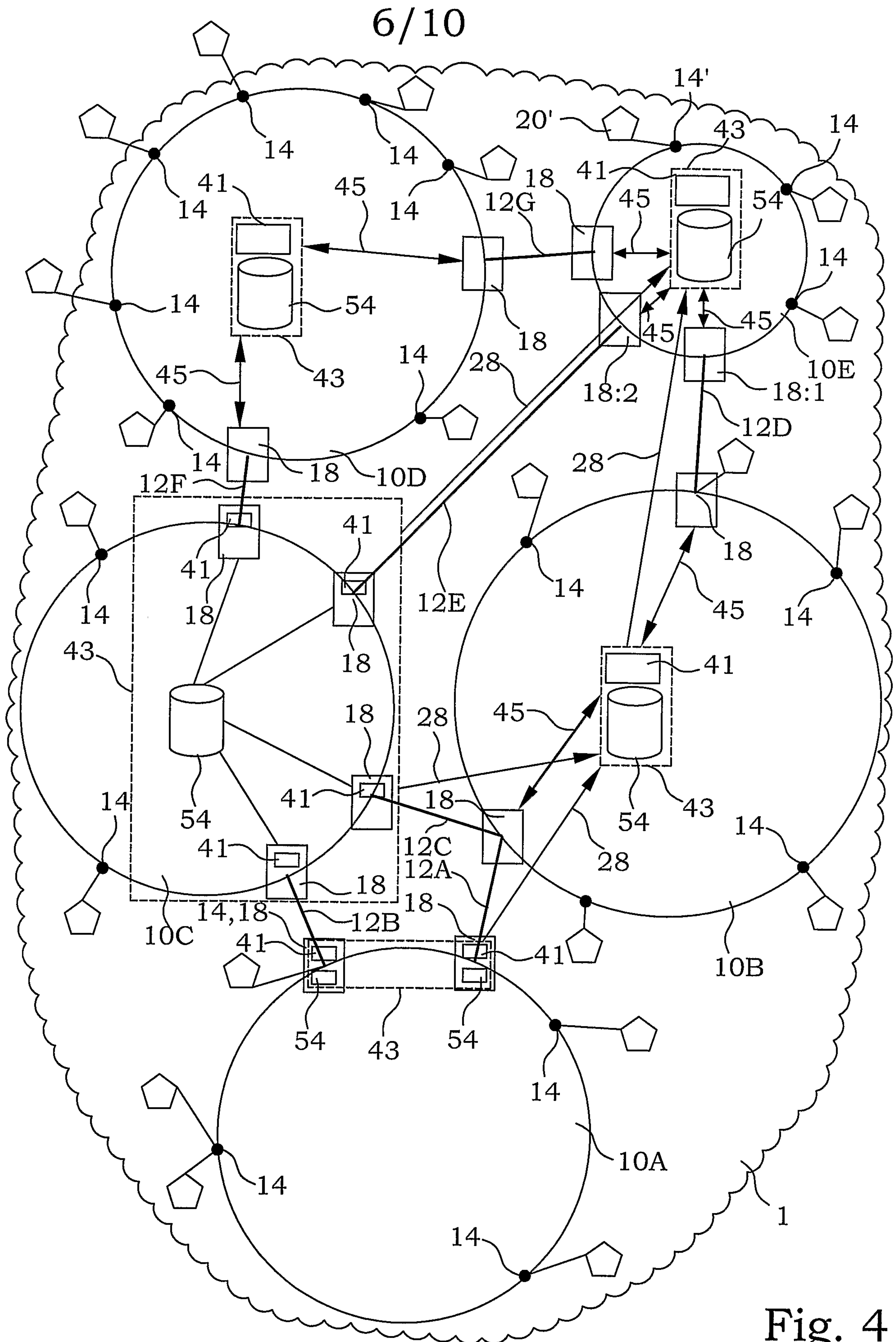


Fig. 4

7/10

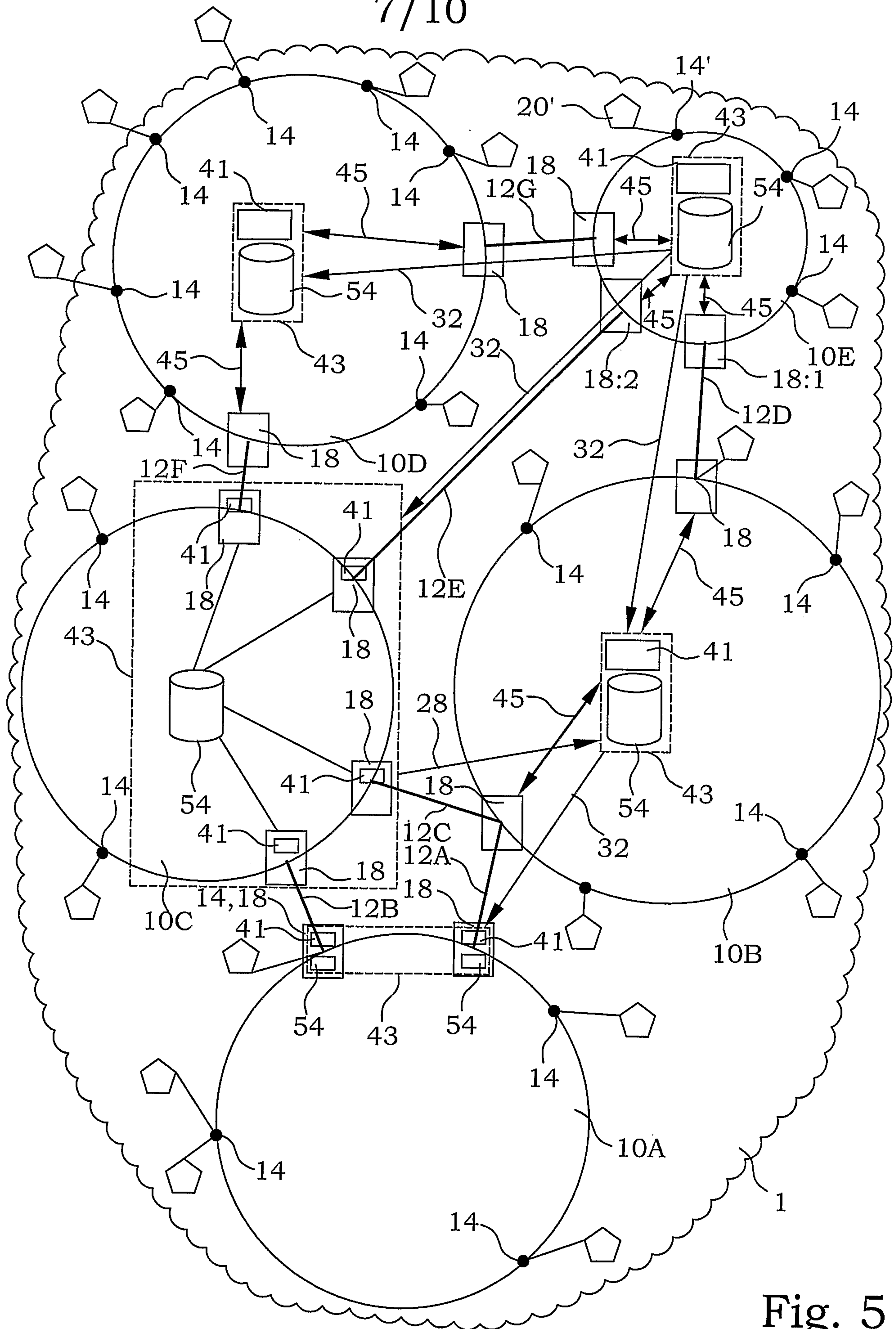


Fig. 5

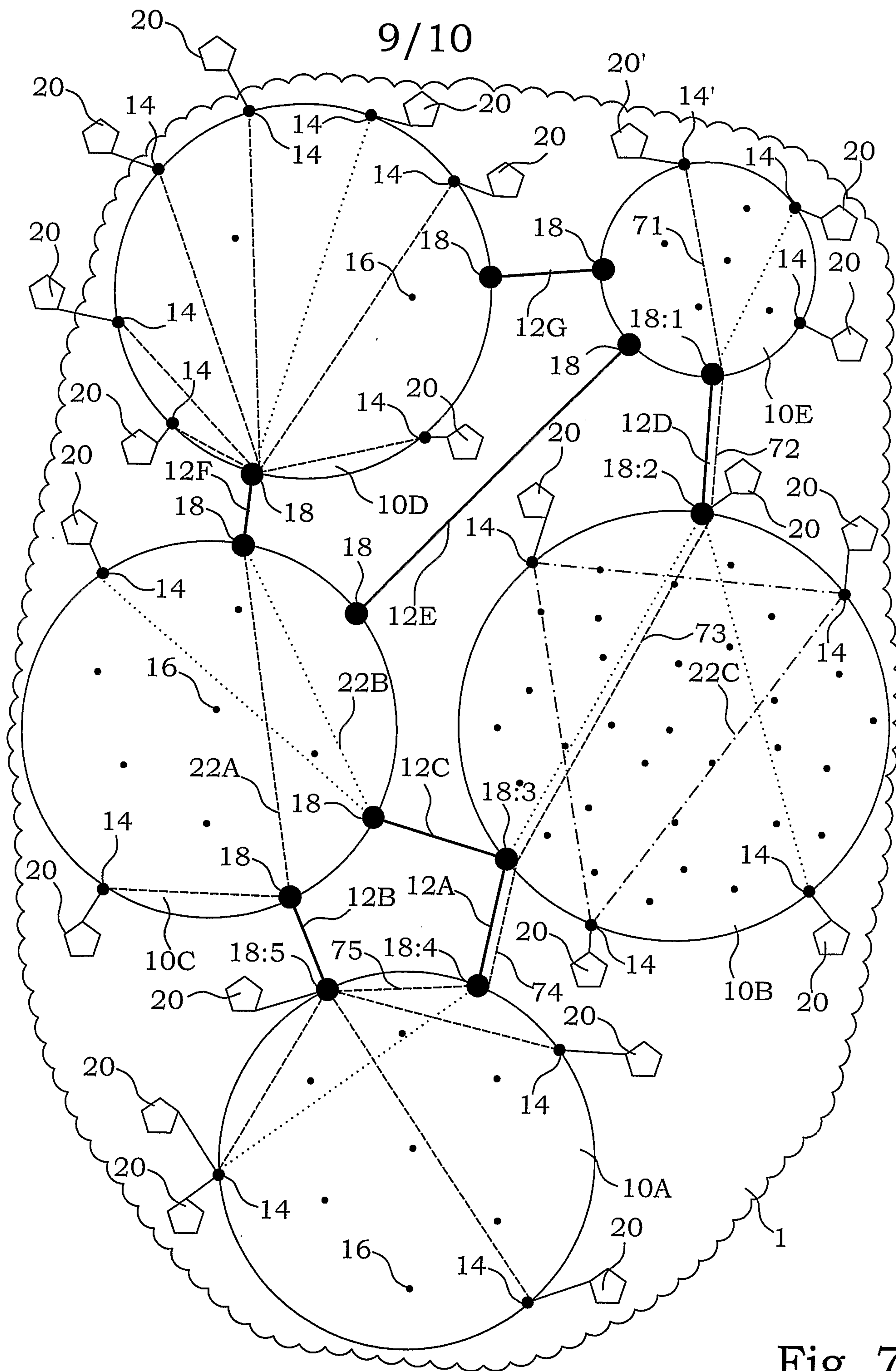


Fig. 7

10/10

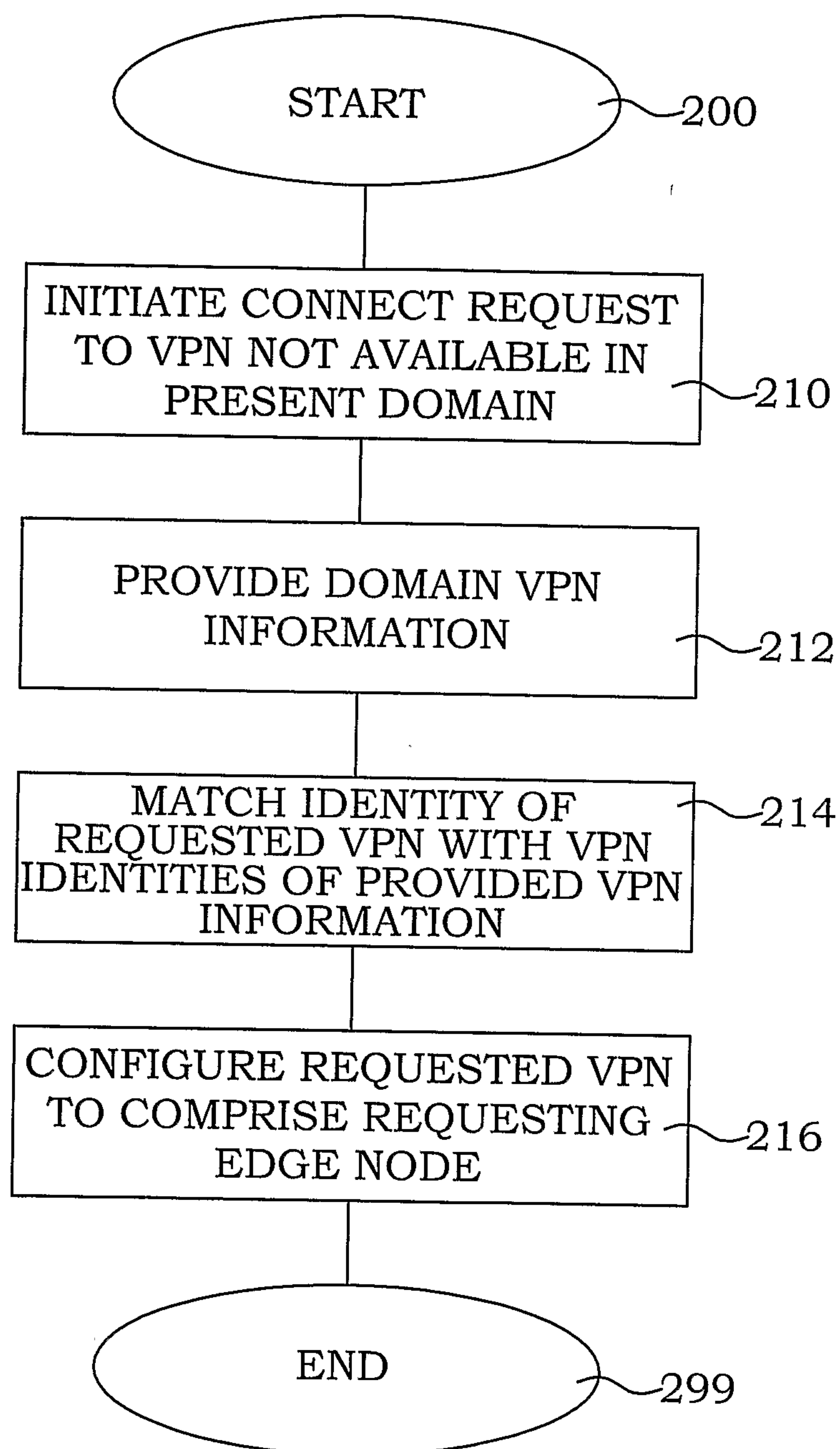


Fig. 8

