República Federativa do Brasil
Ministério da Indústria, Comércio Exterior
e Serviços
Instituto Nacional da Propriedade Industrial

(11) **PI 0512909-5 B1**

(22) Data do Depósito: 23/06/2005

(45) Data de Concessão: 10/07/2018

(54) Título: MÉTODO PARA DETERMINAR UM TRAJETO DE CONEXÃO, E, ARRANJO DE DOMÍNIO DE REDE DE COMUNICAÇÃO

(51) Int.Cl.: H04L 29/06; H04L 12/46

(30) Prioridade Unionista: 30/06/2004 SE PCT/SE2004/001065

(73) Titular(es): TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

(72) Inventor(es): CHRISTOFER FLINTA; JAN-ERIK MÅNGS

"MÉTODO PARA DETERMINAR UM TRAJETO DE CONEXÃO, E, ARRANJO DE DOMÍNIO DE REDE DE COMUNICAÇÃO"

CAMPO TÉCNICO

A presente invenção relaciona-se em geral a redes privadas virtuais em sistemas de comunicação, e em particular à determinação de trajetos de conexão adequados para redes privadas virtuais em sistemas de comunicação de multi-domínio.

FUNDAMENTO

Uma Rede Privada Virtual (VPN) utiliza uma rede de comunicação pública ou privada para conduzir comunicações privadas. Tradicionalmente, uma companhia ou outro cliente que queria construir uma rede de área ampla tinha que prover suas próprias linhas dedicadas entre cada nó para prover a conectividade. Tais soluções são, porém, geralmente caras e inflexíveis. Durante os últimos anos, o conceito de VPNs evoluiu rapidamente. VPNs oferecem uma solução, onde uma rede de comunicação é compartilhada entre muitos clientes, mas onde a comunicação de cada cliente é virtualmente separada. Tecnologia de VPN é freqüentemente baseada na idéia de envelopamento. Envelopamento de rede envolve estabelecer e manter uma conexão de rede lógica. Nesta conexão, pacotes são encapsulados dentro de alguma outra base ou protocolo de portador. Eles são então transmitidos entre o cliente de VPN e servidor e eventualmente desencapsulados no lado de receptor. Autenticação e criptografia ajudam em prover segurança.

Uma tendência é que o número de nós de rede que formam uma VPN cresça rápido, que resulta em estruturas e topologia de rede complexas grandes. Isto é causado, parcialmente por causa do tráfego crescente em VPNs e parcialmente visto que as VPNs são pedidas para cobrir áreas geográficas cada vez maiores.

Redes de comunicação provendo VPNs tendo nós em todos os continentes estão presentes hoje. Porém, quanto mais nós e o mais tráfego é

para ser transmitido, mais complexa a configuração de VPNs se torna. Convencionalmente, uma VPN é criada conforme com um acordo entre uma operadora de rede e um cliente. O local dos nós, a qualidade de serviço e outras condições são acordadas e um programador na operadora estabelece a configuração manualmente ou consultando ferramentas de ajuda de configuração. Ao ter redes de comunicação cada vez mais complexas, tal configuração se torna mais complexa e demorada.

Ao configurar conexões atravessando através de vários domínios, há tipicamente vários trajetos de conexão alternativos. Informação de vários domínios então tem que ser coletada e compilada de uma maneira apropriada. Além disso, quando um cliente quer modificar sua VPN, o procedimento inteiro tem que ser repetido.

SUMÁRIO

Um problema geral de soluções da anterior-arte é assim que redes de comunicação provendo redes privadas virtuais tendo uma grande cobertura geográfica e/ou tendo grande tráfego se tornam muito complexas. Um problema adicional é que configuração de novas VPNs ou modificações de VPNs já existentes se tornam complexas e demoradas. Um problema adicional é que recursos de comunicação de operadoras de rede cobrindo áreas geográficas menores geralmente não podem ser utilizados para VPNs de área ampla. Ainda um problema adicional é que coleta e compilação de informação de VPN de domínios diferentes é ambos demorada e complexa.

Um objetivo geral da presente invenção é assim melhorar métodos para achar trajetos de conexão adequados de VPNs como também prover sistemas e arranjos implementando tais métodos. Um objetivo adicional da presente invenção é prover métodos para achar trajetos de conexão para VPNs utilizando mais de um domínio de rede. Outro objetivo adicional da presente invenção é prover métodos para achar trajetos de conexão para VPNs que são basicamente independentes na tecnologia de

09

VPN atual usada nos domínios diferentes. Ainda um objetivo adicional da presente invenção é prover um método habilitando configuração ótima ou quase ótima de uma VPN.

Os objetivos acima são alcançados por métodos e dispositivos de acordo com as reivindicações de patente inclusas. Em palavras gerais, informação sobre VPNs em uma rede de comunicação tendo dois domínios interconectados pelo menos é coletada em um primeiro domínio por um mecanismo de impulso. A informação sobre as VPNs inclui pelo menos ID de domínio de domínios nos quais as VPNs diferentes estão atualmente disponíveis. Informação de VPN de domínio é coletada em cada domínio. A provisão de informação de VPN de domínio pode ser executada de modos diferentes, por exemplo coleta de dados de uma maneira centralizada ou distribuída, ou recuperando dados armazenados. Um nó de controle de VPN distribuído está, em concretizações particulares, localizado a nós de fronteira de um domínio. A informação de VPN de domínio é, em concretizações particulares, coletada dos nós de borda do domínio. Isto pode ser executado extraindo passivamente informação radiodifundida dos nós de borda, pedindo informação de VPN de domínio dos nós de borda ou uma combinação disso. A coleta pode ser ativada por um evento externo, tal como uma mudança em informação de VPN. A informação de VPN de domínio é espalhada para outros domínios, preferivelmente sob constrições postas por SLAs entre operadoras de domínio. Em uma incorporação preferida, a informação de VPN de domínio é espalhada para domínios adjacentes, que modifica sua própria informação de VPN de domínio e por esse meio também remete a informação de VPN recebida para domínios adjacentes adicionais. Em tal maneira em cascata, a informação de VPN de domínio disponível inteira é espalhada para todos os domínios. A informação coletada sobre as VPNs é avaliada a fim de achar trajetos de conexão adequados. Em uma concretização, uma avaliação de acordo com uma medida de qualidade é

executada e um trajeto de conexão ótimo é selecionado por conseguinte. Em uma concretização preferida, uma avaliação é executada e todos os trajetos de conexão excedendo um limiar predeterminado são configurados. Uma avaliação estatística da necessidade prática pode ser então executada depois de algum tempo de operação de inicial.

Uma vantagem importante com a presente invenção é que ela provê uma plataforma simples e estável na qual os operadoras de domínios diferentes podem cooperar. A informação de VPN de domínio é feita disponível para apoiar configuração de VPN essencialmente em todos os domínios de um sistema de multi-domínio. A abordagem inventiva provê um meio para assegurar que um trajeto de conexão ótimo ou quase ótimo seja possível de achar de acordo com condições de domínio presentes. A invenção é particularmente bem adequada para ser implementada em redes de comunicação tendo uma configuração e topologia relativamente estáveis.

BREVE DESCRIÇÃO DOS DESENHOS

A invenção, junto com objetivos adicionais e vantagens dela, pode ser entendida melhor fazendo referência à descrição seguinte tomada junto com os desenhos acompanhantes, caracterizado pelo fato de que:

Figura 1 é uma ilustração esquemática de uma rede de comunicação de multi-domínio provendo redes privadas virtuais;

Figura 2A é uma ilustração esquemática de coleta de informação de VPN de acordo com uma concretização da presente invenção;

Figuras 2B-D são ilustrações esquemáticas de coleta de informação de VPN de acordo com outras concretizações da presente invenção;

Figuras 3A-D são concretizações de acordo com a presente invenção de configurações de nó de controle de VPN dentro de um domínio;

Figura 4 é uma ilustração esquemática de remessa de informação de VPN e pedidos de conexão de acordo com uma concretização

da presente invenção;

Figura 5 é uma ilustração esquemática de uma situação de malha contínua em remessa de informação de VPN;

Figura 6A é um esquema de bloco de uma concretização de um nó de controle de VPN geral de acordo com a presente invenção;

Figura 6B é um esquema de bloco de outra concretização de um nó de controle de VPN de acordo com a presente invenção;

Figura 7 é uma ilustração esquemática de configuração de VPN de acordo com uma concretização da presente invenção; e

Figura 8 é um fluxograma ilustrando as etapas principais de uma concretização de um método de acordo com a presente invenção.

DESCRIÇÃO DETALHADA

Uma concretização de uma arquitetura de provedor de VPN geral 1 é ilustrada na Figura 1. Nesta Arquitetura de Provedor de VPN, há cinco Domínios de Provedor de VPN 10A-E presentes, que estão conectados um ao outro por conexões de dados de inter-domínio 12A-G. Uma operadora pode controlar um ou mais destes domínios 10A-E, ou eles podem todos ser controlados por operadoras separadas. A relação entre os domínios 10A-E, isto é, o controle das conexões de dados de inter-domínio 12A-G é tipicamente regulada de acordo com acordos entre as operadoras envolvidas, por exemplo um Acordo de Nível de Serviço de VPN (SLA). Cada domínio de provedor de VPN 10A inclui nós de borda de VPN 14 e nós de núcleo 16, que podem ser cientes de VPN ou não cientes de VPN, de quais só alguns são providos com números de referência. Os nós de borda de VPN 14 são nós pelos quais locais de cliente 20 de clientes diferentes são conectados a VPNs diferentes na arquitetura 1. Nós não cientes de VPN 16 são apenas nós intermediários dentro de um domínio e só são usados para remeter mensagens e dados entre nós de borda de VPN 14. Os clientes são não cientes de quais nós não cientes de VPN que são usados para a comunicação. O único assunto

12

importante é o nó de borda de VPN 14 de começo e fim. Uma VPN conectada em um domínio pode assim ser representada por uma linha direta entre nós de borda de VPN 14, até mesmo se a comunicação atual puder acontecer por um ou vários nós não cientes de VPN 16. Na parte restante da presente exposição, a existência de nós não cientes de VPN será em geral negligenciada, como as etapas processuais básicas de acordo com a presente invenção não são diretamente dependentes da existência de quaisquer nós não cientes de VPN 16 ou não. Na implementação prática, é, porém, provável que nós não cientes de VPN 16 sejam usados para prover a conectividade atual.

Os domínios de provedor de VPN 10A-E estão conectados em um plano de dados por nós de borda de VPN 18, isto é, as conexões de dados de inter-domínio 12A-G começam e terminam em um nó de borda de VPN 18. O nó de borda de VPN 18 pode ou não ao mesmo tempo também atuar como um nó de borda de VPN 14. Um local de cliente 20 está conectado a um dos nós de borda de VPN 14. Locais de cliente 20 do mesmo cliente podem então ser conectados pelos domínios de provedor de VPN 10A-E por uma VPN 22A-C. Um cliente pode ter locais de cliente 20 conectados a VPNs 22A-C diferentes. Também, mais de um local de cliente 20 pode ser conectado ao mesmo nó de borda de VPN 14, mas será não ciente da existência do outro local de cliente 20 como também da VPN à qual o outro local de cliente 20 está conectado.

Na presente concretização, três VPNs 22A-C são ilustradas. Porém, qualquer um qualificado na arte percebe que o número de VPNs em um sistema real é tipicamente muito mais alto. Uma primeira VPN 22A, ilustrada por linhas interrompidas, está estendida através de três domínios 10A, 10C, 10D e conecta locais de cliente 20 em todos destes domínios. Uma segunda VPN 22B, ilustrada por linhas pontilhadas, está estendida através de todos os domínios 10A-E da presente concretização. Finalmente, uma terceira VPN 22C, ilustrada por uma linha de traço-ponto, conecta locais de cliente 20

só dentro do domínio 10B. Cada local de cliente 20 está não ciente da existência de locais de cliente 20 de outros clientes como também da existência de quaisquer VPNs, exceto a na qual está conectado. De tal maneira, o caráter de privacidade das VPNs é preservado, embora todas elas compartilhem os mesmos recursos de comunicação básicos. Este é o cenário no qual a presente invenção opera preferivelmente.

Na presente exposição, conexões diferentes são discutidas - inter-domínio, intra-domínio, conexões de plano de usuário, conexões de plano de controle, conexões de controle cobertas, conexões entre nós e terminais de usuário, etc. É assumido ao longo da descrição inteira que estas conexões podem ser de qualquer tipo. A idéia básica da presente invenção não é dependente da tecnologia de conexão atual. Isto significa que ambas as tecnologias por fios e sem fios podem ser usadas para quaisquer destas conexões. Em particular, relativo ao uso de conexões sem fios, os terminais de usuário podem ser moveis relativos aos nós de borda. Os nós dentro de um domínio podem ser móveis relativos aos outros nós. Até mesmo os domínios podem ser moveis relativos um ao outro.

Agora, considere que um novo local de cliente 20' está conectado a um nó de borda de VPN 14' em domínio 10E. Se o local de cliente 20' quiser ser conectado à VPN 22B, os procedimentos são provavelmente relativamente simples, desde que a VPN 22B já está presente dentro de domínio 10E. Procedimentos de reconfiguração de VPN manuais ou automáticos de acordo com arte anterior podem ser empregados, como também mistura entre eles. Porém, se o novo local de cliente 20' quiser se conectar à VPN 22A ou 22C, a situação se torna mais difícil. Na arte anterior, não há nenhum procedimento de configuração de VPN de inter-domínio geral.

Uma idéia básica da presente invenção relaciona-se à provisão de informação de VPN de domínio, incluindo identidade de VPN de VPNs

14

disponíveis no domínio respectivo.

Primeiro, alguns exemplos são descritos, ilustrando como informação de domínio pode ser coletada. Isto é feito em conexão às Figuras 2A-3D. As idéias inventivas principais então seguem.

Figura 2A ilustra uma concretização de uma fase inicial de prover informação de VPN de domínio. Cada nó de borda de VPN 14 armazenou informação refletindo sua própria configuração de VPN presente considerando pelo menos quais VPNs que conectaram locais de cliente naquele nó de borda de VPN 14 particular. Em concretizações particulares, o nó de borda de VPN 14 também tem informação sobre quais clientes que estão conectados ao nó de borda de VPN 14 e associações entre as VPNs presentes e locais de cliente 20. Em algumas concretizações, informação, tal como espaço de endereço de VPN e tipo de endereço (local ou global), qualidade de VPN de classes de serviço, especificadas por requisitos tais como largura de banda, atraso e instabilidade e/ou instalação de VPN, isto é, uso de envelopes ou filtros, é provido. Também informação tais como propriedades de criptografia, propriedades de camada de transparência, propriedades de envelopamento e propriedades de topologia pode ser incluída. Além disso, os nós de borda de VPN 18 armazenaram informação sobre a identidade do domínio de provedor de VPN ao qual pertencem.

De acordo com uma concretização da presente invenção, a informação de VPN de domínio armazenada em cada nó de borda de VPN 14, ou pelo menos partes dela, é coletada por cada nó de fronteira 18 no mesmo domínio 10A-E. Isto está visualizado na Figura 2A como setas, das quais algumas são providas com número de referência 24. De tal modo, a informação de nó de domínio coletivo para o próprio domínio está disponível em cada nó de borda de VPN 18 de cada domínio 10A-E. Uma alternativa para a comunicação é usar um protocolo de comunicação semelhante a BGP (Protocolo de Portal de Borda), espalhando a informação toda através do

domínio sem qualquer conhecimento particular sobre onde é a necessidade por informação. Os nós de borda podem então colher toda a informação necessária. Isto é um exemplo de um mecanismo de impulso para distribuir informação de VPN de domínio.

Figura 2B ilustra outra concretização para prover informação de VPN de domínio, agora concentrada a um domínio 10C. Se os nós de borda de VPN 18 armazenaram informação sobre quais nós de borda 14 que estão presentes no mesmo domínio 10C, o nó de borda de VPN 18 pode simplesmente pedir 23 qualquer nó de borda de VPN 14 para retornar sua informação de nó de domínio 24. Na forma mais simples de pedir informação, o próprio pedido poderia ser uma pergunta se o nó de borda de VPN 14 está associado a uma certa VPN ou não, por exemplo recebida pela interconexão de domínio 12F. Uma mensagem de reconhecimento em tal caso não incluirá qualquer informação tal como, mas transferirá implicitamente informação desta VPN particular àquele nó de borda de VPN particular. Isto é um exemplo de um mecanismo de impulso para distribuir informação de VPN de domínio.

A informação de nó de domínio também pode ser coletada com temporização diferente. Uma alternativa é coletar continuamente ou pelo menos regularmente tal informação para os nós de borda a fim de assegurar que a informação disponível sempre esteja atualizada. Em tais concretizações, a informação é preferivelmente armazenada nos nós de borda ou em qualquer outro nó, onde seja recuperável do nó de borda, veja concretizações descritas ademais abaixo. Outra alternativa é que a coleta de informação seja ativada por algum evento. Este evento poderia, por exemplo, ser uma mensagem de radiodifusão de um nó de borda que há uma mudança de algum tipo ou, como sendo descrito acima, um pedido para achar uma VPN particular. Se todos os nós de borda tiverem conhecimento sobre quais nós de borda que estão disponíveis no domínio, a informação também poderia ser enviada

diretamente para todos os nós de borda quando uma tal mudança ocorre. No caso que a informação é pesquisada como ativada por um pedido para achar uma certa VPN, a informação coletada pode ser restringida àquela VPN e pode até mesmo não necessariamente ser armazenada para uso posterior.

Figura 2C ilustra uma concretização, onde a informação de VPN de domínio é coletada de uma maneira centralizada. Um armazenamento 54 é provido para armazenar todo a informação de VPN de domínio 24 provida pelos nós de borda 14 diferentes. Qualquer funcionalidade usando tal informação de VPN de domínio pode recuperar esta informação do armazenamento central 54.

Figura 2D ilustra outra concretização baseada em uma coleta centralizada de dados de VPN de domínio. Aqui, um pedido 23 ou outro sinal externo pode iniciar a provisão de dados de VPN 24 para o armazenamento 54. Este pedido 23 não tem necessariamente que vir do próprio armazenamento 54.

Como uma alternativa a coletar informação de VPN de domínio entre os nós de domínio, a informação de VPN de domínio pode ao invés ser provida recuperando dados de um armazenamento de dados. Estes dados armazenados poderiam por exemplo ser o resultado de uma coleta prévia de dados de acordo com os procedimentos acima, ou poderiam ser providos de qualquer outro lugar.

Na concretização previamente descrita, a provisão de dados dentro de um domínio é executada pelos nós de borda ou um nó em associação direta com ele. Tal situação também é ilustrada na Figura 3A. Aqui, um domínio 10A em um sistema de multi-domínio é ilustrado em mais detalhes. Os nós de borda 18 são responsáveis pelo tráfego de dados e de outros domínios pelas conexões de dados 12A e 12B. Os nós de borda 18 incluem, nesta concretização particular, meio 41 para coletar informação de VPN de domínio, na forma de por exemplo, funcionalidade de software nos

processadores do nó de fronteira 18. A informação de VPN de domínio pode ser armazenada em um armazenamento 54. Um nó de controle de VPN 43 para operar informação de VPN de domínio relativa ao domínio como um todo é assim nesta concretização particular implementado como uma distribuição de meio local 41 em todo nó de fronteira 18.

Na Figura 3B, outra concretização particular é ilustrada. Aqui, os nós de borda 18 ainda incluem entidades de funcionalidade 41 envolvidas com informação de VPN de domínio. Porém, um nó de controle de VPN distribuído 43 inclui nesta concretização particular meio 41 para prover informação de VPN de domínio situado ou em conexão com os nós de borda 18 e um banco de dados central 54. No banco de dados central 54, a informação de VPN atualizada real e preferivelmente também histórica é armazenada.

Na Figura 3C, ainda outra concretização particular é ilustrada. Aqui, o nó de controle de VPN 43 é centralizado e inclui o meio 41 para prover informação de VPN de domínio e o banco de dados central 54 provido basicamente no mesmo local. Os nós de borda 18 são nesta concretização particular meramente usados para operar comunicações 45 entre o nó de controle de VPN e domínios vizinhos. Funcionalidades nos nós de borda 18 relativas à sinalização de controle associada com o tráfego de dados atual podem de tal modo serem utilizadas também para sinalizar mensagens de controle relativas à configuração de VPN.

Na Figura 3D, uma concretização tendo um nó de controle de VPN 43 que está separado virtualmente dos nós de borda no sistema, é ilustrada. O nó de controle de VPN 43 está, em tal concretização, conectado a nós de controle de VPN em outros domínios por conexões de sinal de controle de VPN dedicadas 47, criando uma rede de alto nível de sua propriedade.

Em uma concretização particular da presente invenção, a informação de VPN de domínio provida pode ser transferida dentro do

sistema, isto é, entre os domínios diferentes. Isto é ilustrado na Figura 4. A primeira etapa é provisão de informação de VPN dentro de cada domínio. Isto é executado por um nó de controle de VPN 43 em cada domínio. Porém, a configuração dos nós de controle de VPN 43 pode diferir entre os domínios diferentes. Na Figura 4, é indicado que domínio 10A tem um nó de controle de VPN 43 semelhante ao exemplo mostrado na Figura 3A, domínio 10C tem um nó de controle de VPN 43 semelhante ao exemplo mostrado na Figura 3B e domínios 10B, 10D e 10E têm nós de controle de VPN 43 semelhantes ao exemplo mostrado na Figura 3C. De acordo com cada SLA regulando o tráfego entre os domínios diferentes, pelo menos uma parte da informação de VPN de domínio disponível em cada nó de controle de VPN 43 é nesta concretização transferida ao nó de controle de VPN oponente nos domínios vizinhos. Setas 28 ilustram esta transferência de informação de inter-domínio. O SLA pode incluir acordos sobre quanto da informação disponível que deveria ser feita disponível para o domínio vizinho. Em um caso geral, o nó de controle de VPN processa informação de VPN de intra-domínio disponível em informação de VPN compilada ou processada que é adequada para remeter a domínios vizinhos. Se os domínios estiverem relacionados proximamente, por exemplo pertencendo à mesma operadora, o SLA poderia envolver uma transparência total ao trocar informação de VPN de domínio. Em outros casos, a informação processada 28 que é transferida entre os nós de controle de VPN 43 pode ser informação de VPN compilada, só revelando fato muito básico sobre as VPNs de domínio individual. A informação mínima que tem que ser enviada através das conexões de inter-domínio 12A-G na presente concretização são as identidades das VPNs que estão disponíveis em algum lugar além do nó de borda que envia a informação.

De acordo com a presente invenção, a informação sobre VPNs inclui pelo menos ID de domínio de domínios nos quais a VPNs estão atualmente disponíveis. Preferivelmente, a informação sobre VPNs também

inclui dados adicionais, tais como, mas não limitados a propriedades das VPNs, qualidades de ligação de ligações atualmente usadas pela VPNs, qualidades de ligação de ligações disponíveis para estender as VPNs, ID de nó de nós aos quais as VPNs estão disponíveis, e informação sobre quais domínios que têm que ser transitados para alcançar um domínio no qual as VPNs estão disponíveis. As propriedades das VPNs podem incluir por exemplo, propriedades de qualidade de serviço, propriedades de criptografia, propriedades de camada de transparência, propriedades de envelopamento; e propriedades de topologia.

Na Figura 4A, a informação 28 enviada nas conexões de inter-domínio 12A-G causa uma atualização da situação de informação de VPN disponível total no nó de controle de VPN de recepção. Este nó de controle de VPN agora também tem informação por exemplo de quais VPNs estão disponíveis pelas conexões de inter-domínio. Se informação mais completa estiver disponível, o nó de controle de VPN também pode determinar por exemplo identidades de nó de borda aos quais estas VPNs diferentes estão disponíveis, qualidade de serviço de VPN, etc. A informação de VPN assim alcançada é agora uma propriedade do domínio vizinho e pode, se permitido pelo SLA, ser usada para atividades naquele domínio. A informação armazenada no armazenamento 54 do nó de controle de VPN 43 poderia ser idêntica à informação recebida do domínio vizinho ou uma versão processada dela, adicionando, removendo ou modificando a informação recebida. Por exemplo, a informação poderia ser rotulada com uma indicação de qual domínio se originou.

Esta distribuição de informação pode continuar em muitas etapas sucessivas, em alguns casos aplicando modificação adicional da informação antes de remetida para outro domínio, em analogia com a primeira transferência. Eventualmente, todos os nós de controle de VPN na arquitetura de provedor de VPN 1 inteira tem pelo menos uma versão processada de toda

a informação de VPN de domínio disponível no sistema. Em cada nó de controle de VPN, a informação pode ser processada de acordo com o SLA que é válido para a conexão de inter-domínio associada a ser usada.

A troca de informação de VPN de domínio pode ser executada com temporização diferente. Uma alternativa é trocar continuamente ou pelo menos regularmente tal informação a fim de assegurar que a informação disponível sempre esteja atualizada. Em tais concretizações, a informação é preferivelmente armazenada nos nós de controle de VPN ou em qualquer outro nó, onde é recuperável pelo nó de controle de VPN. Em outras palavras, esta alternativa é um mecanismo de impulso típico para distribuição de dados.

Outra alternativa é que a troca de informação seja ativada por algum evento. Este evento pode por exemplo ser que uma mudança de algum tipo ocorreu em um domínio.

Em uma concretização preferida, o espalhamento de informação de VPN também está associado com um procedimento de reconhecimento. Quando um domínio recebeu informação de VPN de um domínio adjacente, uma mensagem de reconhecimento é retornada a fim de informar o domínio provendo a informação de VPN que a informação está agora disponível no domínio. Preferivelmente, reconhecimentos que estão associados com informação de VPN remetida são remetidos ao domínio do qual a informação de VPN entrou em primeiro lugar. Em outras palavras, informação de VPN é remetida em uma direção e mensagens de reconhecimento correspondentes são remetidas em retorno.

Agora, considere a conexão de um novo local de cliente 20' a um nó de borda 14' pretendido para ser conectado a uma certa VPN. O nó de controle 43 identifica que um novo local de cliente 20' está conectado e investiga para qual VPN está pretendido. De acordo com a presente invenção, meio é provido para achar informação sobre a VPN pretendida e de acordo com uma medida de qualidade, achar trajetos de conexão adequados para ela.

Quando um nó de controle de VPN 43 inicia um pedido de conexão de VPN, ele compara a VPN pedida à informação armazenada sobre VPNs que estão disponíveis por suas conexões de inter-domínio. Informação sobre em qual domínio a VPN existe e por quais conexões de inter-domínio a VPN é alcançável, está disponível. Na Figura 4, a VPN pedida é a VPN 22A da Figura 1. Nó de controle de VPN 43 de domínio 10E tem informação sobre essa VPN 22A que está disponível por nó de fronteira 18:1 de acordo com dois trajetos diferentes. Uma alternativa para alcançar a VPN 22A é através de conexão de inter-domínio 12D, por domínio 10B e através de conexão de inter-domínio 12A. A VPN 22A está então presente dentro de domínio 10A. Outro alternativa para alcançar a VPN 22A é através de conexão de inter-domínio 12D, por domínio 10B e através de conexão de inter-domínio 12C. A VPN 22A está então presente dentro de domínio 10C. Porém, o nó de controle de VPN 43 de domínio 10E também tem informação sobre VPN 22A por outro nó de fronteira 18. Aqui, a VPN 22A pedida é alcançável através de conexão de inter-domínio 12E, desde que a VPN 22A está disponível em domínio 10C. Finalmente, a VPN 22A pedida é alcançável através de conexão de inter-domínio 12G, desde que a VPN 22A também está disponível em domínio 10D.

Informação sobre como os domínios diferentes estão conectados juntos tem que estar presente ao analisar possíveis conexões. Esta informação pode ser obtida de muitos modos diferentes. Como a presente invenção opera mais vantajosamente em sistemas tendo uma configuração relativamente estável, um "mapa" é assumido dos domínios e conexões de inter-domínio são assumidos serem espalhados através dos domínios diferentes.

O nó de controle de VPN 43 assim tem toda a informação necessária para achar a VPN pedida. O nó de controle de VPN 43 avalia a informação disponível sobre a VPN requerida, determinando uma medida de

qualidade para cada possível trajeto de conexão. Tal medida de qualidade pode ser baseada por exemplo no numero de novas ligações a serem estabelecidas, no numero de domínios a passar antes de alcançar a VPN requerida, como o nó central ao qual a VPN é alcançada está localizado dentro da VPN requerida, propriedades de qualidade de serviço mínimas de ligações a serem estabelecidas, etc. Neste exemplo, a rota através de conexão de inter-domínio 12E parece muito simples de usar, mas por exemplo níveis de qualidade de serviço podem mudar tais decisões.

O processo de achar trajetos de conexão adequados poderia ser executado de acordo com princípios diferentes. Uma possibilidade é ter um limiar de aceitação e só trajetos de conexão tendo uma medida de qualidade excedendo o limiar de aceitação serão considerados de qualquer modo. Para os trajetos de conexão adequados restantes, alguém pode selecionar o tendo a medida de qualidade mais alta a ser configurada. Alguém também pode escolher selecionar mais de um trajeto de conexão a ser configurado, no caso extremo que todos aceitaram candidatos de conexão.

Na presente invenção, a informação de VPN de domínio provida é espalhada para todos os nós de controle de VPN 43 do sistema 1 inteiro. De tal modo, um pedido para achar uma VPN adequada pode ser posto diretamente a um nó de controle de VPN 43 do domínio "doméstico". A provisão e troca de informação de VPN podem, como indicado antes, serem executadas continuamente, regularmente ou ativadas plano pelo próprio pedido.

Esta abordagem tem a desvantagem que o sistema 1 inteiro tem que ser atualizado em todo único nó de controle de VPN 43. Porém, em sistemas onde a estrutura de domínios e VPNs é bastante estática, os esforços de comunicação necessários para manter os nós de controle de VPN 43 atualizados são relativamente baixos.

No processo de espalhar a informação de VPN através do

sistema, há preferivelmente uma limitação de remessa adicional de informação recebida. Na Figura 5, uma situação potencialmente dando um risco para malhas contínuas de provisão de informação de VPN é ilustrada. Uma rede de comunicação 1 inclui cinco domínios 10A-E. Em domínio 10E, uma VPN 22A está disponível. Agora, considere uma situação onde a VPN 22A é mudada de alguma maneira, por exemplo que uma conexão de intra-domínio é atualizada para suportar uma largura de banda mais alta. Domínio 10E executa uma atualização interna da informação de VPN e envia informação de VPN atualizada para seu domínio 10A adjacente sozinho. O domínio 10A atualiza seu próprio banco de dados e remete a informação de VPN para domínio 10B.

Também em domínio 10B, a informação sobre a VPN 22A é atualizada. A informação de atualização é então remetida aos domínios adjacentes adicionais 10C e 10D. O procedimento também é repetido nestes domínios e outra remessa da informação de VPN é executada. Domínio 10C envia a informação ao domínio 10D e o domínio 10D envia a mesma informação ao domínio 10C. O procedimento continua, e uma malha contínua de informação de VPN circulará entre domínios 10B-D. Em uma concretização preferida da presente invenção, meio para proibir os pedidos de informação de serem remetidos em malhas contínuas é provido. Tal meio para proibir circulação em malha de pedidos de informação é provido preferivelmente com relação a envio ou recebimento de tais pedidos de informação, isto é, eles são arranjados tanto para proibir a remessa atual para um novo domínio adjacente ou para proibir a aceitação de um pedido de informação recebido. Várias concretizações de por restrições em remessa são possíveis. Algumas delas são mencionadas brevemente aqui abaixo.

Em uma concretização de um arranjo de proibição de malha, cada mensagem de informação de VPN é provida com uma identidade. Esta identidade pode por exemplo ser um campo separado tendo um certo número

de identidade único, ou a identidade poderia ser baseada na informação atual que leva. Se identidades separadas de mensagens de informação de VPN forem usadas, mensagens de informação de VPN recebidas e aceitas são armazenadas preferivelmente em um armazenamento. Quando uma nova mensagem de informação de VPN chega, uma comparação é feita com os dados armazenados para revelar se o pedido de informação já foi recebido antes. Em tal caso, o pedido é desprezado. Caso contrário, o pedido é aceito e a identidade é adicionada ao armazenamento.

A comparação também poderia ser executada com relação à remessa atual da informação de VPN. Em tal caso, a identidade de mensagem poderia ser armazenada no armazenamento e uma condição extra para remeter o pedido poderia ser que não deveria haver duas identidades de mensagem idênticas dentro do banco de dados.

Se a identidade for baseada na própria informação de VPN, a informação de VPN recebida é comparada com a informação de VPN correspondente presentemente armazenada no domínio. Se a informação de VPN não causar qualquer mudança ser feita, a informação de VPN recebida é considerada como uma mensagem duplicada e é rejeitada. Em tal arranjo, só atualizações verdadeiras são remetidas.

Outra concretização para proibição de malha é baseada em informação sobre trajetos de remessa. Adicionando informação na própria mensagem de informação de VPN sobre quais domínios que são passados durante o processo de remessa, um domínio receptor pode facilmente pesquisar por sua própria identidade entre esta informação. Se a própria identidade estiver presente, a informação é desprezada. Caso contrário, a própria identidade é adicionada e a informação pode ser remetida. A comparação também pode ser feita ao lado remetente. Antes de remeter uma mensagem de informação de VPN para um domínio, o domínio remetente pesquisa a informação de trajeto de remessa para as identidades de seus

domínios adjacentes. Para domínios que já estão presentes no trajeto de remessa, remessa é proibida.

Ainda outra concretização é baseada em tempo de vida. Um certo tempo de vida pode ser ajustado ao criar a atualização de informação de VPN original, por exemplo fixando um tempo de expiração de validade. Ao receber e/ou remeter tal informação, este tempo de expiração de validade é verificado contra, por exemplo, um tempo de sistema, e quando a validade é expirada, nenhuma remessa mais é executada. Uma variação do conceito de linha de tempo é ajustar um tempo de vida restante, que então é reduzido em relação a cada remessa. Quando o tempo de vida restante expira, nenhuma remessa mais é executada. Esta abordagem pode também ser usada então utilizando o número de remessas como uma medida de "tempo", isto é, é declarado da iniciação que um número máximo de remessas é permitido. Para cada remessa, o número restante é reduzido por uma unidade.

Figure 6A ilustra um esquema de bloco de uma concretização particular de um nó de controle de VPN 43 relativamente geral de acordo com a presente invenção provendo o arranjo de determinação de trajeto de conexão. O nó de controle de VPN 43 inclui meio 52 para prover informação de VPN de domínio. Esta informação pode ser provida por outros nós no domínio por conexões 62. Uma interface de comunicação de controle principal 40 é provida para comunicação com outros domínios. Esta interface 40 pode ser arranjada em combinação com as conexões de intra-domínio 62. Uma unidade de avaliação 49 investigando se uma identidade de uma VPN pedida casa com a informação de VPN de domínio, é provida. A unidade de avaliação 49 é ademais arranjada para executar a avaliação discutida acima da informação sobre a VPN pedida de acordo com uma medida de qualidade para achar trajetos de conexão adequados. O pedido de VPN pode ser recebido de outro nó do próprio domínio ou pode ser iniciado dentro do nó de controle de VPN. Uma seção de operação de VPN externa 44 é responsável

por operar configuração de VPN de inter-domínio. A seção de operação de VPN externa 44 inclui meio para espalhar 71 a informação sobre VPNs disponíveis no próprio domínio para domínios adjacentes. A seção de operação de VPN externa 44 ademais inclui meio para receber 73 informação sobre VPNs de domínios adjacentes e meio para distribuir 72 informação baseada em informação recebida sobre VPNs de domínios adjacentes para outros domínios adjacentes. Os meios 71-73, e em particular meios 71-72, podem ser preferivelmente arranjados de uma maneira integrada, desde há muitas funcionalidades de parte comuns dos meios diferentes. Porém, em outras concretizações, unidades separadas. podem ser providas Uma seção de operação de VPN interna 41 tem funcionalidades para configurar conexões internas dentro do próprio domínio e inclui preferivelmente o meio para coletar informação sobre VPNs disponíveis no próprio domínio, isto é, o meio 52 para prover informação de VPN de domínio.

Figure 6B ilustra um esquema de bloco de outra concretização particular de um nó de controle de VPN 43 de acordo com a presente invenção. Informação de VPN de domínio relativa ao próprio domínio é provida por uma seção de operação de VPN interna 41, incluindo meio para coletar 52 informação sobre VPNs. A informação de VPN de domínio interna é, nesta concretização particular, armazenada em uma memória de dados 74. Esta informação é, nesta concretização particular, provida, como ilustrado pela seta 62, por comunicação com outros nós dentro do domínio. Em outras concretizações, esta informação pode ser obtida de outros modos. A informação de VPN de domínio interno também é remetida a um banco de dados de informação de VPN total 54 em uma seção de operação de VPN externa 44. A seção de operação de VPN interna 41 também inclui uma máquina de configuração interna 46, tendo funcionalidades para configurar conexões internas dentro do próprio domínio. A seção de operação de VPN interna 41 é provida com informação de VPN de domínio interna, como

também informação do banco de dados 54. Comunicações relativas a assuntos de domínio interno são assim executadas através de uma conexão 42 entre a seção de operação de VPN interna 41 e a seção de operação de VPN externa 44. O nó de controle de VPN 43 tem uma interface de comunicação de controle principal 40 com outros domínios através de uma conexão de inter-domínio. Informação de VPN de domínio de outros domínios é recebida pela interface 40, e uma unidade de processamento de entrada 56 extrai informação útil dos dados recebidos e armazena esta informação externa em um banco de dados de entrada 58. Neste banco de dados de entrada 58, informação adicional como de qual domínio os dados externos foram recebidos, também é armazenada. A unidade de processamento de entrada 56 e o banco de dados de entrada 58 estão nesta concretização incluídos no meio para receber 73 informação sobre VPNs de domínios adjacentes. O banco de dados de entrada 58 atualiza a banco de dados de informação de VPN total 54 quando apropriado. A seção de operação de VPN externa 44 também inclui uma máquina de configuração externa 60, tendo funcionalidades para configurar partes de conexões de inter-domínio que são pertinentes para o domínio. Esta funcionalidade será descrita em mais detalhes abaixo.

A seção de operação de VPN externa 44 provê informação para outros domínios. Informação de VPN de domínio, associada com o próprio domínio e/ou com outros domínios é extraída do banco de dados 54 e provida a uma unidade de processamento de dados de saída 50. A informação recuperada é processada de acordo com SLAs associados com os domínios de vizinho diferentes e armazenada em uma banco de dados de saída 48. Os SLAs por esse meio determinam qual informação é permitida ser espalhada aos domínios vizinhos diferentes. Operadoras de domínio tendo uma relação íntima podem permitir troca de informação mais transparente, enquanto domínios pertencendo a operadoras não relacionadas podem aplicar uma troca de informação mais restritiva. Informação sobre VPNs é transmitida na

interface 40, quando adequado. O banco de dados 54, a unidade de processamento de dados de saída 50 e o banco de dados de saída 48 estão, nas presentes concretizações, incluídos em uma unidade comum 71, 72 para espalhar a informação sobre VPNs disponíveis no próprio domínio e para distribuir informação baseada em informação recebida sobre VPNs de domínios adjacentes.

Um exemplo, ilustrado na Figura 7, mostra como uma configuração subseqüente de uma VPN de inter-domínio pode ser automatizada. Um novo local de cliente 20' no domínio 10E deverá ser conectado à VPN 22A. É assumido que envelopes de VPN são usados para conexões de VPN ambos dentro de domínios e entre domínios. As etapas seguintes são tomadas.

O nó de controle de VPN em domínio 10E obtém um pedido, de algum modo, do cliente para se conectar à VPN 22A. Como o banco de dados de VPN de domínio 10E mostra que a VPN 22A não está presente em domínio 10E, o nó de controle de VPN em domínio 10E não pode conectar o local de cliente 20' diretamente à VPN 22A dentro de domínio 10E. Porém, informação de VPN originada de outros domínios está disponível mostrando que um trajeto de conexão para VPN 22A pode ser achado no "próximo salto" 10B, 10C e 10D.

O nó de controle de VPN em domínio 10E escolhe só estabelecer a VPN pelo "próximo salto" 10B, de acordo com a avaliação da medida de qualidade discutida acima. estabelece um envelope de VPN 71 para VPN 22A do nó de borda 14', onde o local de cliente 20' está conectado, ao nó de fronteira 18:1, que está conectado a domínio 10B por ligação 12D. O nó de controle de VPN em domínio 10E inicia comunicação com o nó de controle de VPN em domínio 10B e instala um envelope de VPN 72 para VPN 22A através da ligação 12D a nó de fronteira 18:2.

O nó de controle de VPN em domínio 10B estabelece a VPN pelo "próximo salto" 10A. Instala um envelope de trânsito de VPN 73 para

VPN 22A do nó de fronteira 18:2, que está conectado a domínio 10B por ligação 12D ao nó de fronteira 18:3, que está conectado a domínio 10A por ligação 12A. O nó de controle de VPN em domínio 10B inicia comunicação com o nó de controle em domínio 10A e instala um envelope de VPN 74 através da ligação 12A a nó de fronteira 18:4. Como a VPN 22A está presente em domínio 10A, o nó de controle em domínio 10A pode instalar um envelope interno 75 do nó de fronteira que está conectado a domínio 10B por ligação 12A, ao nó de fronteira 18:5, que está conectado à VPN 22A.

Depois de cada etapa, os bancos de dados de VPN atualizados estarão disponíveis para a próxima rodada de coletar informação de VPN.

As etapas básicas de uma concretização de um método de acordo com a presente invenção são ilustradas na Figura 8. O procedimento começa na etapa 200. Na etapa 210, informação sobre VPNs disponíveis em cada domínio é coletada em domínio respectivo. Na etapa 212, a informação sobre VPNs é espalhada para domínios adjacentes. Na etapa 214, informação sobre VPNs de domínios adjacentes é recebida. Baseado na informação recebida sobre VPNs de domínios adjacentes, informação é distribuída para outros domínios adjacentes na etapa 216, com ou sem qualquer processamento intermediário. Da informação total sobre VPNs, uma avaliação de medidas de qualidade é feita na etapa 218 para achar trajetos de conexão adequados. O procedimento termina na etapa 299.

As concretizações descritas acima são para serem entendidas como alguns exemplos ilustrativos da presente invenção. Será entendido por aqueles qualificados na arte que várias modificações, combinações e mudanças podem ser feitas às concretizações sem partir da extensão da presente invenção. Em particular, soluções de parte diferentes nas concretizações diferentes podem ser combinadas em outras configurações onde tecnicamente possível. A extensão da presente invenção está, porém, definida pelas reivindicações anexas.

REIVINDICAÇÕES

1. Método para determinar um trajeto de conexão, em uma rede privada virtual de multi-domínio - VPN - dentro de uma rede de comunicação tendo pelo menos dois domínios interconectados, entre um primeiro nó em um primeiro domínio e uma primeira VPN, caracterizado pelo fato de compreender as etapas de:

coletar, em cada domínio, informação sobre VPNs disponíveis em dito cada domínio;

espalhar a informação sobre VPNs para domínios adjacentes;

receber informação sobre VPNs de domínios adjacentes;

distribuir informação baseado em informação recebida sobre VPNs de domínios adjacentes para outros domínios adjacentes;

a informação sobre VPNs incluindo pelo menos ID de domínio de domínios nos quais as VPNs estão atualmente disponíveis; e

avaliar informação sobre a primeira VPN de acordo com uma medida de qualidade para achar trajetos de conexão adequados entre dito primeiro nó dentro de dito primeiro domínio e dita primeira VPN.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de espalhar é executada em direção a todos os domínios adjacentes e a etapa de distribuir é executada em direção a todos os domínios adjacentes, exceto o domínio adjacente provendo a informação recebida sobre VPNs.

3. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que pelo menos uma da etapa de espalhamento e da etapa de distribuição é executada regularmente.

4. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que pelo menos em uma da etapa de espalhamento e da etapa de distribuição é executada quando ativada por um evento.

5. Método de acordo com a reivindicação 4, caracterizado pelo

fato de que o evento é uma mudança na informação sobre VPNs disponíveis em dito cada domínio.

6. Método de acordo com a reivindicação 4, caracterizado pelo fato de que o evento é uma recepção de informação sobre VPNs de um domínio adjacente.

7. Método de acordo com quaisquer das reivindicações 1 a 6, caracterizado pelo fato de compreender as etapas adicionais de:

retornar uma mensagem de reconhecimento para domínios adjacentes dos quais informação sobre VPNs é alcançada;

receber mensagens de reconhecimento de domínios adjacentes; e

remeter mensagens de reconhecimento recebidas para a informação distribuída baseado em informação recebida sobre VPNs de domínios adjacentes para o domínio adjacente do qual a informação sobre VPNs foi recebida.

8. Método de acordo com quaisquer das reivindicações 1 a 7, caracterizado pelo fato de compreender as etapas adicionais de proibir a informação sobre VPNs ser remetida em malhas contínuas dentro da rede de comunicação.

9. Método para determinar um trajeto de conexão de acordo com a reivindicação 8, caracterizado pelo fato de que a etapa de proibição é executada antes de distribuir a informação sobre VPNs para um domínio adjacente.

10. Método para determinar um trajeto de conexão de acordo com a reivindicação 8, caracterizado pelo fato de que a etapa de proibição é executada antes de aceitar informação recebida sobre VPNs de outro domínio.

11. Método para determinar um trajeto de conexão de acordo com quaisquer das reivindicações 8 a 10, caracterizado pelo fato de que a etapa de proibição está baseada em uma comparação entre a informação

presentemente recebida sobre VPNs e um armazenamento de dados representando informação recebida anteriormente sobre VPNs.

12. Método para determinar um trajeto de conexão de acordo com quaisquer das reivindicações 8 a 10, caracterizado pelo fato de que a etapa de proibição está baseada em uma comparação entre identidades de domínio e dados representando domínios que a informação recebida sobre VPNs passou, incluídos na informação sobre VPNs.

13. Método para determinar um trajeto de conexão de acordo com quaisquer das reivindicações 8 a 10, caracterizado pelo fato de que a etapa de proibição está baseada em uma tempo de vida da informação sobre VPNs.

14. Método de acordo com quaisquer das reivindicações 1 a 13, caracterizado pelo fato de que a informação sobre a VPNs inclui adicionalmente pelo menos uma de:

propriedades da primeira VPN;

qualidades de ligação de ligações usadas atualmente pela primeira VPN;

qualidades de ligação de ligações disponíveis para estender a primeira VPN;

ID de nó de nós aos quais a VPNs estão disponíveis; e

informação sobre quais domínios que têm que ser transitados para alcançar um domínio no qual as VPNs estão disponíveis.

15. Método de acordo com a reivindicação 14, caracterizado pelo fato de que propriedades da primeira VPN incluem um pelo menos uma de:

propriedades de qualidade de serviço;

propriedades de criptografia;

propriedades de camada de transparência;

propriedades de envelopamento; e

propriedades de topologia.

16. Arranjo de domínio de rede de comunicação, caracterizado pelo fato de compreender:

meio para coletar informação sobre redes privadas virtuais - VPNs - disponíveis em um domínio do arranjo de domínio de rede de comunicação;

meio para espalhar a informação sobre VPNs para domínios adjacentes em uma rede de comunicação tendo pelo menos dois domínios;

meio para receber informação sobre VPNs de domínios adjacentes na rede de comunicação;

meio para distribuir informação baseada em informação recebida sobre VPNs de domínios adjacentes para outros domínios adjacentes;

a informação sobre a primeira VPN incluindo pelo menos ID de domínio de domínios nos quais VPNs estão atualmente disponíveis; e

meio para avaliar a informação sobre VPNs de acordo com uma medida de qualidade para achar trajetos de conexão adequados de nós do domínio para uma primeira VPN.

17. Arranjo de domínio de rede de comunicação de acordo com a reivindicação 16, caracterizado pelo fato de que o meio para espalhamento é arranjado para espalhar a informação sobre VPNs para todos os domínios adjacentes e o meio para distribuição é arranjado para distribuir a informação recebida sobre VPNs para todos os domínios adjacentes, exceto o domínio adjacente provendo a informação recebida sobre VPNs.

18. Arranjo de domínio de rede de comunicação de acordo com a reivindicação 16 ou 17, caracterizado pelo fato de compreender:

meio para retornar uma mensagem de reconhecimento para domínios adjacentes dos quais informação sobre VPNs é alcançada;

meio para receber mensagens de reconhecimento de domínios

adjacentes; e

meio para remeter mensagens de reconhecimento recebidas para a informação distribuída baseado em informação recebida sobre VPNs de domínios adjacentes para o domínio adjacente do qual a informação sobre VPNs foi recebida.

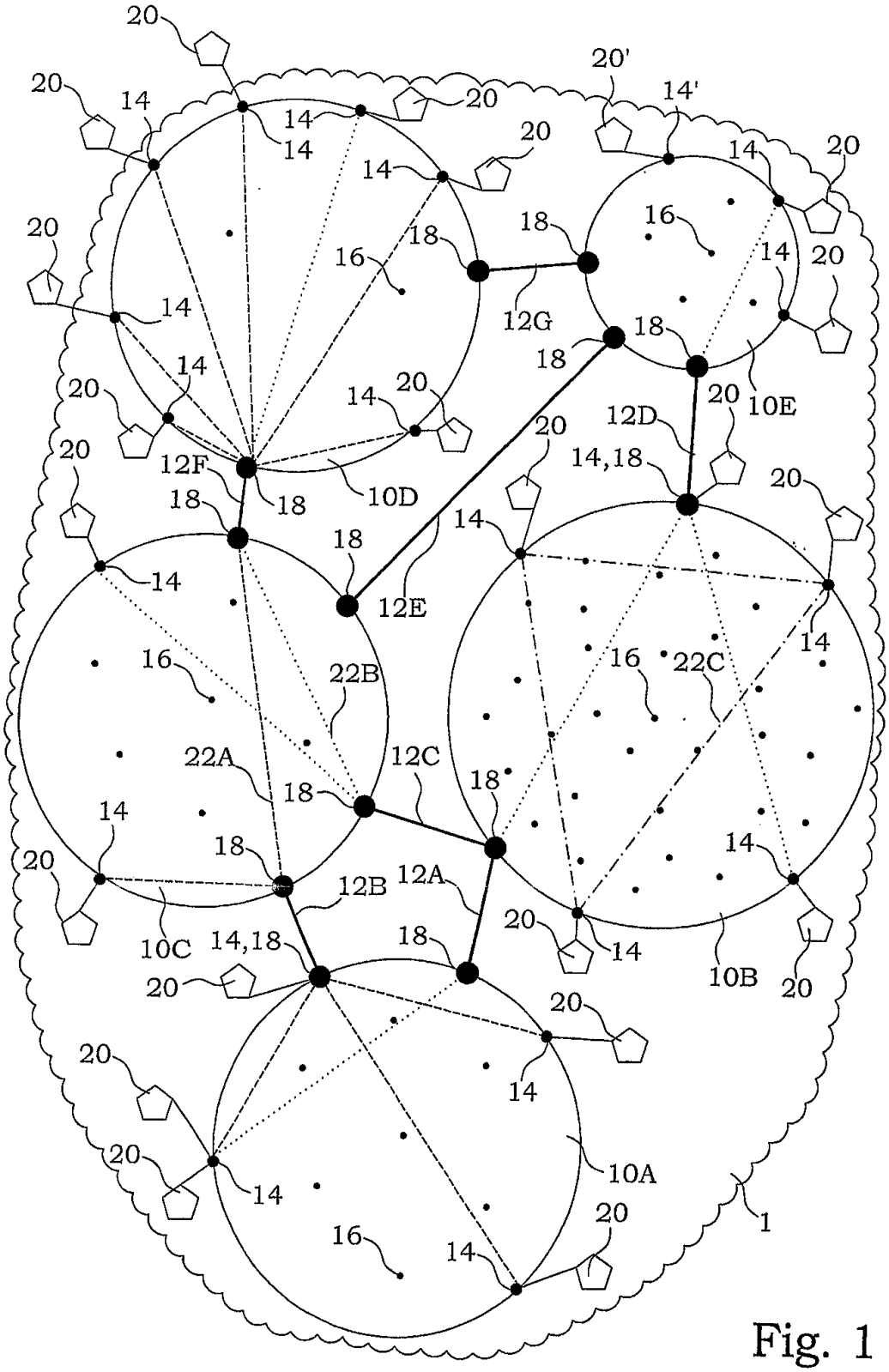

Fig. 1

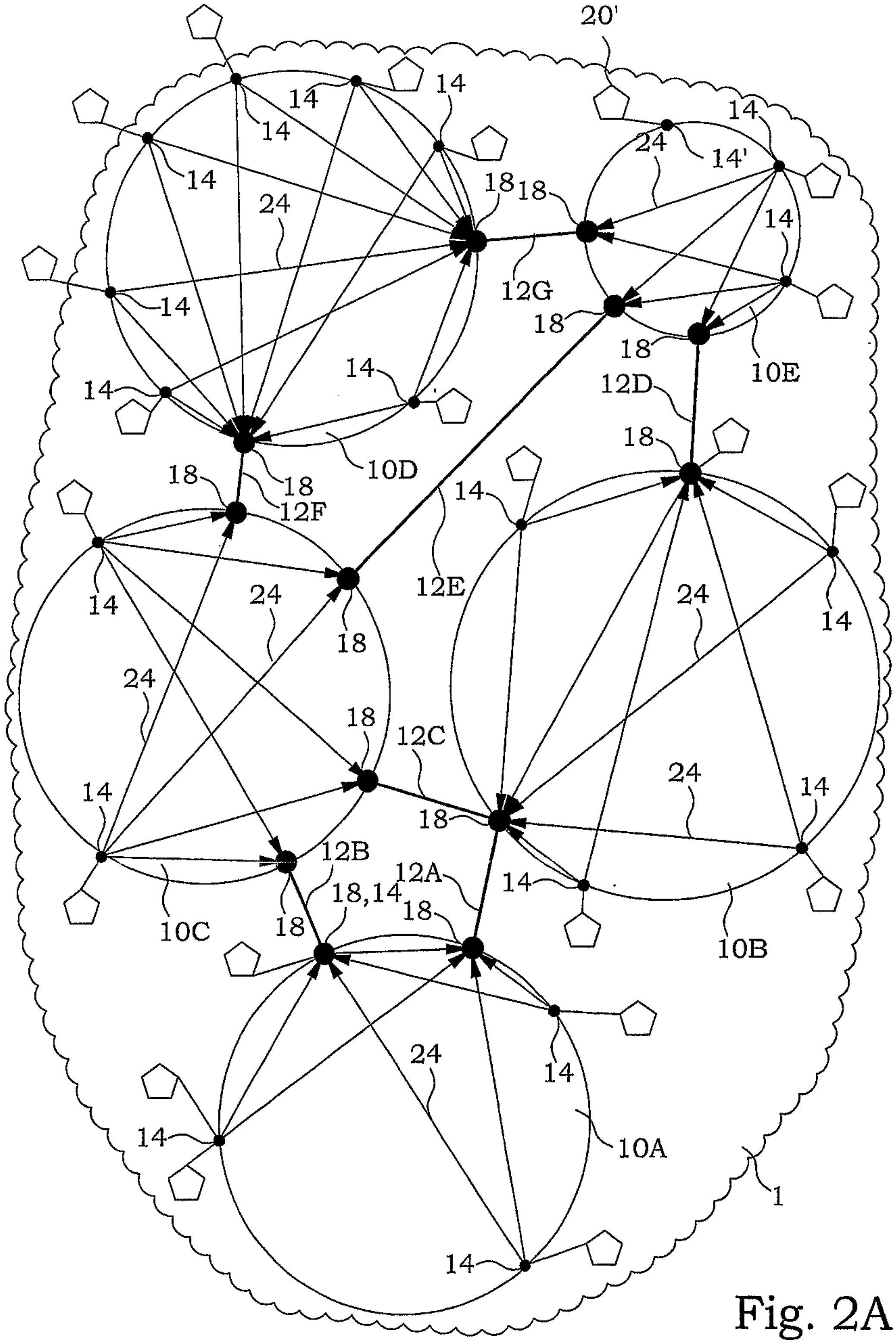
20'
14
14
14
14
24
18
18
24
14'
14
14
24
14
12G
18
14
18
10E
14
14
12D
18
10D
18
18
12F
14
14
24
12E
18
24
24
14
14
18
12C
24
14
24
14
18
12B
12A
14
18
18,14
18
10C
10B
24
14
14
10A
1
14

Fig. 2A

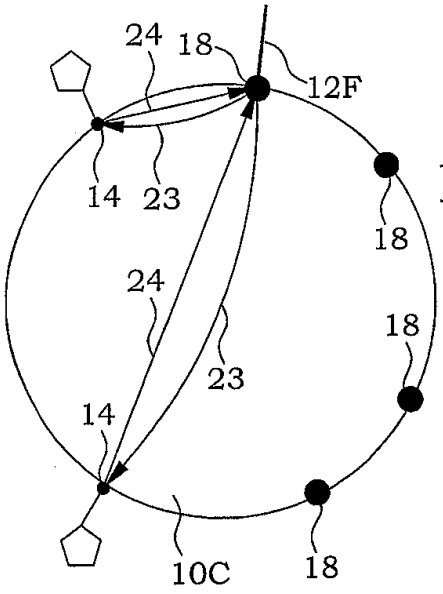

Fig. 2B

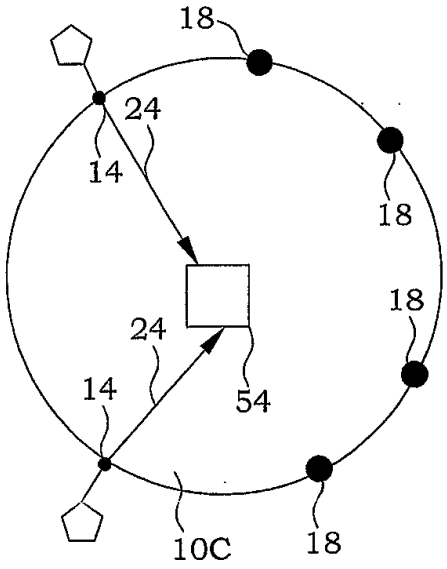

Fig. 2C

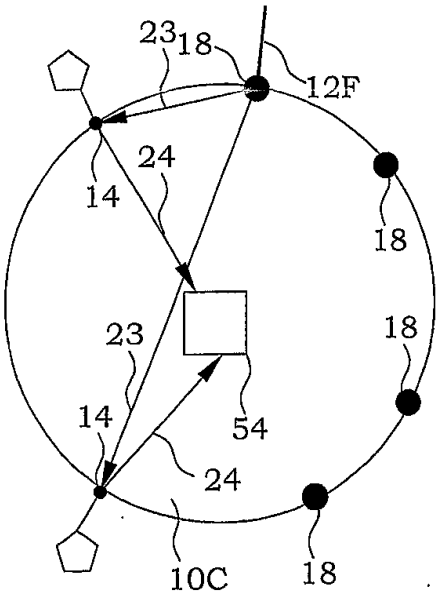

Fig. 2D

38

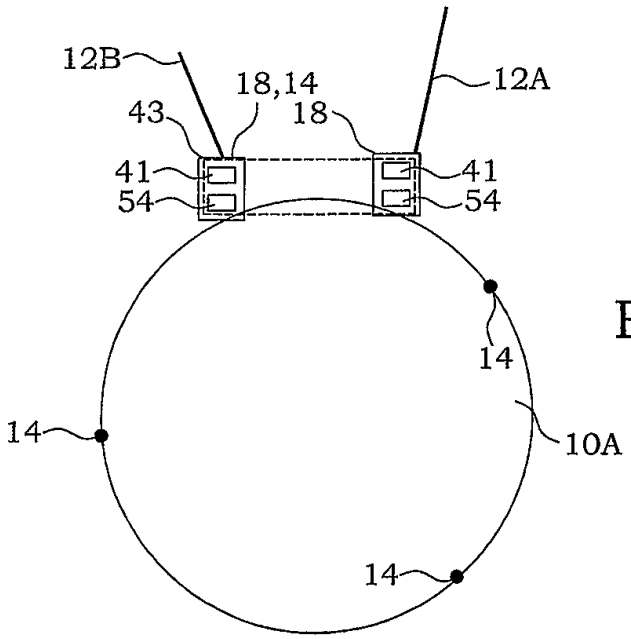

Fig. 3A

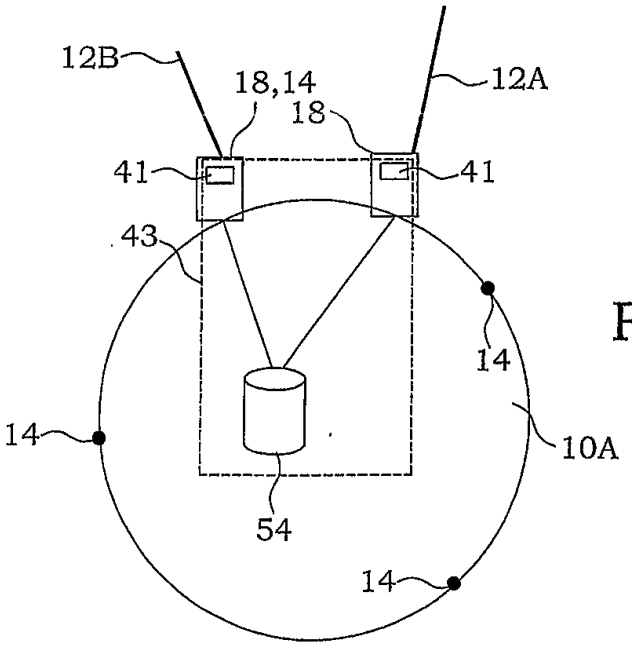

Fig. 3B

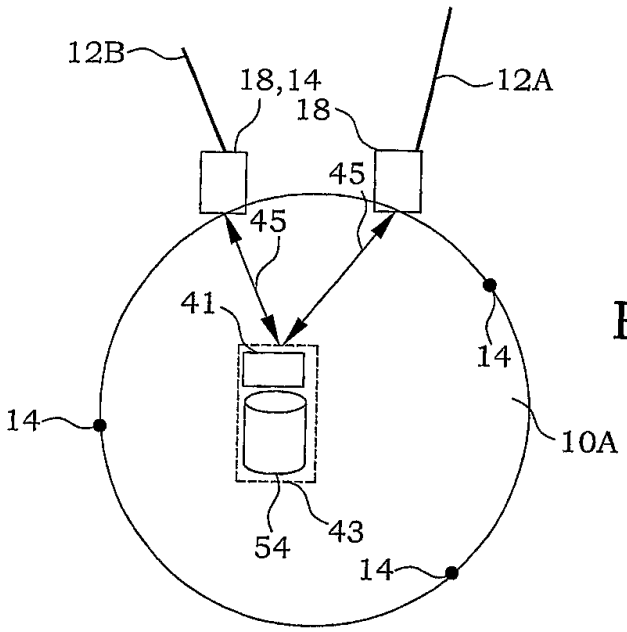
12B
18,14
18
12A
45
45
41
14
14
10A
54
43
14

Fig. 3C

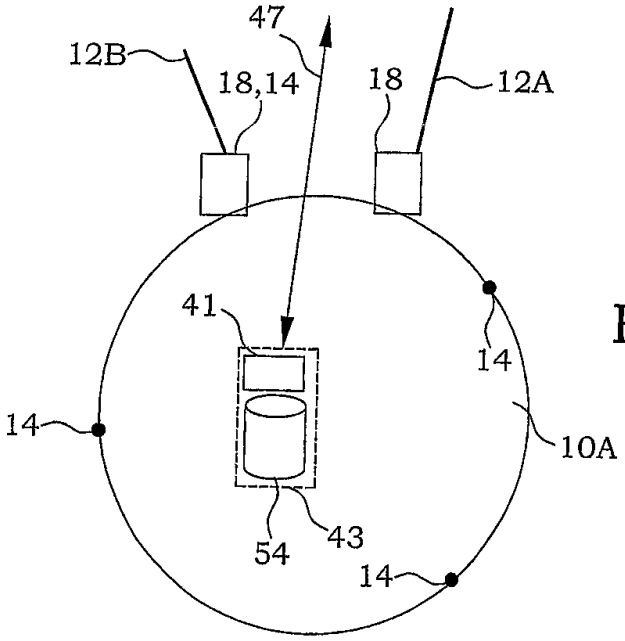
47
12B
18,14
18
12A
41
14
14
10A
54
43
14

Fig. 3D

40

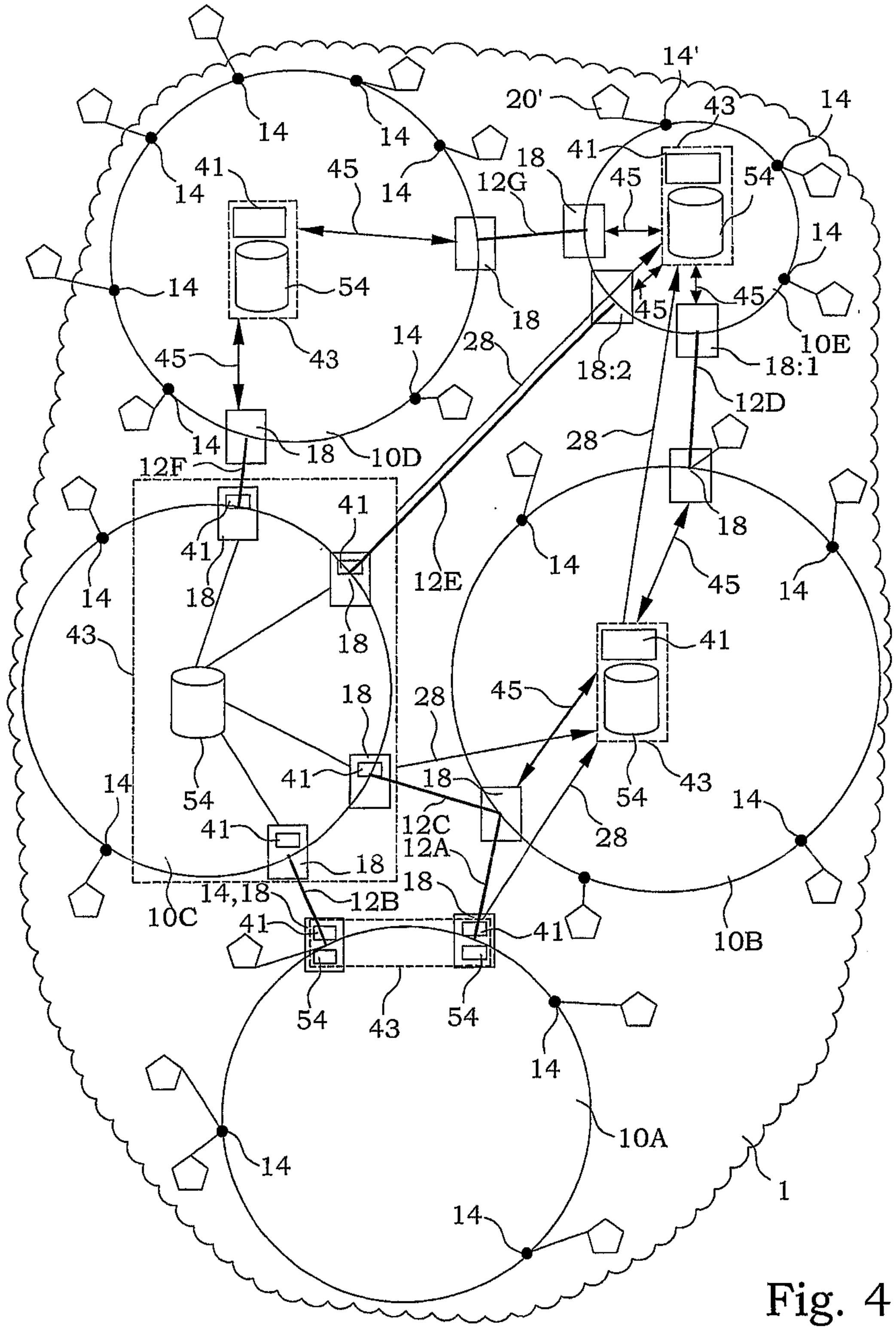
14'
20'
43
14
41
18
12G
45
54
14
41
45
14
14
14
14
14
54
18
45
45
18:2
18:1
10E
43
14
28
28
12D
45
14
18
10D
14
18
12F
41
41
12E
41
18
18
14
14
14
43
45
18
28
54
18
41
12C
12A
54
43
28
14
14
41
54
18
14,18
12B
10C
18
41
41
10B
54
43
54
14
10A
14
1
14

Fig. 4

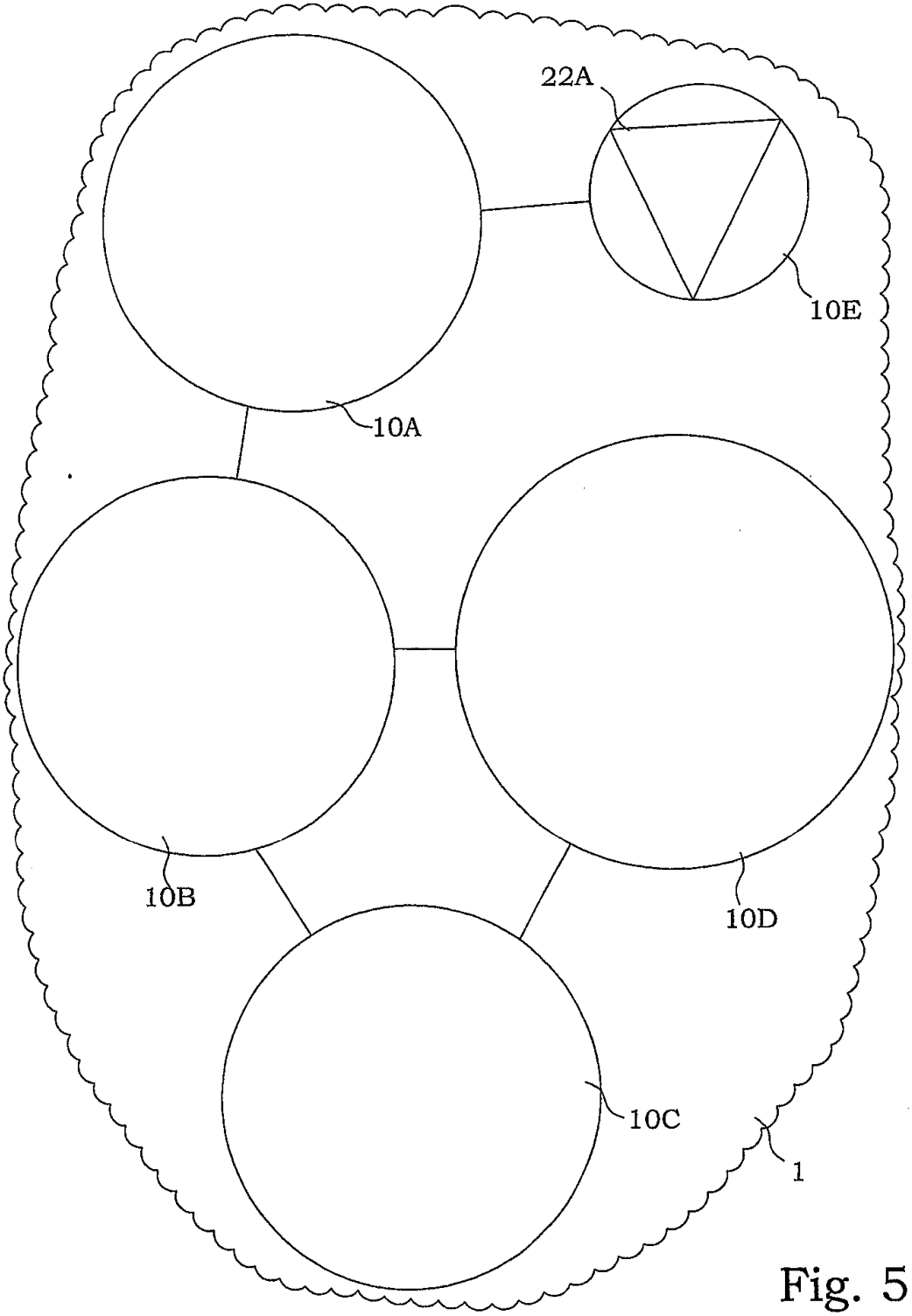

Fig. 5

42

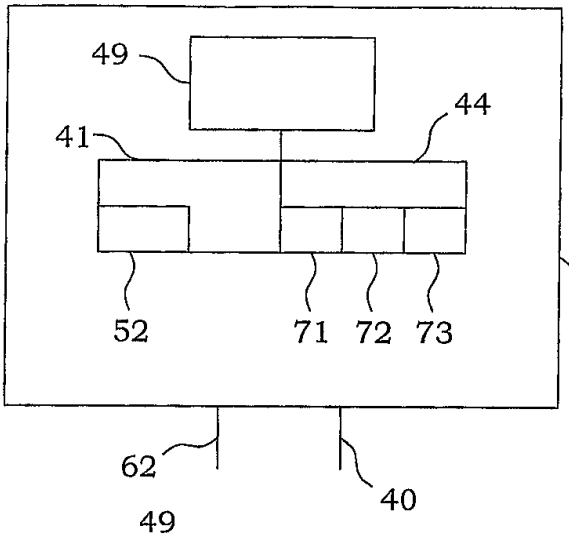

Fig. 6A

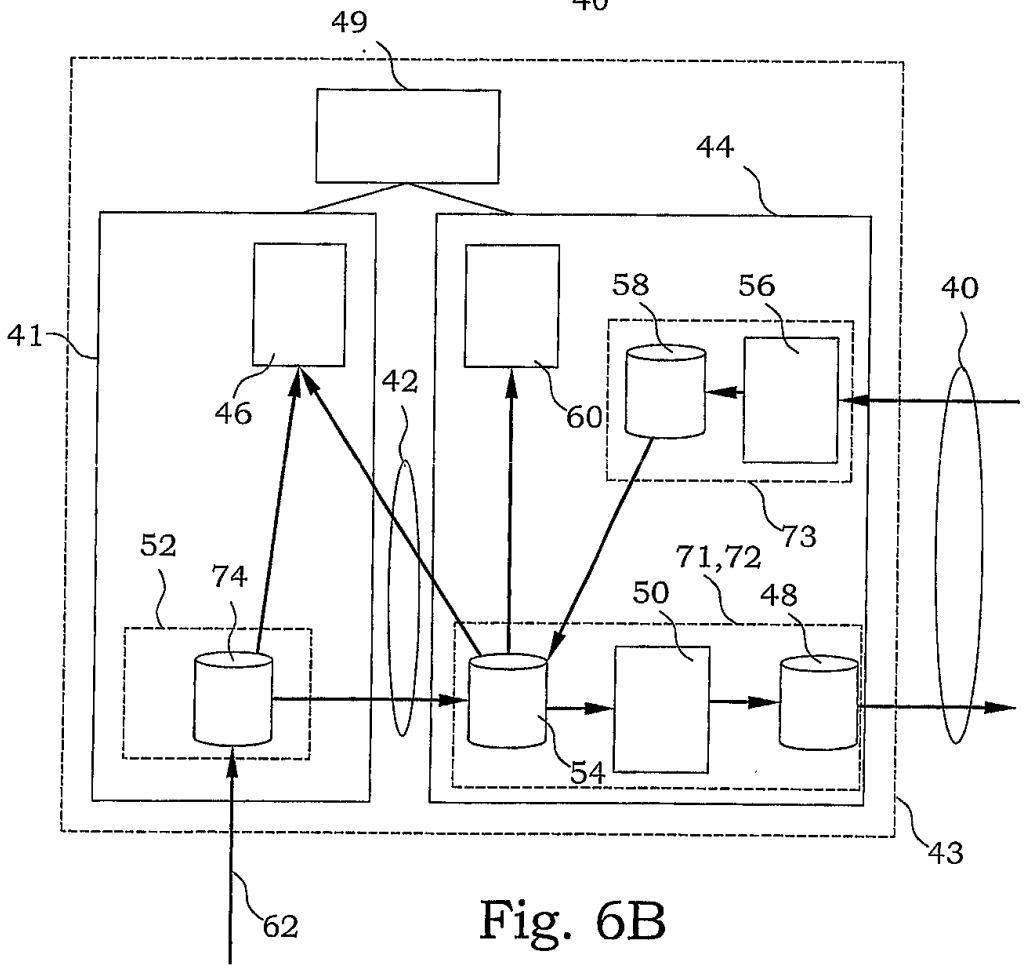

Fig. 6B

43

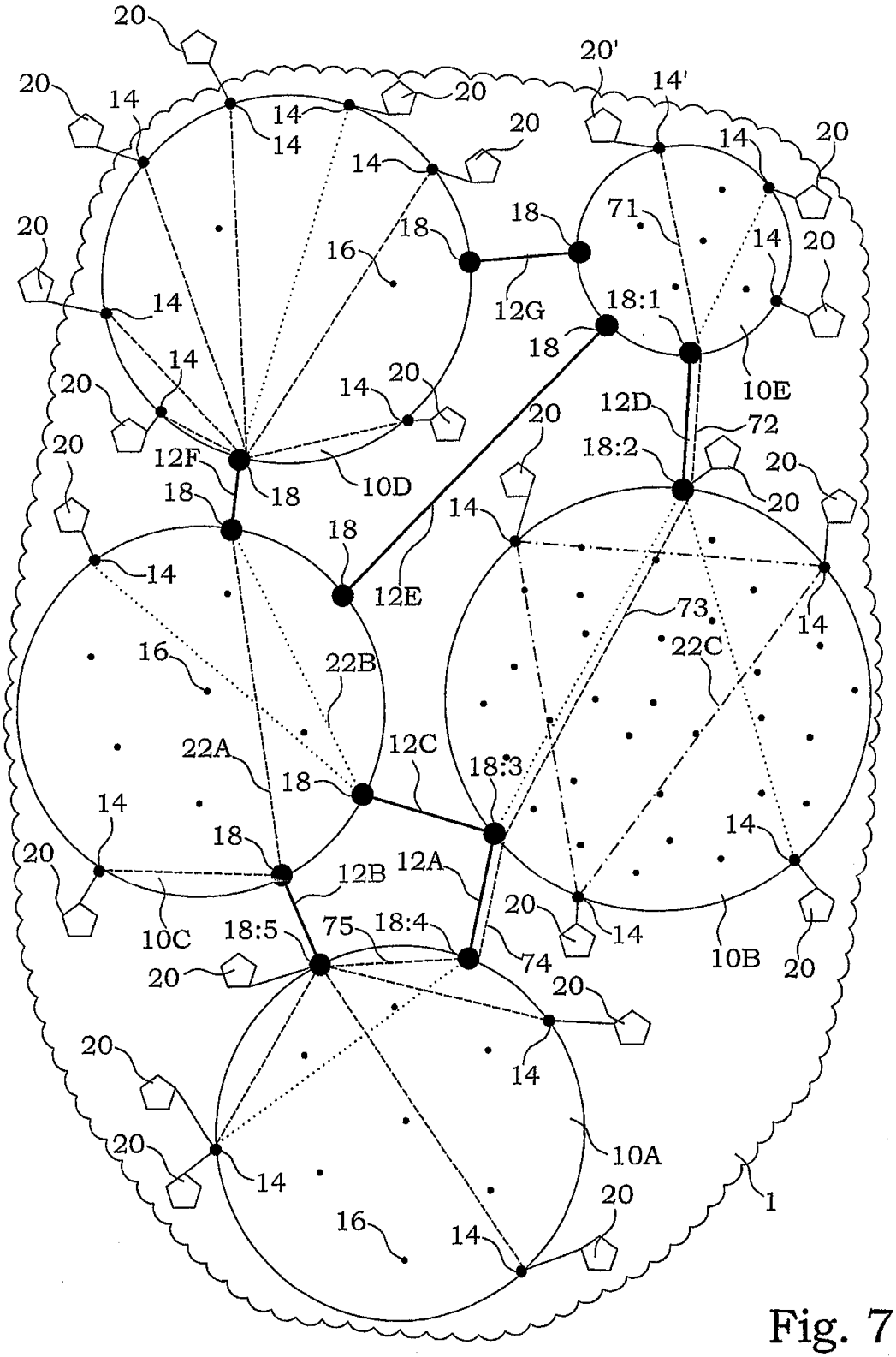
20
20'
14'
14
18
71
12G
18:1
10E
12D
72
18:2
12F
10D
12E
73
22C
22B
22A
12C
18:3
12B
12A
10C
18:5
75
18:4
74
10B
10A
1
16

Fig. 7

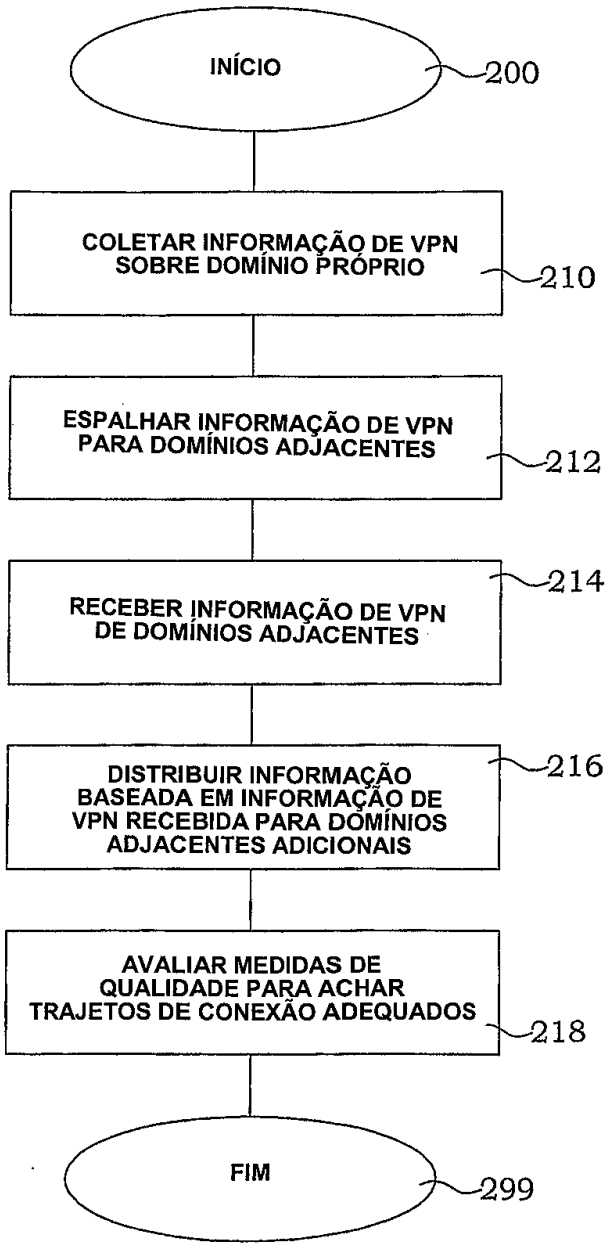
INÍCIO
200
COLETAR INFORMAÇÃO DE VPN SOBRE DOMÍNIO PRÓPRIO
210
ESPALHAR INFORMAÇÃO DE VPN PARA DOMÍNIOS ADJACENTES
212
RECEBER INFORMAÇÃO DE VPN DE DOMÍNIOS ADJACENTES
214
DISTRIBUIR INFORMAÇÃO BASEADA EM INFORMAÇÃO DE VPN RECEBIDA PARA DOMÍNIOS ADJACENTES ADICIONAIS
216
AVALIAR MEDIDAS DE QUALIDADE PARA ACHAR TRAJETOS DE CONEXÃO ADEQUADOS
218
FIM
299

Fig. 8