(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 389**

(51) Int. CI.:
H04L 12/46 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04749103 .0**
(96) Fecha de presentación: **30.06.2004**
(97) Número de publicación de la solicitud: **1762048**
(97) Fecha de publicación de la solicitud: **14.03.2007**

(54) Título: **PROCEDIMIENTO Y SISTEMA PARA CONFIGURACIÓN DE RED PRIVADA VIRTUAL MULTI-DOMINIO.**

(45) Fecha de publicación de la mención BOPI:
19.01.2012

(45) Fecha de la publicación del folleto de la patente:
19.01.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
FLINTA, Christofer;
MÅNGS, Jan-Erik y
WESTBERG, Lars

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento y sistema para configuración de red privada virtual multi-dominio

Campo técnico

La presente invención se refiere, en general, a redes privadas virtuales en sistemas de comunicaciones y, en particular, a la configuración de redes privadas virtuales en sistemas de comunicaciones multi-dominio.

Antecedentes

Una red privada virtual (VPN) utiliza una red de comunicaciones, pública o privada, para llevar a cabo comunicaciones privadas, véase, por ejemplo, el documento US 2004/0034702. Tradicionalmente, una empresa u otro cliente que quería construir una red de área amplia tenía que proporcionar sus propias líneas dedicadas entre cada nodo, para proporcionar la conectividad. Sin embargo, dichas soluciones son, en general, caras e inflexibles. Durante los últimos años, el concepto de VPN se ha desarrollado rápidamente. Las VPN ofrecen una solución en la que una red de comunicaciones es compartida entre muchos clientes, pero en la que la comunicación de cada cliente está separada virtualmente. La tecnología VPN se basa, frecuentemente, en la idea de la tunelización. La tunelización de red implica establecer y mantener una conexión de red lógica. En esta conexión, los paquetes son encapsulados en algún otro protocolo base o portador. A continuación, son transmitidos entre el cliente y el servidor de VPN y, finalmente, son des-encapsulados en el lado receptor. Una autenticación y un cifrado ayudan a proporcionar seguridad.

Una tendencia es que el número de nodos de red que forman una VPN crezca rápidamente, lo que resulta en una topología y unas estructuras de red largas y complejas. Esto es causado, en parte, debido al tráfico creciente en las VPNs y, en parte, a que se exige que las VPNs cubran áreas geográficas cada vez más grandes. En la actualidad, hay presentes redes de comunicación que proporcionan VPNs que tienen nodos en todos los continentes. Sin embargo, cuantos más nodos y cuanto más tráfico deba ser transmitido, más compleja será la configuración de las VPNs. Convencionalmente, una VPN es creada según un acuerdo entre un operador de red y un cliente. La ubicación de los nodos, la calidad del servicio y otras condiciones son acordadas, y un programador en el operador establece la configuración manualmente o consultando herramientas de ayuda a la configuración. Con redes de comunicaciones cada vez más complejas, dicha configuración se hace cada vez más compleja y requiere cada vez más tiempo. Además, cuando un cliente desea modificar su VPN, debe repetirse todo el procedimiento.

En el establecimiento de VPNs en una red, pueden usarse también diferentes tecnologías. Cada tecnología tiene sus propias ventajas y desventajas y su propia manera de configuración de la VPN. No hay una arquitectura de VPN general que sea independiente de la tecnología VPN.

Resumen

De esta manera, un problema general de las soluciones de la técnica anterior es que las redes de comunicaciones, que ofrecen redes privadas virtuales que tienen una gran cobertura geográfica y/o que tienen un gran tráfico, se vuelven muy complejas. Un problema adicional es que la configuración de VPNs nuevas o las modificaciones de VPNs ya existentes se vuelven complejas y requieren mucho tiempo. Un problema adicional es que los recursos de comunicación de los operadores de redes que cubren áreas geográficas más pequeñas no pueden ser utilizados, en general, para VPNs de área amplia.

Un objeto general de la presente invención es, de esta manera, mejorar los procedimientos para la configuración de VPNs, así como el suministro de sistemas y dispositivos adecuados para ello. Otro objeto de la presente invención es proporcionar procedimientos de configuración de VPNs utilizando más de un dominio de red. Otro objeto adicional de la presente invención es proporcionar procedimientos de configuración de VPNs que sean básicamente independientes de la tecnología de VPN real usada. Todavía un objeto adicional de la presente invención es proporcionar un procedimiento de configuración automática de una VPN.

Los objetivos anteriores se consiguen mediante procedimientos y dispositivos según las reivindicaciones de patente adjuntas. En términos generales, se proporciona información acerca de las VPNs en un dominio. Comparando una solicitud para una configuración de una VPN, con la información proporcionada de otros dominios conectados, puede encontrarse una correspondencia. A continuación, la re-configuración puede llevarse a cabo en base al resultado de la correspondencia. La provisión de información de dominio de VPN puede ser realizada de maneras diferentes, por ejemplo, recogiendo datos de una manera centralizada o distribuida, o recuperando datos almacenados. Un nodo de control de VPN distribuida está ubicado, en realizaciones particulares, en los nodos frontera del dominio. La información de dominio de VPN es recogida, en realizaciones particulares, desde los nodos frontera del dominio. Esto puede ser realizado extrayendo, de manera pasiva, la información transmitida desde los nodos frontera, solicitando información de dominio de VPN desde los nodos frontera o una combinación de ambos. La recogida puede ser desencadenada por un evento externo, tal como una solicitud de configuración VPN. La información de dominio de VPN proporcionada es propagada, en

una realización, a otros dominios bajo restricciones establecidas por los SLAs entre los operadores de dominio. En otra realización, la solicitud de configuración de VPN es propagada, por el contrario, a diferentes dominios. De esta manera, la correspondencia puede realizarse a diversas distancias desde el dominio solicitante original.

Una ventaja importante con la presente invención es que proporciona una plataforma simple y estable en la que los operadores de diferentes dominios pueden cooperar. La información de dominio de VPN se hace disponible para soportar la configuración de VPN en prácticamente todos los dominios de un sistema multi-dominio. Sin embargo, al mismo tiempo, en una realización, la información real es propagada sobre el sistema multi-dominio restringido por diferentes acuerdos entre los operadores.

Breve descripción de los dibujos

La invención, junto con objetos y ventajas adicionales de la misma, puede ser comprendida mejor haciendo referencia a la descripción siguiente, tomada conjuntamente con los dibujos adjuntos, en los que:

La Fig. 1 es una ilustración esquemática de una red de comunicaciones multi-dominio que proporciona redes privadas virtuales;

La Fig. 2A es una ilustración esquemática de la recogida de información VPN según una realización de la presente invención;

Las Figs. 2B-D son ilustraciones esquemáticas de la recogida de información VPN según otras realizaciones de la presente invención;

Las Figs. 3A-D son realizaciones según la presente invención de configuraciones de un nodo de control de VPN dentro de un dominio;

La Fig. 4 es una ilustración esquemática de solicitudes de conexión y reenvío de información VPN según una realización de la presente invención;

La Fig. 5 es una ilustración esquemática de solicitudes de conexión y reenvío de información VPN según otra realización de la presente invención;

La Fig. 6A es un esquema de bloques de una realización de un nodo de control de VPN general según la presente invención;

La Fig. 6B es un esquema de bloques de otra realización de un nodo de control de VPN según la presente invención.

La Fig. 7 es una ilustración esquemática de una configuración de VPN según una realización de la presente invención; y

La Fig. 8 es un diagrama de flujo que ilustra las etapas principales de una realización de un procedimiento según la presente invención.

Descripción detallada

Una realización de una arquitectura 1 de proveedor de VPN general es ilustrada en la Fig. 1. En esta arquitectura de proveedor de VPN, hay presentes cinco dominios 10A-E de proveedor VPN, que están unidos entre sí por conexiones 12A-G de datos entre dominios. Un operador puede controlar uno o más de estos dominios 10A-E, o todos ellos pueden ser controlados por operadores separados. La relación entre los dominios 10A-E, es decir, el control de las conexiones 12A-G de datos entre dominios son reguladas, típicamente, según los acuerdos entre los operadores implicados, por ejemplo, un Acuerdo de Nivel de Servicio de VPN (Service Level Agreement, SLA). Cada dominio 10A proveedor de VPN comprende nodos 14 frontera VPN y nodos 16 de núcleo, que pueden ser conocedores de la existencia de VPN o no conocedores de la existencia de VPN, de las cuales sólo unas pocas cuentan con números de referencia. Los nodos 14 frontera VPN son nodos a través de los cuales los sitios 20 de diferentes clientes están conectados a diferentes VPN en la arquitectura 1. Los nodos 16 conocedores de la existencia de VPN son sólo nodos intermedios dentro de un dominio y son usados sólo para reenviar mensajes y datos entre los nodos 14 frontera VPN. Los clientes no son conscientes de qué nodos no conocedores de la existencia de VPN son usados para la comunicación. La única cuestión importante es el nodo 14 frontera VPN inicial y final. De esta manera, una VPN conectada en un dominio puede ser representada por una línea directa entre los nodos 14 frontera VPN, incluso si la comunicación real puede tener lugar a través de uno o varios nodos 16 no conocedores de la existencia de VPN. En el resto de la presente divulgación, la existencia de nodos no conocedores de la existencia de VPN, será descartada, en general, ya que las etapas básicas del procedimiento según la presente invención no dependen directamente de la existencia o no de ningún nodo 16 no conocedor de la existencia de VPN. Sin embargo, en la aplicación práctica, es probable que los nodos 16 no conocedores de la existencia de VPN sean usados para proporcionar la conectividad real.

Los dominios 10A-E de proveedor están conectados en un plano de datos a través de los nodos 18 frontera VPN, es decir, las conexiones 12A-G de datos entre dominios empiezan y terminan en un nodo 18 frontera VPN. El nodo 18 frontera VPN puede también actuar o no, al mismo tiempo, como un nodo 14 frontera VPN. Entonces, los sitios 20 de cliente del mismo cliente pueden estar conectados a través de los dominios 10A-E de proveedor de VPN por una VPN 22A-C. Un cliente puede tener sitios 20 de cliente conectados a diferentes VPNs 22A-C. Además, más de un sitio 20 de cliente pueden estar conectados al mismo nodo 14 frontera VPN, pero no serán conscientes de la existencia de otro sitio 20 de cliente, así como de la VPN a la que está conectado el otro sitio 20 de cliente.

En la presente realización, se ilustran tres VPN 22A-C. Sin embargo, cualquier persona con conocimientos en la materia reconoce que el número de VPNs en un sistema real es, típicamente, mucho mayor. Una primera VPN 22A, ilustrada mediante líneas discontinuas, se extiende sobre tres dominios 10A, 10C y 10D y conecta los sitios 20 de cliente en todos estos dominios. Una segunda VPN 22B, ilustrada por líneas de puntos, se extiende sobre todos los dominios 10A-E de la presente realización. Finalmente, una tercera VPN 22C, ilustrada por una línea de puntos y líneas, conecta los sitios 20 de cliente sólo dentro del dominio 10B. Cada sitio 20 de cliente no es consciente de la existencia de sitios 20 de cliente de otros clientes, así como de la existencia de ninguna VPN, excepto aquella a la que está conectado. De esta manera, se conserva el carácter de privacidad de las VPNs, aunque todas ellas comparten los mismos recursos básicos de comunicaciones. Este es el escenario en el que opera, preferentemente, la presente invención.

Ahora, considérese que un nuevo sitio 20' de cliente es conectado a un nodo 14' frontera VPN en el dominio 10E. Si el sitio 20' de cliente desea ser conectado a una VPN 22B, los procedimientos son probablemente relativamente simples, ya que la VPN 22B ya está presente dentro del dominio 10E. Pueden emplearse procedimientos de reconfiguración VPN manual o automática según la técnica anterior, así como mezclas de los mismos. Sin embargo, si el nuevo sitio 20' de cliente desea conectarse a una VPN 22A o 22C, la situación se torna más difícil. En la técnica anterior, no hay procedimientos generales de configuración VPN entre dominios.

Una idea básica de la presente invención se basa en tres actividades parciales. Una parte se refiere a la provisión de información de dominio VPN, que comprende, en su versión más básica, la identidad VPN de las VPNs disponibles en el dominio respectivo. Otra parte se refiere a la búsqueda de una VPN específica a la que conectarse. En otras palabras, una correspondencia entre una VPN solicitada y la información de dominio de VPN proporcionada. En algunas realizaciones, este procedimiento de correspondencia comprende la transferencia de la información de dominio de VPN o de información derivada desde el mismo a otros dominios. En otras realizaciones, por el contrario, una solicitud para una VPN determinada es transferida entre dominios. La parte final se refiere a la re-configuración real de una VPN. Las ideas fundamentalmente nuevas de la presente invención están implicadas principalmente en las dos primeras etapas.

La Fig. 2A muestra una realización de una fase inicial de provisión de información de dominio VPN. Cada nodo 14 frontera VPN ha almacenado información que refleja su propia configuración VPN presente que indica al menos qué VPNs tienen sitios de cliente conectados a ese particular nodo 14 frontera VPN. En realizaciones particulares, el nodo 14 frontera VPN tiene también información acerca de qué clientes están conectados al nodo 14 frontera VPN y las asociaciones entre las VPN presentes y los sitios 20 de cliente. En algunas realizaciones, se proporciona información, tal como el espacio de direcciones VPN y el tipo de dirección (local o global), la calidad de las clases de servicio VPN, especificada por requerimientos tales como ancho de banda, retardo y fluctuación y/o establecimiento de VPN, es decir, el uso de túneles o filtros. También puede incluirse información tal como propiedades de encriptación, propiedades de transparencia de la capa, propiedades de tunelización y propiedades de la topología. Además, los nodos 18 frontera VPN han almacenado información sobre la identidad del dominio del proveedor VPN al que pertenecen.

Según una realización de la presente invención, la información del dominio VPN almacenada en cada nodo 14 frontera VPN, o al menos partes de la misma, es recogida por cada nodo 18 frontera en el mismo dominio 10A-E. Esto se visualiza en la Fig. 2A como flechas, algunas de las cuales están provistas de un número de referencia 24. De esta manera, la información de nodo de dominio colectivo para el propio dominio está disponible en cada nodo 18 frontera VPN de cada dominio 10A-E. Una alternativa para la comunicación es el uso de un protocolo de comunicación similar a BGP (Border Gateway Protocol), que propaga la información a lo largo de todo el dominio sin ningún conocimiento particular acerca de donde se requiere la información. A continuación, los nodos frontera pueden recoger toda la información necesaria. Este es un ejemplo de un mecanismo de tipo “push”, para la distribución de información de dominio VPN.

La Fig. 2B ilustra otra realización para proporcionar información de dominio VPN, concentrada ahora en un dominio 10C. Si el nodo 18 frontera VPN ha almacenado información acerca de qué nodos 14 frontera están presentes en el mismo dominio 10C, el nodo 18 frontera VPN puede solicitar 23 simplemente a cualquier nodo 14 frontera VPN que devuelva su información 24 de nodos de dominio. En la forma más simple de solicitud de información, la propia solicitud podría ser una consulta de si el nodo 14 frontera VPN está asociado o no a cierta VPN, por ejemplo, recibida por la interconexión 12F de dominio. En tal caso, un mensaje de confirmación no comprenderá ninguna información, como tal, sino que transmitirá, implícitamente, información de esta VPN particular en ese nodo frontera VPN particular. Este es un ejemplo de un mecanismo de tipo “push” para distribuir información de dominio VPN.

La información de nodo de dominio puede ser recogida también con una temporización diferente. Una alternativa es recoger de manera continua o al menos regularmente dicha información en los nodos frontera con el fin de asegurar que la información disponible esté siempre actualizada. En estas realizaciones, la información es almacenada, preferentemente, en los nodos frontera o en cualquier otro nodo en el que pueda ser recuperada desde el nodo frontera, véase las realizaciones descritas más adelante. Otra alternativa es que la recogida de información sea desencadenada por algún evento. Este evento podría ser, por ejemplo, un mensaje de difusión desde un nodo frontera que indique que hay un cambio de algún tipo o, tal como se ha descrito anteriormente, una solicitud para encontrar una VPN particular. Si todos los nodos frontera tienen conocimiento acerca de qué nodos frontera están disponibles en el dominio, la información podría ser enviada también directamente a todos los nodos frontera, cuando ocurra un cambio tal como el indicado. En el caso de que la búsqueda de información sea desencadenada por una solicitud para encontrar una cierta VPN, la información recogida puede ser restringida a esa VPN e incluso, puede no ser almacenada necesariamente para un uso posterior.

La Fig. 2C ilustra una realización en la que la información de dominio VPN es recogida de manera centralizada. Hay provisto un almacenamiento 54 para almacenar toda la información 24 de dominio VPN proporcionada por los diferentes nodos 14 frontera. Cualquier funcionalidad que use dicha información de dominio VPN puede recuperar esta información desde el almacenamiento 54 central.

La Fig. 2D ilustra otra realización basada en una recogida centralizada de datos de dominio VPN. Aquí, una solicitud 23 u otra señal externa pueden inicializar la provisión de datos 24 VPN al almacenamiento 54. Esta solicitud 23 no tiene que provenir necesariamente del propio almacenamiento 54.

Como una alternativa para recoger la información de dominio VPN entre los nodos de dominio, la información de dominio VPN puede ser proporcionada, por el contrario, recuperando los datos desde un almacenamiento de datos. Por ejemplo, estos datos almacenados podrían ser el resultado de una recogida previa de datos según los procedimientos anteriores, o podrían ser proporcionados desde otros lugares.

En la realización descrita anteriormente, la provisión de datos dentro de un dominio es ejecutada por los nodos frontera o un nodo en asociación directa con los mismos. Dicha situación se ilustra también en la Fig. 3A. Aquí, se ilustra, con mayor detalle, un dominio 10A en un sistema multidominio. Los nodos 18 frontera son responsables del tráfico de datos hacia y desde otros dominios por medio de las conexiones 12A y 12B de datos. En esta realización particular, los nodos 18 frontera comprenden medios 41 para recoger la información de dominio VPN, en la forma de, por ejemplo, una funcionalidad de software en los procesadores de los nodos 18 frontera. La información de dominio VPN puede ser almacenada en un almacenamiento 54. Un nodo 43 de control de VPN para gestionar la información de dominio VPN con relación al dominio VPN, en su conjunto, es implementado, de esta manera, en esta realización particular, como una distribución de medios 41 locales en cada nodo 18 frontera.

En la Fig. 3B se ilustra otra realización particular. Aquí, los nodos 18 frontera todavía comprenden entidades 41 de funcionalidad implicadas con la información de dominio VPN. Sin embargo, un nodo 43 de control VPN distribuido comprende, en esta realización particular, medios 41 para proporcionar información de dominio VPN situada en o en conexión con los nodos 18 frontera y una base de datos 54 central. En la base de datos 54 central, se almacena la información VPN histórica y, preferentemente, también la información real actualizada.

En la Fig. 3C se ilustra todavía otra realización particular. Aquí, el nodo 43 de control VPN está centralizado y comprende los medios 41 para proporcionar la información de dominio VPN y la base de datos 54 central provista, básicamente, siempre en la misma ubicación. En esta realización particular, los nodos 18 frontera son usados meramente para gestionar las comunicaciones 45 entre el nodo de control de VPN y los dominios vecinos. Las funcionalidades en los nodos 18 frontera con respecto a la señalización de control asociada con el tráfico de datos real pueden ser utilizadas también para la señalización de mensajes de control en relación a la configuración de VPN

En la Fig. 3D, se ilustra una realización que tiene un nodo 43 de control VPN que está virtualmente separado de los nodos frontera en el sistema. En dicha realización, el nodo 43 de control VPN está conectado a los nodos de control de VPN en otros dominios, por medio de conexiones 47 dedicadas de señal de control VPN, creando una red de alto nivel en sí misma.

En una realización particular de la presente invención, la información de dominio VPN proporcionada puede ser transferida dentro del sistema, es decir, entre los diferentes dominios. Esto se ilustra en la Fig. 4. La primera etapa es la provisión de información VPN dentro de cada dominio. Esto se realiza mediante un nodo 43 de control VPN en cada dominio. Sin embargo, la configuración de los nodos 43 de control de VPN puede diferir entre los diferentes dominios. En la Fig. 4 se indica que el dominio 10A tiene un nodo 43 de control VPN, similar al ejemplo mostrado en la Fig. 3A, el dominio 10C tiene un nodo 43 de control VPN similar al ejemplo mostrado en la Fig. 3B y los dominios 10B, 10D y 10E tienen nodos 43 de control de VPN similares al ejemplo mostrado en la Fig. 3C. Según cada SLA que regula el tráfico entre los diferentes dominios, al menos una parte de la información de dominio VPN disponible en cada nodo 43 de control VPN es transferida, en esta realización, al nodo de control de VPN opuesto en los dominios vecinos. Las flechas

28 ilustran esta transferencia de información entre dominios. El SLA puede comprender acuerdos acerca de qué cantidad de la información disponible debería hacerse disponible para el dominio vecino. En un caso general, el nodo de control de VPN procesa la información VPN entre dominios en una información VPN compilada o procesada que es adecuada para ser reenviada a los dominios vecinos. Si los dominios están estrechamente relacionados, por ejemplo, pertenecen al mismo operador, el SLA podría implicar una transparencia total en el intercambio de información de dominio VPN. En otros casos, la información 28 procesada que es transferida entre los nodos 43 de control de VPN puede ser información VPN compilada, que revela sólo hechos muy básicos acerca de las VPNs de dominio individuales. La información mínima que debe ser enviada sobre las conexiones 12A-G entre dominios en la presente realización son las identidades de las VPN que están disponibles en algún lugar más allá del nodo frontera que envía la información.

La información 28 enviada en las conexiones 12A-G entre dominios causa una actualización de la situación de la información VPN disponible total en el nodo de control VPN receptor. Ahora, este nodo de control de VPN tiene también información, por ejemplo, de qué VPNs están disponibles a través de las conexiones entre dominios. Si hay disponible más información detallada, el nodo de control de VPN puede determinar también, por ejemplo las identidades de los nodos frontera en los que estas diferentes VPNs están disponibles, la calidad del servicio de VPN, etc. La información de VPN, conseguida de esta manera, es ahora una propiedad del dominio vecino y puede, si lo permite el SLA, ser usada para actividades en ese dominio. La información almacenada en el almacenamiento 54 del nodo 43 de control VPN podría ser idéntica a la información recibida desde el dominio vecino o una versión procesada de la misma, agregando, eliminando o modificando la información recibida. Por ejemplo, la información podría estar etiquetada con una indicación acerca de en qué dominio se originó.

Esta distribución de la información puede continuar en muchas etapas sucesivas, en algunos casos, aplicando modificaciones adicionales a la información antes de reenviarla a otro dominio, en analogía con la primera transferencia. Eventualmente, todos los nodos de control de VPN en toda la arquitectura 1 del proveedor VPN tienen al menos una versión procesada de toda la información de dominio VPN disponible en el sistema. En cada nodo de control de VPN, la información puede estar procesada según el SLA que es válido para la conexión asociada entre dominios a usar.

En una realización alternativa, la distribución de información entre los dominios puede ser realizada de una manera “broadcast push”. Entonces, la información de dominio VPN es enviada directamente a uno, a varios o a todos los otros nodos de control de VPN en los otros dominios en el sistema total, sin limitarse a los dominios vecinos. Esto significa que la información de dominio VPN no es reenviada en una cadena, tal como en la otra realización, sino que es difundida meramente a través del sistema. La disponibilidad de dicho reenvío directo de solicitud puede ser regulada por los SLAs de dominio.

El intercambio de información de dominio VPN puede ser realizado con una temporización diferente. Una alternativa es intercambiar, de manera continua o al menos regularmente, dicha información para asegurar que la información disponible esté siempre actualizada. En dichas realizaciones, la información está almacenada, preferentemente, en los nodos de control de VPN o en cualquier otro nodo, en el que pueda ser recuperada por el nodo de control de VPN. En otras palabras, esta alternativa es un mecanismo “push” típico para distribución de datos.

Otra alternativa es que el intercambio de información sea desencadenado por algún evento. Este evento podría ser, por ejemplo, que se ha producido un cambio de algún tipo en un dominio o, tal como se describe más adelante, se emite una solicitud para buscar una VPN particular. En otras palabras, esta alternativa puede ser descrita como un mecanismo “push” desencadenado para la distribución de datos.

En el caso en el que la información es intercambiada como resultado de un desencadenamiento por una solicitud para encontrar una VPN determinada, la información intercambiada puede estar restringida a esa VPN y puede incluso no ser almacenada necesariamente para su uso posterior. Este es un ejemplo de un mecanismo “pull” para la distribución de datos.

Ahora, considérese la conexión de un nuevo sitio 20' de cliente a un nodo 14' frontera, destinado a estar conectado a una VPN determinada. En una realización particular, la conexión iniciará un procedimiento "plug-and-play" que encontrará automáticamente la VPN apropiada y sugiere al menos cómo disponer la configuración VPN revisada. El nodo 43 de control identifica que un nuevo sitio 20' de cliente está conectado e investiga a qué VPN está destinado.

Cuando un nodo 43 de control VPN inicia una solicitud de conexión VPN, compara la VPN solicitada con la información almacenada acerca de las VPNs que están disponibles a través de sus conexiones entre dominios: Si hay una correspondencia, hay disponible información sobre la existencia de la correspondencia y, preferentemente, también sobre en qué dominio existe y a través de qué conexiones entre dominios es accesible la VPN. En una realización, el camino para llegar a un nodo frontera conectado a la VPN solicitada, si está disponible, es devuelto al nodo de control de VPN solicitante. En la Fig. 4, la VPN solicitada es la VPN 22A de la Fig. 1. El nodo 43 de control de VPN del dominio 10E tiene información acerca de qué VPN 22A está disponible a través del nodo 18:1 frontera, según dos caminos diferentes. Una alternativa para llegar a la VPN 22A es sobre una conexión 12D entre dominios, a través del dominio 10B y sobre la conexión 12A entre dominios. La VPN 22A está presente, entonces, dentro del dominio 10A. Otra alternativa para llegar a

la VPN 22A es sobre la conexión 12D entre dominios, a través del dominio 10B y sobre la conexión 12C entre dominios. Entonces, la VPN 22A está presente en el dominio 10C. Sin embargo, el nodo 43 de control VPN del dominio 10E tiene también información acerca de la VPN 22A a través de otro nodo 18 frontera. Aquí, la VPN 22A solicitada es accesible sobre la conexión 12E entre dominios, ya que la VPN 22A está disponible en el dominio 10C. Finalmente, la VPN 22A solicitada está disponible sobre la conexión 12G entre dominios, ya que la VPN 22A está disponible también en el dominio de 10D.

El nodo 43 de control de VPN tiene toda la información necesaria para encontrar la VPN solicitada. En este ejemplo, la ruta sobre la conexión 12E entre dominios parece más simple de usar, pero, por ejemplo, los niveles de calidad de servicio pueden cambiar dichas decisiones.

En esta realización particular, la información de dominio VPN proporcionada es propagada a todos los nodos 43 de control de VPN de todo el sistema 1. De esta manera, una solicitud de búsqueda de una VPN adecuada puede ser realizada directamente a un nodo 43 de control de VPN del dominio “local”. La provisión y el intercambio de información VPN pueden ser realizados, tal como se ha indicado anteriormente, de manera continua, regular o desencadenados por la propia solicitud.

Otra realización particular de la presente invención se ilustra en la Fig. 5. Aquí, la provisión de información de dominio VPN inicial es realizada justo como antes. En esta realización particular, sin embargo, la información de dominio VPN no es enviada a cualquier dominio vecino, incluso en forma procesada. Esto significa que los nodos 43 de control de VPN ahora tienen sólo información acerca de las VPNs de su propio dominio. Cuando el nodo 43 de control de VPN inicia una solicitud de conexión del nodo 43 de control de VPN de su propio dominio 10E, sólo tiene la información sobre las VPNs en el propio dominio disponible fácilmente en sus propias bases de datos. Sin embargo, el nodo 43 de control de VPN sabe a qué dominios está conectado y reenvía, por el contrario, la solicitud sobre la conexión 12A-G entre dominios a los dominios vecinos. Esto se ilustra mediante las flechas 32. Un nodo 43 de control de VPN que recibe dicha solicitud sobre una conexión entre dominios investiga en sus propias bases de datos para ver si hay algún dato de interés. Si no, se producirá un nuevo reenvío sobre una conexión entre dominios hasta que se consiga la información acerca de la VPN solicitada. A continuación, esta información será enviada de nuevo al nodo de control de VPN del dominio 10E original.

Esta forma de realización particular tiene la ventaja de que no todo el sistema 1 tiene que ser actualizado en todos los nodos 43 de control de VPN. Sin embargo, por el contrario, la búsqueda de la VPN será algo más complicada.

En una realización alternativa, la solicitud de conexión VPN es enviada directamente a uno, a varios o a todos los otros nodos de control de VPN en los otros dominios en el sistema total, sin limitarse a los dominios vecinos. Esto significa que la solicitud no es reenviada en una cadena, tal como en la otra realización, sino que es difundida, simplemente, a lo largo del sistema. La disponibilidad de dicho reenvío directo de solicitud puede ser regulada por los SLAs de dominio.

La Fig. 6A muestra un esquema de bloques de una realización particular de un nodo 43 de control de VPN, relativamente general, según la presente invención. El nodo 43 de control de VPN comprende medios 52 para proporcionar información de dominio VPN. Esta información puede ser proporcionada por otros nodos en el dominio, por medio de las conexiones 62. Una interfaz 40 de control principal de comunicación 40 está provista para la comunicación con otros dominios. Esta interfaz 40 puede ser dispuesta en combinación con las conexiones 62 intra-dominio. Hay provista una unidad 49 de correspondencia que investiga si una identidad de una VPN solicitada se corresponde con la información de dominio VPN. La solicitud de VPN puede ser recibida desde otro dominio, desde otro nodo del propio dominio o una solicitud de conexión VPN puede ser iniciada dentro del nodo de control de VPN. Una sección 44 externa de gestión de VPN es responsable de gestionar la configuración entre dominios VPN. Una sección 41 interna de gestión de VPN tiene funcionalidades para configurar las conexiones internas dentro del propio dominio.

La Fig. 6B ilustra un esquema de bloques de otra realización particular de un nodo 43 de control de VPN según la presente invención. La información de dominio VPN relacionada con el propio dominio es proporcionada por una sección 41 interna de gestión de VPN. La información interna de dominio de VPN está almacenada, en esta realización particular, en una memoria de datos 52. Esta información es proporcionada, en esta realización particular, tal como se ilustra por medio de la flecha 62, por medio de una comunicación con otros nodos dentro del dominio. En otras realizaciones, esta información puede ser obtenida de otras maneras. La información interna de dominio VPN es reenviada también a una base de datos 54 de información de VPN total en una sección 44 externa de gestión de VPN. La sección 41 interna de gestión de VPN incluye también una máquina 46 de configuración interna, que tiene funcionalidades para configurar las conexiones internas dentro del propio dominio. La sección 41 interna de gestión de VPN es provista de información interna de dominio VPN, así como de información desde la base de datos 54. Las comunicaciones relativas a asuntos internos de dominio son realizadas, de esta manera, sobre una conexión 42 entre la sección 41 interna de gestión de VPN y la sección 44 externa de gestión de VPN.

El nodo 43 de control de VPN tiene una interfaz 40 de control de comunicación de control principal con otros dominios sobre una conexión entre dominios. La información del dominio VPN desde otros dominios es recibida por medio de la interfaz 40, y una unidad 56 de procesamiento de entrada extrae información útil de los datos recibidos y almacena esta

información externa en una base de datos 58 de entradas. En esta base de datos 58 de entradas, se almacena también información adicional, tal como desde qué dominio fueron recibidos los datos externos. La base de datos 58 de entradas actualiza la base de datos 54 de información VPN total cuando sea apropiado. La sección 44 externa de gestión de VPN comprende también una máquina 60 externa de configuración, que tiene funcionalidades para configurar partes de las conexiones entre dominios que son relevantes para el dominio. Esta funcionalidad se describe más detalladamente más adelante.

La sección 44 externa de gestión de VPN proporciona también información a otros dominios. La información de dominio VPN, asociada con el propio dominio y/o con otros dominios, es extraída de la base de datos 54 y es proporcionada a una unidad 50 de procesamiento de datos de salida. La información recuperada es procesada según los SLAs asociados con los diferentes dominios vecinos y es almacenada en una base de datos 48 de salida. Los SLAs determinan, de esta manera, qué información se permite que sea propagada a los diferentes dominios vecinos. Los operadores de dominio que tienen una estrecha relación pueden permitir un intercambio más transparente de la información, mientras que los dominios pertenecientes a operadores no relacionados pueden aplicar un intercambio de información más restrictivo. La información relativa a las VPNs es transmitida en la interfaz 40, cuando sea adecuado.

Hay provista una unidad 49 de correspondencia que investiga si una identidad de una VPN solicitada se corresponde con la información de dominio VPN. La solicitud de VPN puede ser recibida desde otro dominio, desde otro nodo del propio dominio o una solicitud de conexión VPN puede ser iniciada dentro del propio nodo de control VPN. Cuando se consigue una correspondencia entre una VPN solicitada y la información VPN de los nodos de control de VPN, debe realizarse una re-configuración de una VPN entre dominios. La implementación puede ser realizada de muchas maneras diferentes, usando procedimientos típicos conocidos, tales como los conocidos en la técnica anterior. Más adelante, se describirá una realización ejemplar que supone que toda la información VPN es propagada a lo largo de todo el sistema, es decir, similar a lo que se ilustra en la Fig. 4.

Después de la correspondencia de la solicitud de conexión VPN para un usuario, se supone que todos los nodos de control de VPN en todos los dominios tienen una base de datos VPN que indica donde encontrar las VPNs en el sistema. En cada base de datos de dominios, hay información "siguiente-hop" para cada ID de VPN que no está actualmente en el dominio, que apunta al ID de dominio vecino en el que este ID de VPN puede ser encontrado. En el dominio vecino, hay una VPN ya configurada para este ID de VPN, o hay una nueva información "siguiente-hop" que indica dónde encontrar el ID de VPN. Las diferentes bases de datos en los dominios pueden ser interpretadas, de esta manera, como "tablas de enrutamiento VPN", que muestran cómo encontrar caminos a VPNs ya configuradas. Para cada información "siguiente-hop", puede haber diferentes reglas de política asociadas. Dependiendo de las reglas de política, el nodo de control de VPN en cada dominio puede elegir configurar conexiones VPN a uno o a varios de los dominios "siguiente-hop".

Un ejemplo, ilustrado en la Fig. 7, muestra cómo puede automatizarse la configuración de una VPN entre dominios. Un nuevo sitio 20' de cliente en el dominio 10E se conectará a la VPN 22A. Se supone que los túneles VPN son usados para las conexiones VPN, tanto en el interior de los dominios como entre dominios. Se realizan las etapas siguientes.

El nodo de control de VPN en el dominio de 10E recibe una solicitud, de alguna manera, desde el cliente, para conectarse a la VPN 22A. Debido a que la base de datos de VPN del dominio 10E muestra que la VPN 22A no está presente en el dominio 10E, el nodo de control de VPN en el dominio 10E no puede conectar directamente el sitio 20' de cliente a la VPN 22A en el interior del dominio 10E. Sin embargo, se encuentra una correspondencia entre la solicitud de conexión y la información de VPN proveniente de otros dominios. La base de datos muestra que la VPN 22A puede ser encontrada en "siguiente-hop" 10B, 10C y 10D, configurada como presente y ejecutándose en los dominios 10A, 10B y 10D.

El nodo de control de VPN en el dominio 10E elige configurar la VPN sólo a través de la "siguiente-hop" 10B. Establece un túnel 71 VPN para la VPN 22A desde el nodo 14' frontera, en el que está conectado el sitio 20' de cliente, al nodo 18:1 frontera, que está conectado al dominio 10B a través del enlace 12D. El nodo de control de VPN en el dominio 10E inicia una comunicación con el nodo de control de VPN en el dominio 10B y configura un túnel 72 VPN para la VPN 22A sobre el enlace 12D al nodo 18:02 frontera. Debido a que la VPN 22A no está presente en el dominio 10B, el nodo de control de VPN en el dominio 10B comprueba su base de datos de VPN y ve que esa VPN 22A puede ser encontrada en "siguiente-hop" 10A y 10C.

El nodo de control de VPN en el dominio 10B elige configurar la VPN sólo a través de la "siguiente-hop" 10A. Establece un túnel 73 de tránsito VPN para la VPN 22A desde el nodo 18:2 frontera, que está conectado al dominio 10B a través del enlace 12D, al nodo 18:3 de frontera, que está conectado al dominio 10A a través del enlace 12A. El nodo de control de VPN en el dominio 10B inicia una comunicación con el nodo de control en el dominio 10A y establece un túnel 74 VPN sobre el enlace 12A al nodo 18:4 frontera. Debido a que la VPN 22A está presente en el dominio 10A, el nodo de control en el dominio 10A puede establecer un túnel 75 interno desde el nodo frontera, que está conectado al dominio 10B a través del enlace 12 A, al nodo 18:5 frontera, que está conectado a la VPN 22A.

Después de cada etapa, las bases de datos de VPN actualizadas estarán disponibles para la siguiente ronda de recogida de información VPN.

Las etapas básicas de una realización de un procedimiento según la presente invención se ilustran en la Fig. 8. El procedimiento se inicia en la etapa 200. En la etapa 210, se inicia una solicitud de conexión. Esta solicitud se refiere a conectar un primer nodo frontera en un primer dominio a una VPN que no está disponible actualmente en el primer dominio. En la etapa 212, se recoge información de nodos de dominio. En la etapa 214, se busca una correspondencia entre una identidad de la primera VPN y las identidades VPN de la información de nodos recogida. En base a los resultados de la etapa de correspondencia, la primera VPN es configurada para comprender el primer nodo frontera, en la etapa 216. El procedimiento termina en la etapa 299.

Las realizaciones descritas anteriormente deben entenderse como unos pocos ejemplos ilustrativos de la presente invención. Las personas con conocimientos en la materia entenderán que pueden realizarse diversas modificaciones, combinaciones y cambios a las realizaciones, sin apartarse del alcance de la presente invención. En particular, las diferentes soluciones parciales en las diferentes realizaciones pueden ser combinadas en otras configuraciones, cuando sea técnicamente posible. En particular, puede aplicarse cualquier combinación información/solicitud y comunicación pull/push, entre dominios/intra-dominio, difusión/entre vecinos. Sin embargo, el alcance de la presente invención está definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para la configuración de una red privada virtual VPN-(22A-C) multi-dominio dentro de una red (1) de comunicaciones, teniendo la red (1) de comunicaciones al menos dos dominios (10A-E) interconectados entre sí, y en el que los clientes están conectados a las VPNs (22A-C) en los nodos (14; 14') frontera de al menos dos dominios (10A-E), que comprende las etapas de:

iniciar una solicitud de conexión para conectar un primer nodo (14') frontera en un primer dominio (10E) a una primera VPN (22A) no disponible actualmente en el primer dominio (10E);

proporcionar (24, 62) información de dominio VPN dentro de los al menos dos dominios;

comprendiendo la información de dominio VPN al menos un a identidad de VPN de las VPNs disponibles en el dominio respectivo;

establecer una correspondencia entre una identidad de la primera VPN (22A) y las identidades de VPN de un segundo dominio de los al menos dos dominios diferentes del primer dominio (10E); y

configurar la primera VPN (22A) para que comprenda el primer nodo (14') frontera, en base al resultado de la etapa de establecimiento de correspondencia.

2. Procedimiento según la reivindicación 1, **caracterizado porque** la etapa de establecimiento de correspondencia comprende, a su vez, las etapas de:

enviar (32) una solicitud de información acerca de la existencia de la primera VPN (22A) desde el primer dominio (10E) a un dominio (10B-D) contiguo; y

comparar la solicitud de información con información de dominios VPN proporcionada en un dominio diferente del primer dominio (10E).

3. Procedimiento según la reivindicación 1, **caracterizado porque** la etapa de establecimiento de correspondencia comprende, a su vez, las etapas de:

enviar (32) una solicitud de información acerca de la existencia de la primera VPN (22A) desde el primer dominio (10E) a uno, a varios o a todos los dominios (10B-D); y

comparar la solicitud de información con información de dominios VPN proporcionada en un dominio diferente del primer dominio (10E).

4. Procedimiento según la reivindicación 2 ó 3, **caracterizado porque** la etapa de establecimiento de correspondencia comprende, a su vez, las etapas de:

devolver un acuse de recibo al primer dominio (10E), si se encuentra una correspondencia.

5. P rocedimiento según la reivindicación 2 ó 4, **caracterizado porque** la etapa de establecimiento de correspondencia comprende además la etapa de:

reenviar la solicitud de información acerca de la existencia de la primera VPN a un dominio contiguo adicional si no se encuentra una correspondencia.

6. Procedimiento según una cualquiera de las reivindicaciones 2 a 5, **caracterizado porque** el acuse de recibo comprende además datos que representan al menos uno de entre:

una ID de dominio del dominio en el que la primera VPN (22A) está disponible;

una ID de nodo frontera del nodo (14) frontera en el que la primera VPN (22A) está disponible;

información acerca de qué dominios deben ser transitados para llegar al dominio en el que la primera VPN (22A) está disponible; y

enrutar información al nodo frontera en el que la primera VPN (22A) está disponible.

7. Procedimiento según la reivindicación 1, **caracterizado porque** la etapa de establecimiento de correspondencia comprende, a su vez, las etapas de:

procesar la información de dominio VPN en información VPN procesada que comprende al menos una identidad de VPN;

transferir (28) la información VPN procesada entre dominios contiguos;

comparar la identidad de la primera VPN (22A) con la información VPN procesada transferida.

8. Procedimiento según la reivindicación 1, **caracterizado porque** la etapa de establecimiento de correspondencia comprende, a su vez, las etapas de:

procesar la información de dominio VPN en información VPN procesada que comprende al menos una identidad de VPN;

transferir (28) la información VPN procesada a uno, a varios o a todos los dominios;

comparar la identidad de la primera VPN (22A) con la información VPN procesada transferida.

9. Procedimiento según la reivindicación 7 u 8, **caracterizado porque** la etapa de establecimiento de correspondencia comprende la etapa adicional de procesamiento adicional de la información VPN transferida antes de la etapa de comparación.

10. Procedimiento según la reivindicación 7 ó 9, **caracterizado porque** la información de VPN procesada a ser transferida a otros dominios comprende además procesar la información VPN procesada recibida desde los dominios contiguos.

11. Procedimiento según la reivindicación 10, **caracterizado porque** la etapa de procesamiento comprende la adición de información de tránsito en relación a la Información VPN procesada transferida de otros dominios o información derivada de la misma.

12. Procedimiento según cualquiera de las reivindicaciones 7 a 11, **caracterizado porque** la información VPN procesada comprende adicionalmente al menos uno de entre:

un ID de dominio de los dominios (10A-E) en los que las diferentes VPNs (22A-C) están disponibles;

un ID de nodo frontera de los nodos frontera (14, 14') en los que las diferentes VPNs (22A-C) están disponibles;

información acerca de qué dominios (10A-E) tienen que ser transitados para llegar al dominio (10A-E) en el que las diferentes VPNs (22A-C) están disponibles; y

enrutar información al nodo frontera (14, 14') en el que las diferentes VPNs (22A-C) están disponibles.

13. Procedimiento según cualquiera de las reivindicaciones 7 a 12, **caracterizado porque** la etapa de transferencia de información VPN procesada es realizada de manera regular.

14. Procedimiento según cualquiera de las reivindicaciones 7 a 12, **caracterizado porque** la etapa de transferencia de información VPN procesada es realizada como una respuesta a los cambios de información de dominio VPN.

15. Procedimiento según cualquiera de las reivindicaciones 7 o 14, **caracterizado porque** la etapa de transferencia de información VPN procesada es realizada como una respuesta de la solicitud de conexión.

16. Procedimiento según cualquiera de las reivindicaciones 1 a 15, **caracterizado porque** la información de dominio VPN comprende además identidades de cliente de los clientes conectados a los nodos frontera (14, 14') respectivos y la VPN (22A-C) asociada.

17. Procedimiento según cualquiera de las reivindicaciones 1 a 16, **caracterizado porque** la información de dominio VPN comprende además las propiedades de las VPNs (22A-C).

18. Procedimiento según la reivindicación 17, **caracterizado porque** las propiedades de las VPNs comprenden al menos uno de entre:

propiedades de calidad de del servicio;

propiedades de encriptación;

propiedades de transparencia de capa;

propiedades de tunelización; y

propiedades de la topología.

19. Procedimiento según cualquiera de las reivindicaciones 1 a 18, **caracterizado porque** la etapa de proporcionar

información de dominio VPN comprende, a su vez, recoger datos de dominio VPN desde los nodos frontera dentro de los mismos dominios.

20. Procedimiento según la reivindicación 19, **caracterizado por que** la recogida de datos de dominio VPN es realizada de manera centralizada en al menos un dominio.

21. Procedimiento según la reivindicación 19, **caracterizado por que** la recogida de datos de dominio VPN es realizada de manera distribuida en al menos un dominio.

22. Procedimiento según cualquiera de las reivindicaciones 19 a 21, **caracterizado porque** la recogida de datos de dominio VPN es realizada mediante un mecanismo “push”.

23. Procedimiento según cualquiera de las reivindicaciones 19 a 21, **caracterizado porque** la recogida de datos de dominio VPN es realizada mediante un mecanismo “pull”.

24. Red (1) de comunicaciones, que comprende:

al menos dos dominios (10A-E) de red, interconectados por conexiones (12A-G) entre los nodos frontera (18);

medios para operar redes privadas virtuales (VPNs) (22A-C) dentro la red (1) de comunicaciones;

estando los nodos frontera (14, 14') conectados por las VPNs (22A-C), en el que los sitios (20) de cliente de las VPNs (22A-C) están conectados en los nodos frontera (14, 14');

medios para iniciar una solicitud de conexión para conectar un primer nodo frontera (14') en un primer dominio (10E) a una primera VPN (22A) no disponible actualmente en el primer dominio (10E);

los nodos (43) de control de VPN en cada uno de los al menos dos dominios (10A-E) de red comprenden medios (41) para proporcionar información de dominio VPN;

la información de dominio VPN comprendiendo al menos una identidad de VPN de las VPNs disponibles en el dominio (10A-E);

medios para establecer una correspondencia entre una identidad de la primera VPN y las identidades VPN de un segundo dominio (10A-D) de los al menos dos dominios (10A-E) diferentes del primer dominio (10E); y

medios para configurar la primera VPN (22A) para comprender el primer nodo frontera (14'), en base al resultado de los medios de correspondencia.

25. Red de comunicaciones según la reivindicación 24, **caracterizada porque** el nodo (43) de control de VPN es un nodo centralizado en al menos un dominio (10A-E).

26. Red de comunicaciones, según la reivindicación 24 ó 25, **caracterizada porque** el nodo (43) de control de VPN es un nodo de distribución en al menos un dominio (10A-E).

27. Red de comunicaciones, según la reivindicación 26, **caracterizada porque** al menos una parte del nodo (43) de control de VPN está en conexión lógica con un nodo frontera (18), en el que la comunicación entre el nodo (43) de control de VPN distribuido y los dominios conectados a través del nodo frontera (18) tiene lugar a través del nodo frontera (18).

28. Red de comunicaciones según cualquiera de las reivindicaciones 24 a 27, **caracterizada porque** el nodo (43) de control de VPN comprende un almacenamiento (54) para información VPN.

29. Red de comunicaciones según cualquiera de las reivindicaciones 24 a 28, **caracterizada porque** los medios de establecimiento de correspondencia están distribuidos en todos los dominios (10A-E), cuyas partes distribuidas comprenden, a su vez:

medios de gestión de solicitudes para enviar y recibir solicitudes de información acerca de la existencia de una VPN particular hacia y desde un dominio contiguo; y

medios para comparar las solicitudes de información recibidas con información de dominio VNP de su propio dominio;

en el que los medios de gestión de solicitudes están dispuestos además para devolver un acuse de recibo si se encuentra una correspondencia.

30. Red de comunicaciones según cualquiera de las reivindicaciones 24 a 28, **caracterizada porque** los medios de

establecimiento de correspondencia están distribuidos en todos los dominios (10A-E), cuyas partes distribuidas comprenden, a su vez:

medios de gestión de solicitudes para enviar y recibir solicitudes de información acerca de la existencia de una VPN particular hacia o desde uno, varios o todos los dominios; y

medios para comparar las solicitudes de información recibidas con información de dominio VPN de su propio dominio;

en el que los medios de gestión de solicitudes está dispuesto adicionalmente para devolver un acuse de recibo si se encuentra una correspondencia.

31. Red de comunicaciones, según la reivindicación 29 ó 30, **caracterizada porque** los medios de gestión de solicitudes están dispuestos además para reenviar una solicitud de información a dominios contiguos adicionales si no se encuentra una correspondencia.

32. Red de comunicaciones según cualquiera de las reivindicaciones 24 a 28, **caracterizado porque** el nodo (43) de control VPN comprende además:

un primer procesador (50) para procesar la información de dominio VPN en información VPN procesada, conectado al almacenamiento (54); y

medios para transferir la información VPN procesada a otros dominios, conectados al primer procesador (50).

33. Red de comunicaciones, según la reivindicación 32, **caracterizada porque** el nodo (43) de control VPN comprende además:

medios para recibir la información VPN procesada desde otros dominios;

un segundo procesador (56) para el procesamiento de la información VPN procesada recibida, conectado a los medios de recepción y el almacenamiento (54);

en el que la información VPN procesada recibida puede ser almacenada en el almacenamiento (54).

34. Red de comunicaciones según cualquiera de las reivindicaciones 24 a 33, **caracterizada porque** los nodos (43) de control VPN en un dominio (10A-E) de red comprenden medios (41) para recoger información de dominio VPN desde los nodos frontera en el mismo dominio.

35. Nodo (43) de control VPN en un primer dominio de una red (1) de comunicaciones que tiene al menos dos dominios (10A-E) y redes privadas virtuales (VPNs) (22A-C) multi-dominio, estando conectados los clientes a las VPNs (22A-C) en los nodos frontera (14, 14') de los al menos dos dominios (10A-E), comprendiendo el nodo (43) de control VPN:

medios (52, 62) para proporcionar información de dominio VPN;

la información de dominio VPN comprendiendo al menos una identidad de VPN de las VPNs disponibles dentro del primer dominio; y

medios para el establecimiento de una correspondencia entre una identidad de una primera VPN solicitada y las identidades de VPN.

36. Nodo de control VPN según la reivindicación 35, **caracterizado porque** comprende además una máquina (46) de configuración para las conexiones de VPN dentro del primer dominio.

37. Nodo de control VPN según la reivindicación 35 ó 36, **caracterizado porque** comprende además una máquina (60) de configuración para conexiones VPN entre dominios que implican el primer dominio.

38. Nodo de control VPN según cualquiera de las reivindicaciones 35 a 37, **caracterizado porque** el nodo (43) de control es un nodo centralizado.

39. Nodo de control VPN según la reivindicación 38, **caracterizado por** medios para establecer comunicación con los nodos de control VPN en otros dominios a través de los nodos frontera.

40. Nodo de control VPN según la reivindicación 38, **caracterizado por** medios para establecer comunicación por medio de conexiones (47) de señal de control de VPN con nodos de control VPN en otros dominios.

41. Nodo de control VPN según cualquiera de las reivindicaciones 35 a 37, **caracterizado porque** el nodo (43) de

control es un nodo distribuido.

42. Nodo de control VPN según la reivindicación 41, **caracterizado porque** al menos una parte del nodo (43) de control distribuido está en conexión lógica con un nodo frontera (18), a través del cual tiene lugar una comunicación de datos a los dominios vecinos.

43. Nodo de control VPN según cualquiera de las reivindicaciones 35 a 42, **caracterizado porque** el nodo (43) de control comprende un almacenamiento (54) para información VPN.

44. Nodo de control VPN según la reivindicación 43, **caracterizado porque** el almacenamiento (54) para información VPN está centralizado.

45. Nodo de control VPN según la reivindicación 43, **caracterizado porque** el almacenamiento (54) para información VPN está distribuido.

46. Nodo de control VPN según cualquiera de las reivindicaciones 35 a 45, **caracterizado por** medios para comunicar información de dominio VPN hacia y desde otros dominios.

47. Nodo de control VPN según cualquiera de las reivindicaciones 35-45, **caracterizado por** medios para la recepción de una solicitud VPN, en el que los medios de establecimiento de correspondencia comprenden medios para enviar un acuse de recibo si se encuentra una correspondencia.

48. Nodo de control VPN según la reivindicación 47, **caracterizado por** medios para reenviar una solicitud VPN a otros dominios si los medios de establecimiento de correspondencia no encuentran una correspondencia.

49. Nodo de control VPN según cualquiera de las reivindicaciones 35 a 45, **caracterizado por** medios (41) para recoger información de dominio VPN desde los nodos frontera en el mismo dominio.

50. Procedimiento según la reivindicación 49, **caracterizado porque** los medios (41) para recoger información de dominio VPN están dispuestos para operar según un mecanismo “push”.

51. Procedimiento según la reivindicación 49 **caracterizado porque** los medios (41) para recoger información de dominio VPN están dispuestos para operar según un mecanismo “pull”.

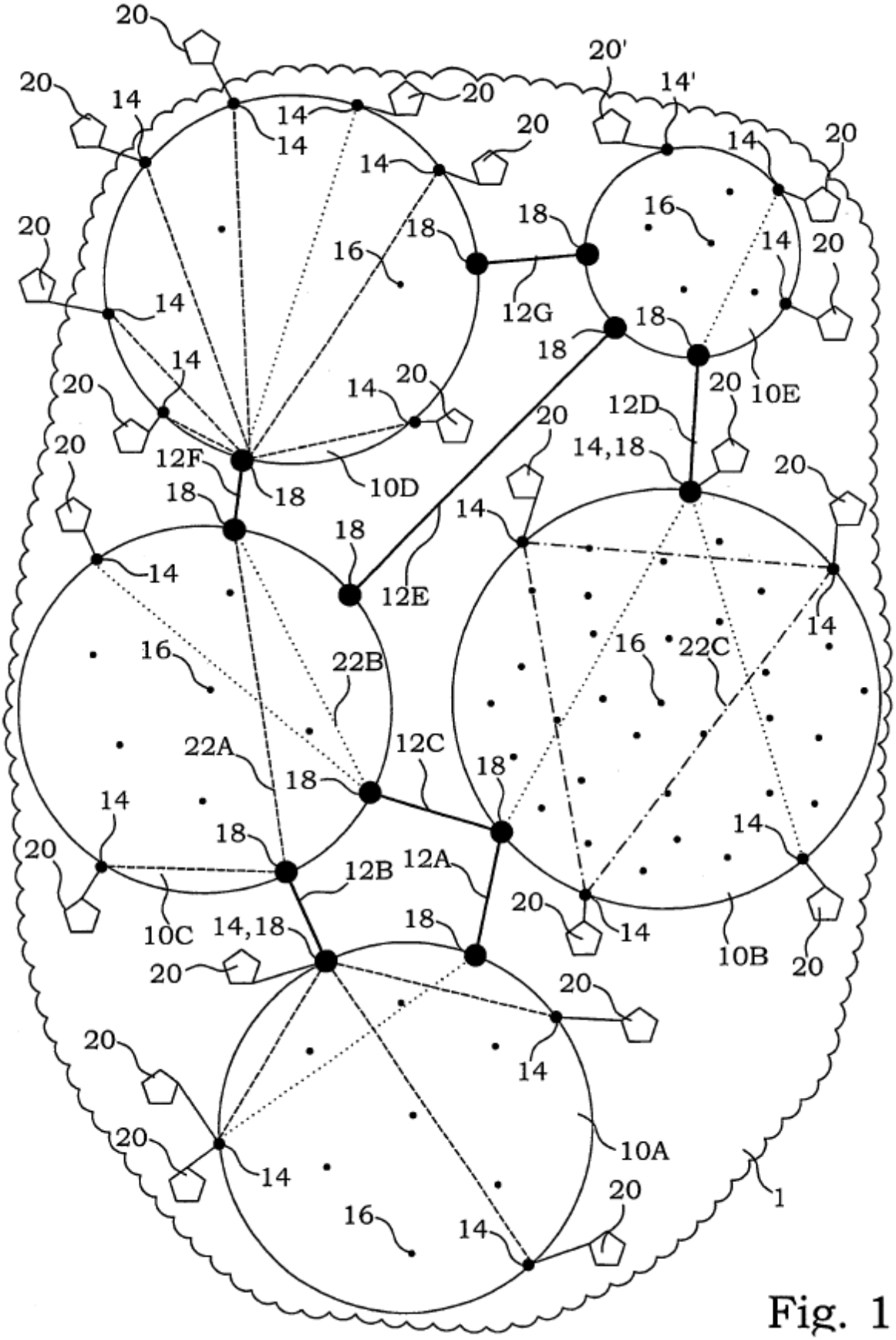
20
20'
14'
14
16
18
12G
10E
12D
14,18
12F
10D
12E
22B
22C
22A
12C
12B
12A
10C
10B
10A
1

Fig. 1

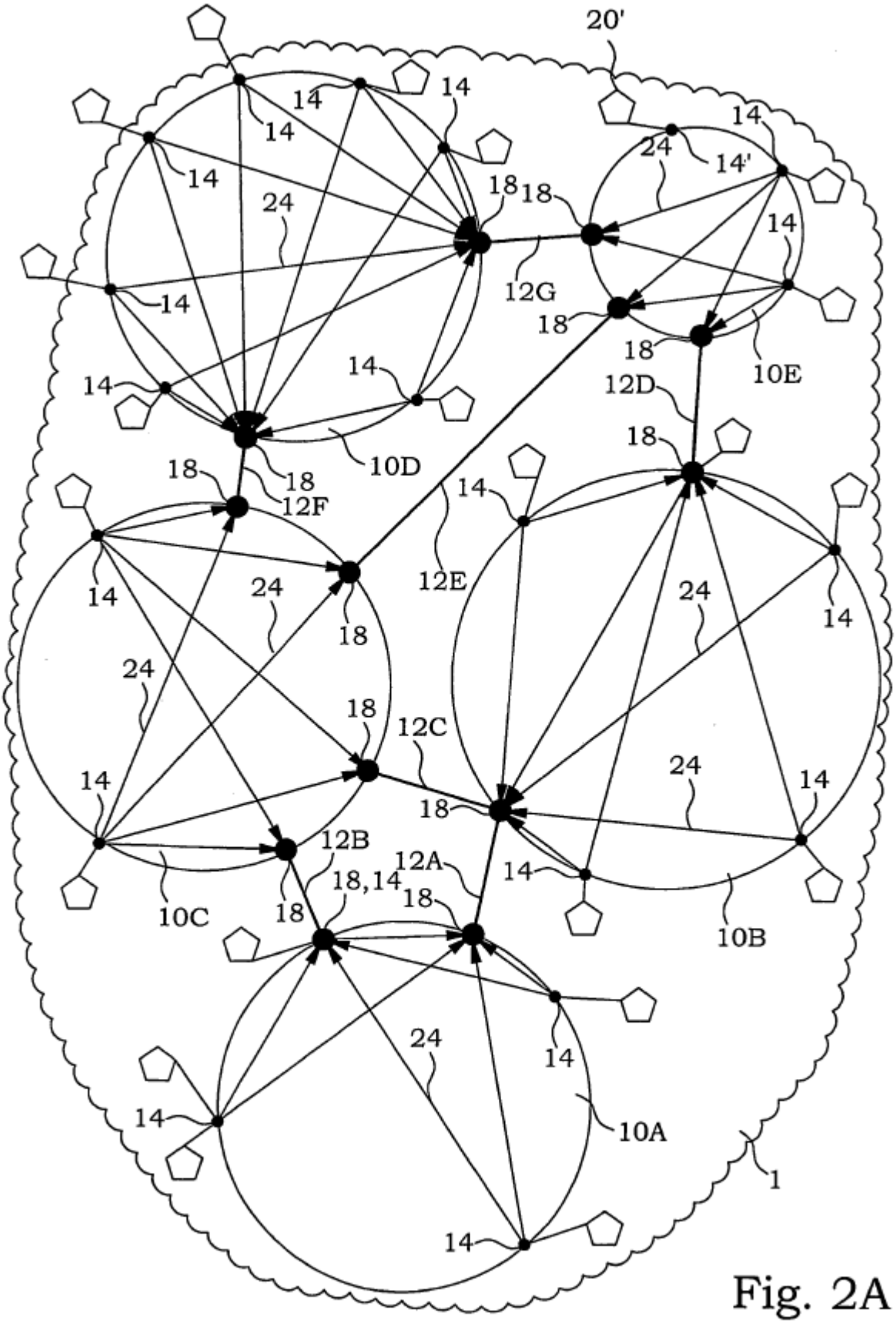
20'
14
14'
24
18
12G
12D
10E
10D
12F
12E
12C
12B
12A
18,14
10C
10B
10A
1

Fig. 2A

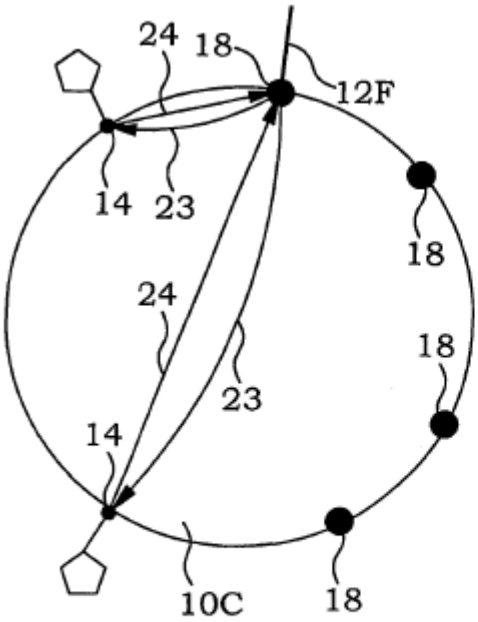

Fig. 2B

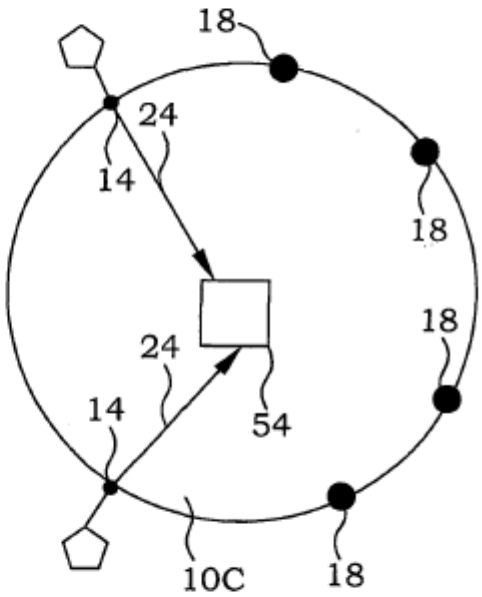

Fig. 2C

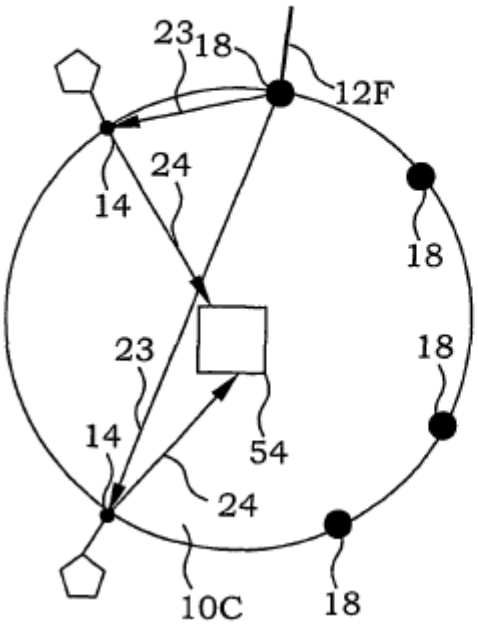

Fig. 2D

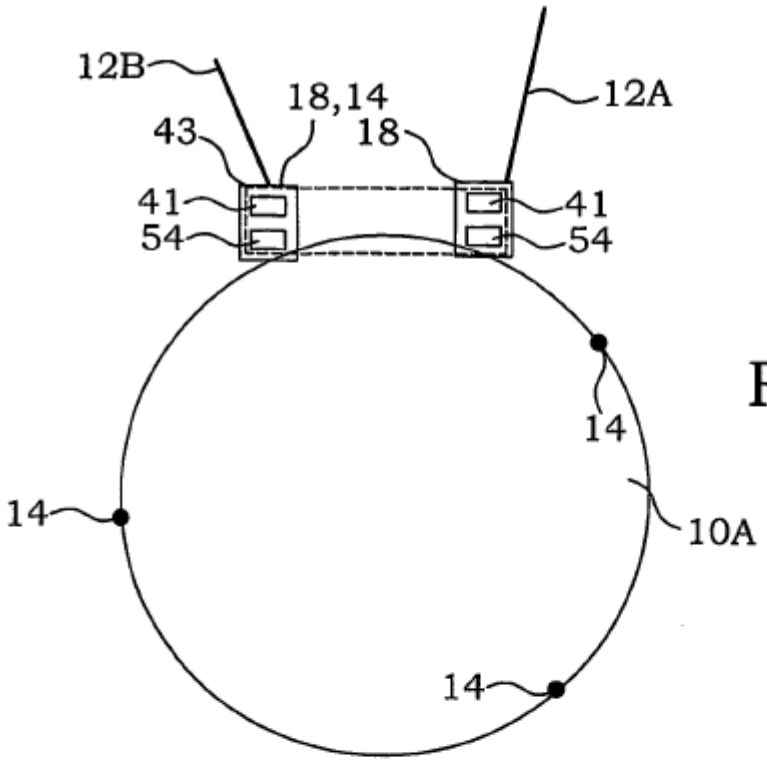
12B
18,14
12A
43
18
41
41
54
54
14
14
10A
14

Fig. 3A

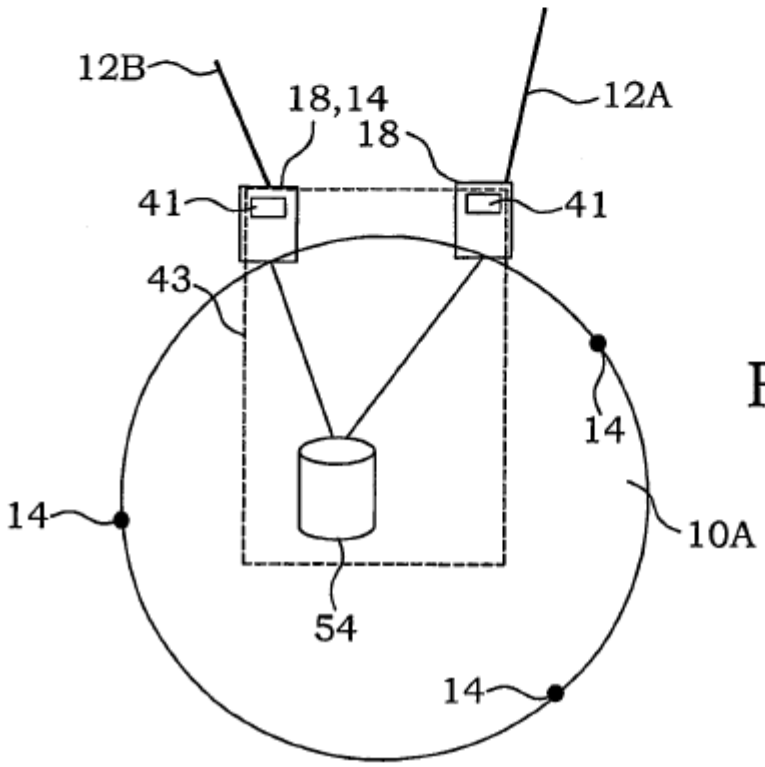
12B
18,14
12A
18
41
41
43
14
14
10A
54
14

Fig. 3B

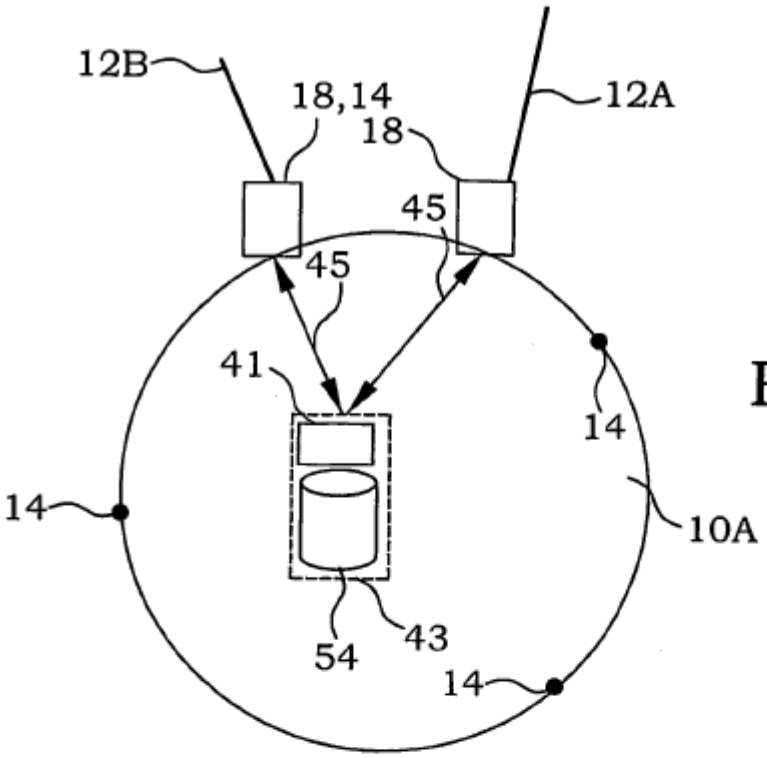
12B
18,14
18
12A
45
45
41
14
14
10A
54
43
14

Fig. 3C

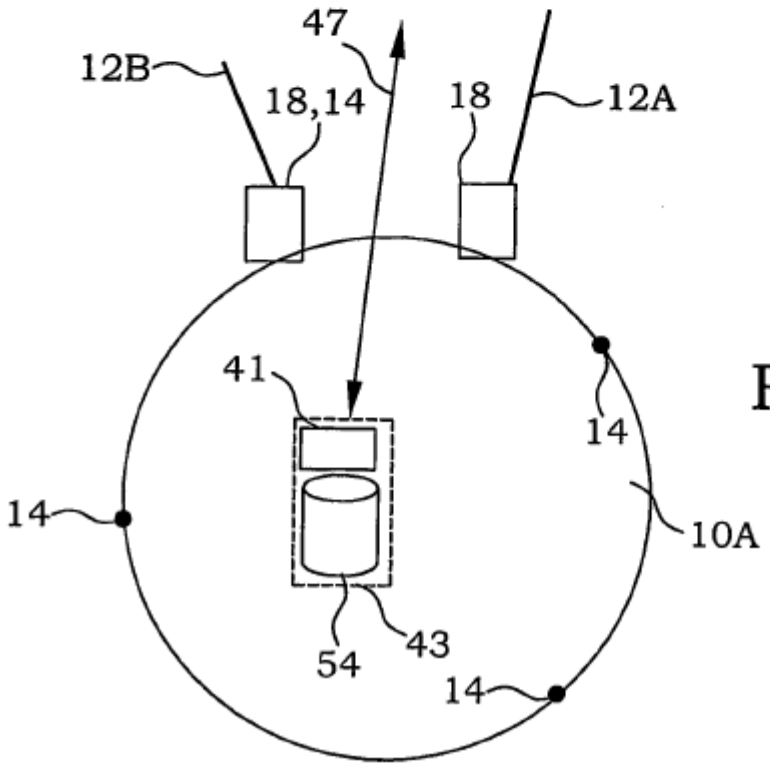
47
12B
18,14
18
12A
41
14
14
10A
54
43
14

Fig. 3D

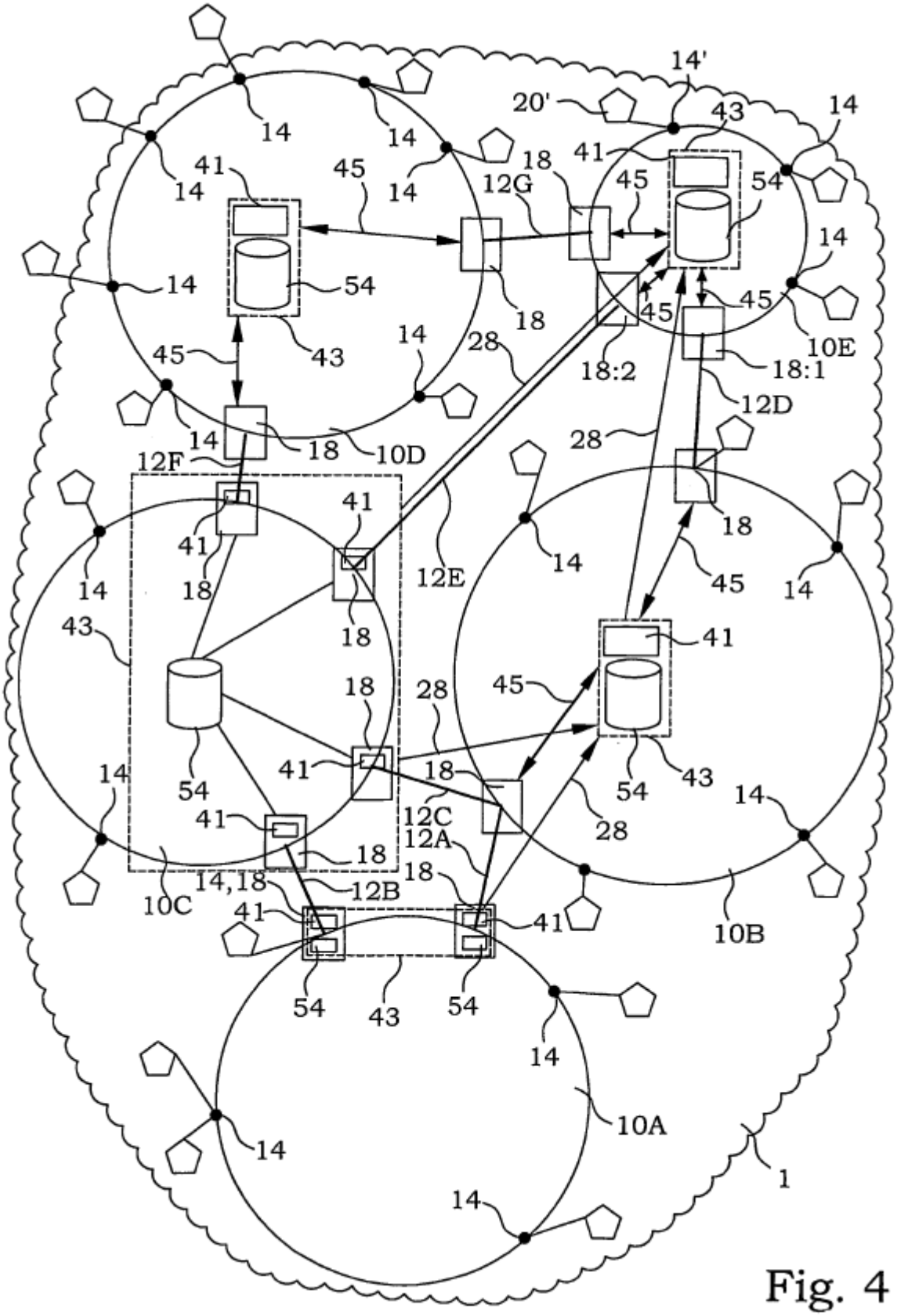
14'
20'
43
14
41
45
18
12G
54
14
28
18:2
18:1
12D
10E
12F
10D
12E
10C
14,18
12B
12A
12C
10B
10A
1

Fig. 4

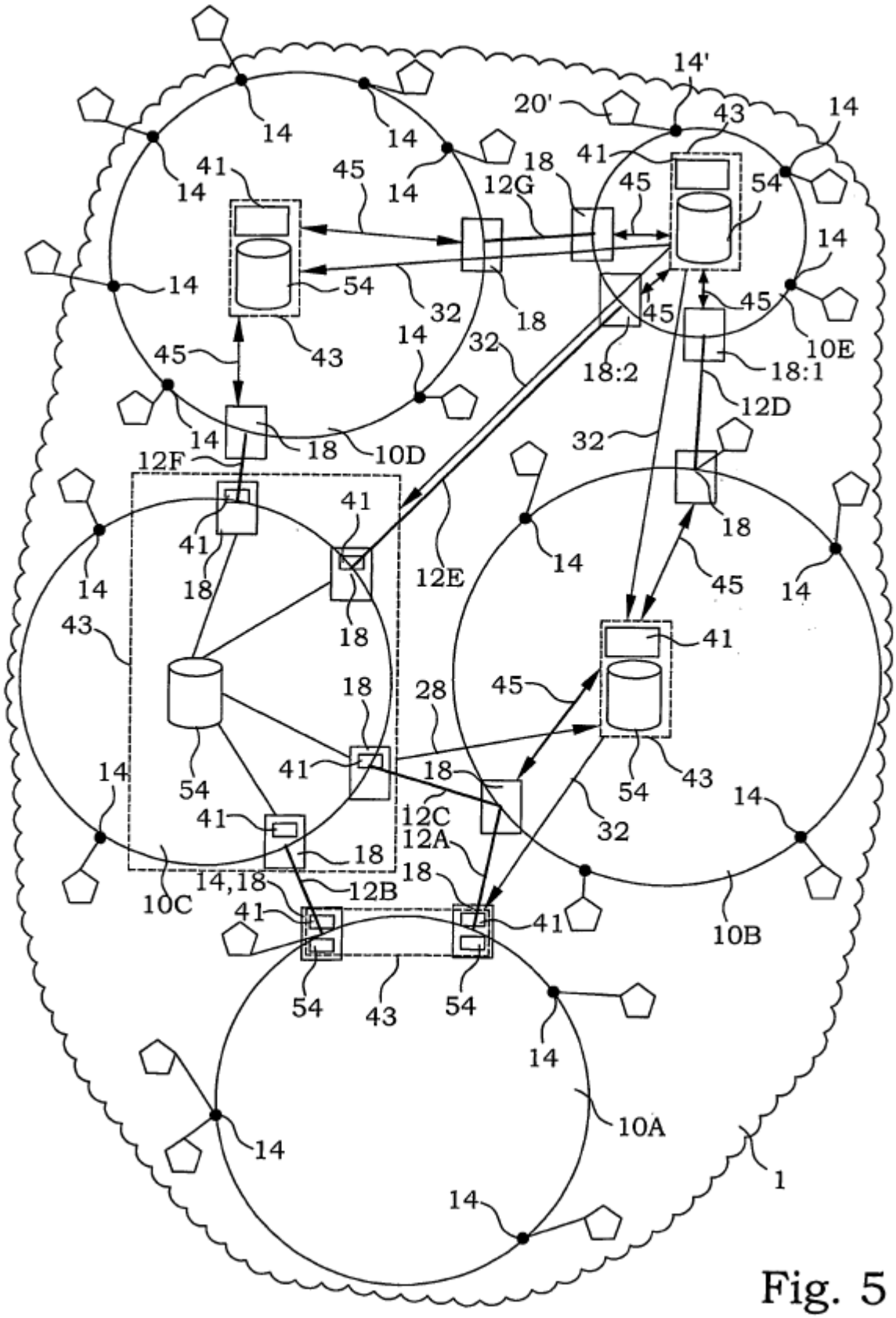
14'
20'
43
14
41
18
12G
45
54
32
12F
12E
12D
18:2
18:1
10E
10D
10C
10B
10A
12C
12A
12B
14,18
28
1

Fig. 5

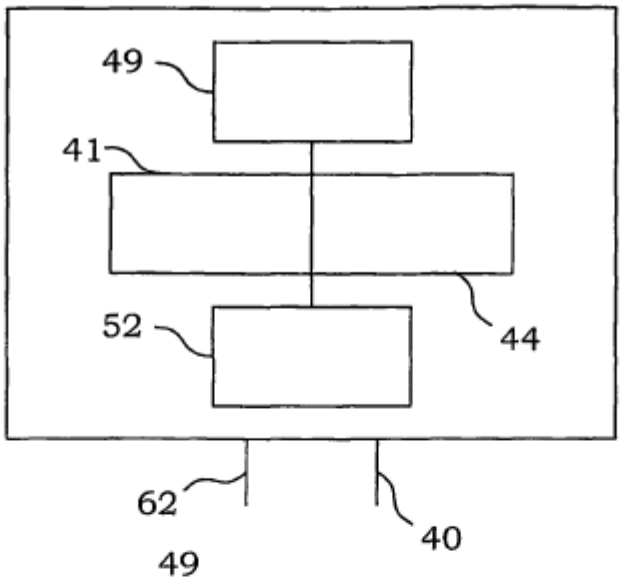

Fig. 6A

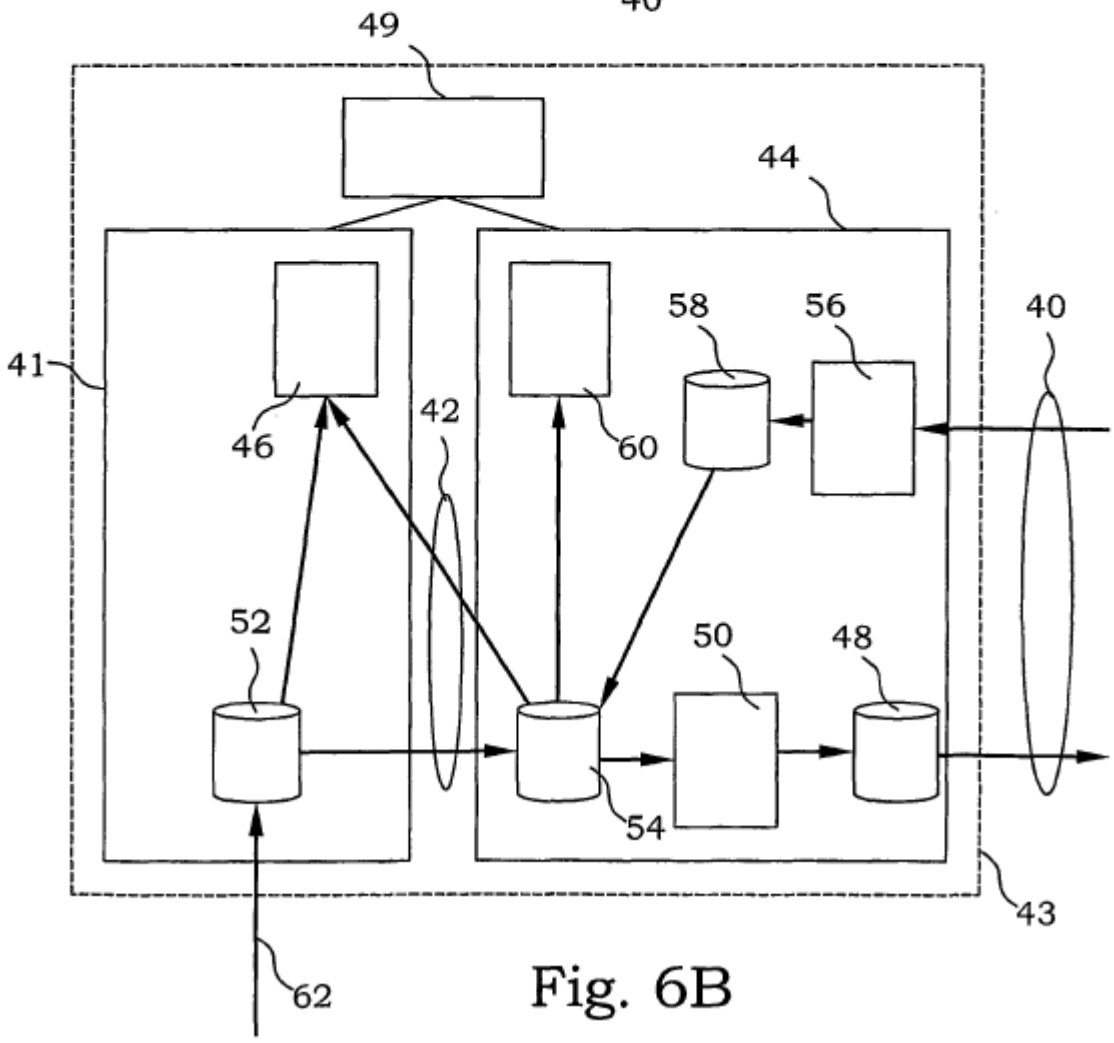

Fig. 6B

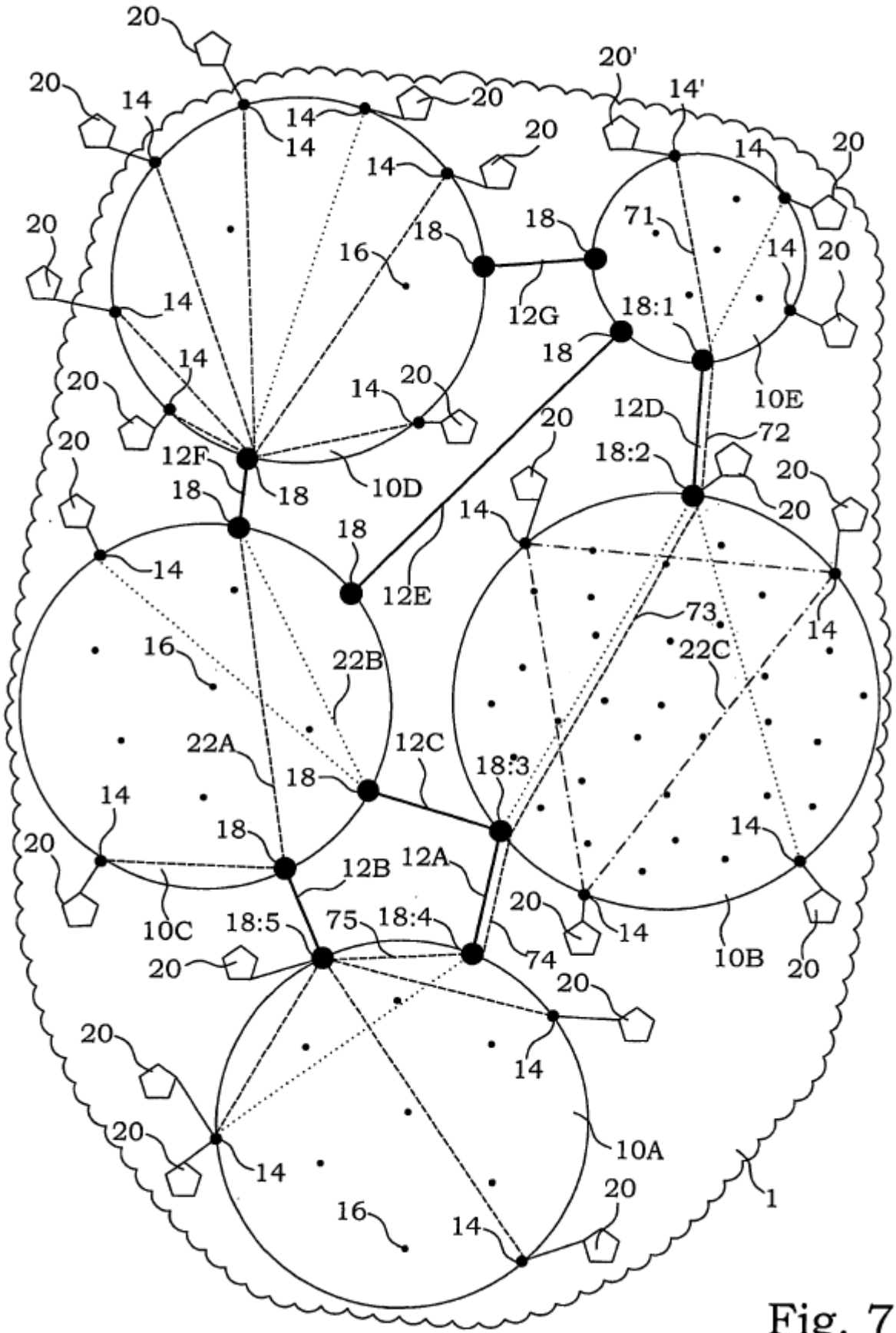
20
20'
14
14'
71
18
18:1
18:2
18:3
18:4
18:5
12A
12B
12C
12D
12E
12F
12G
10A
10B
10C
10D
10E
16
22A
22B
22C
72
73
74
75
1

Fig. 7

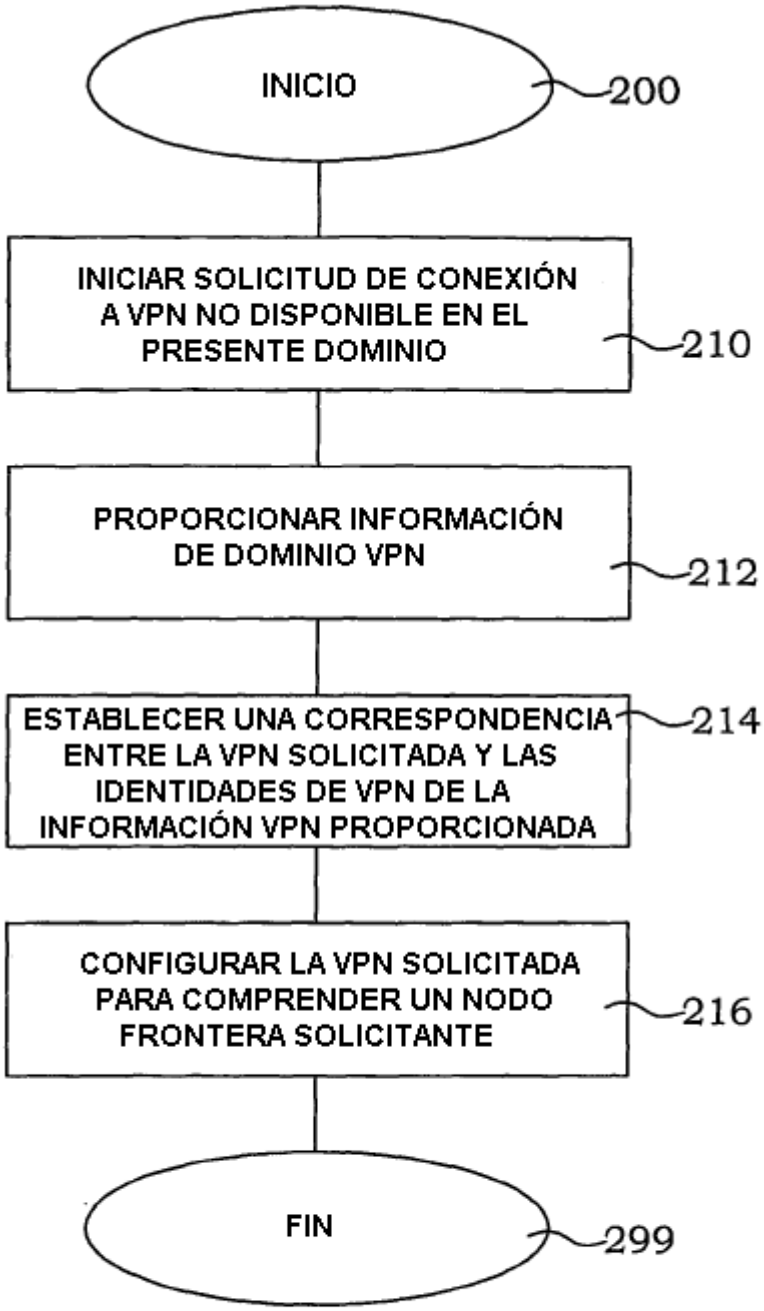
INICIO
200
INICIAR SOLICITUD DE CONEXIÓN A VPN NO DISPONIBLE EN EL PRESENTE DOMINIO
210
PROPORCIONAR INFORMACIÓN DE DOMINIO VPN
212
ESTABLECER UNA CORRESPONDENCIA ENTRE LA VPN SOLICITADA Y LAS IDENTIDADES DE VPN DE LA INFORMACIÓN VPN PROPORCIONADA
214
CONFIGURAR LA VPN SOLICITADA PARA COMPRENDER UN NODO FRONTERA SOLICITANTE
216
FIN
299

Fig. 8