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

(11) PI 0418936-1 B1

(22) Data do Depósito: 30/06/2004

(45) Data de Concessão: 03/07/2018

(54) Título: MÉTODO PARA CONFIGURAR UMA REDE PRIVADA VIRTUAL DE MULTI-DOMÍNIO, REDE DE COMUNICAÇÃO, E, NÓ DE CONTROLE DE VPN

(51) Int.Cl.: H04L 12/46; H04L 12/24

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

(72) Inventor(es): CHRISTOFER FLINTA; JAN-ERIK MANGS; LARS WESTBERG

"MÉTODO PARA CONFIGURAR UMA REDE PRIVADA VIRTUAL DE MULTI-DOMÍNIO, REDE DE COMUNICAÇÃO, E, NÓ DE CONTROLE DE VPN"

CAMPO TÉCNICO

A presente invenção relaciona-se em geral a redes privadas virtuais em sistemas de comunicação, e em particular à configuração de 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. Além disso, quando um cliente quer modificar sua VPN, o procedimento inteiro tem que ser repetido.

Ao estabelecer VPNs em uma rede, tecnologias diferentes também podem ser usadas. Cada tecnologia tem seus próprios benefícios e desvantagens e seu próprio modo de configurar as VPNs. Não há nenhuma arquitetura de VPN geral que seja independente de tecnologia de VPN.

SUMÁRIO

Um problema geral de soluções da arte anterior é assim que redes de comunicação provendo redes privadas virtuais tendo uma cobertura geográfica grande 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 torna complexa e demorada. Um problema adicional é que recursos de comunicação de operadoras de rede cobrindo áreas geográficas menores não podem ser utilizados geralmente para VPNs de área ampla.

Um objetivo geral da presente invenção é assim melhorar métodos para configuração de VPNs como também prover sistemas e dispositivos adequados portanto. Um objetivo adicional da presente invenção é prover métodos para configurar VPNs utilizando mais de um domínio de rede. Outro objetivo adicional da presente invenção é prover métodos para configuração de VPNs que são basicamente independentes da tecnologia de VPN atual usada. Ainda um objetivo adicional da presente invenção é prover um método para configuração automática de uma VPN.

Os objetivos anteriores são alcançados por métodos e dispositivos de acordo com as reivindicações de patente inclusas. Em palavras gerais, informação sobre VPNs em um domínio é provida. Comparando um pedido para uma configuração de uma VPN com a informação provida de outros domínios conectados, um casamento pode ser achado. A reconfiguração pode então ser executada baseada no resultado da casamento. 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 distribuída está em concretizações particulares, localizado para limitar nós 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 para informação de VPN de domínio dos nós de borda ou uma combinação disso. A coleta pode ser ativada por um evento externo, tal como um pedido de configuração de VPN. A informação de VPN de domínio provida é, em uma concretização, espalhada para outros domínios sob constrições postas por SLAs entre operadoras de domínio. Em outra concretização, o pedido de configuração de VPN é ao invés espalhado para domínios diferentes. O casamento pode assim ser executado a várias distâncias do domínio originalmente solicitante.

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 domínio de VPN é feita disponível para suportar configuração de VPN essencialmente em todos os domínios de um sistema de multi-domínio. Porém, ao mesmo tempo, em uma concretização, a informação atual é espalhada através do sistema de multi-domínio constringida por acordos diferentes entre as operadoras.

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, em 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 remessa de informação de VPN e pedidos de conexão de acordo com outra concretização da presente invenção;

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 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.

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 é baseada em três atividades de parte. Uma parte se relaciona à provisão de informação de VPN de domínio, incluindo em sua versão mais básica, identidade de VPN de VPNs disponíveis no domínio respectivo. Outra parte se relaciona à pesquisa por uma VPN específica para se conectar. Isto é, em outras palavras, um casamento entre uma VPN pedida e informação de VPN de domínio provida. Em algumas concretizações, este procedimento de casamento inclui transferência de informação de VPN de domínio ou informação derivada dela para outros domínios. Em outras concretizações, um pedido para uma certa VPN é transferido ao invés entre domínios. A parte final se relaciona à reconfiguração atual de uma VPN. As idéias fundamentalmente novas da presente invenção são principalmente envolvidas em dois primeiros estágios.

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 adicionalmente 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

17

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.

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 que estão disponíveis pelas conexões de inter-domínio. Se mais informação completa estiver disponível, o nó de controle de VPN também pode determinar por exemplo identidades de nó de borda ao qual estas VPNs diferentes estão disponíveis, qualidade de serviço de VPN, etc. A informação de VPN assim alcançada é agora uma propriedade do domínio visinho e pode, se permitido pelo SLA, ser usada para atividades nesse 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.

Em uma concretização alternativa, distribuição de informação entre domínios pode ser executada de uma maneira por impulso radiodifundido. A informação de VPN de domínio é então enviada diretamente a um, vários ou todos dos outros nós de controle de VPN nos outros domínios no sistema total, não restringidos aos domínios vizinhos. Isto significa que a informação de VPN de domínio não é remetida em uma cadeia como na outra concretização, mas meramente radiodifundida pelo sistema. A disponibilidade de tal remessa de pedido direta pode ser regulada por SLAs de domínio.

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 poderia por exemplo ser que uma mudança de algum tipo ocorreu em um domínio ou, como sendo descrito abaixo, um pedido para achar uma VPN particular é emitido. Em outras palavras, esta alternativa pode ser descrita como um mecanismo de impulso ativado para distribuição de dados.

No caso que a informação é trocada quando ativada por um pedido para achar uma certa VPN, a informação trocada pode ser restringida àquela VPN e pode até mesmo não necessariamente ser armazenada para uso posterior. Este é um exemplo de um mecanismo de tração para distribuição de dados.

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. Em uma concretização particular, a conexão iniciará um procedimento de "plugar-e-ligar", que achará automaticamente a VPN apropriada e pelo menos sugerirá como arranjar a configuração de VPN revisada. O nó de controle 43 identifica que um novo local de cliente 20' está conectado e investiga para qual VPN é pretendido.

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. Se houver um casamento, informação sobre a existência do casamento e preferivelmente também sobre em qual domínio a VPN existe e por quais conexões de inter-domínio a VPN é alcançável, está disponível. Em uma concretização, o trajeto para alcançar um nó de borda conectado à VPN pedida, se estiver disponível, é retornado ao nó de controle de VPN solicitante. 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. Outra 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.

O nó de controle de VPN 43 tem toda a informação necessária para achar a VPN pedida. Neste exemplo, a rota através de conexão de inter-domínio 12E parece muito simples para usar, mas por exemplo níveis de qualidade de serviço disponíveis podem mudar tais decisões. Nesta concretização particular, 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 até mesmo ativadas pelo próprio pedido.

Outra concretização particular da presente invenção é ilustrada na Figura 5. Aqui, a provisão de informação de VPN de intra-domínio inicial é executada exatamente como antes. Nesta concretização particular, porém, a informação de VPN de domínio não é trazida adiante a qualquer domínio vizinho, até mesmo em uma forma processada. Isto significa que os nós de controle de VPN 43 agora só têm informação sobre suas próprias VPNs de domínio. Quando o nó de controle de VPN 43 inicia um pedido de conexão do nó de controle de VPN 43 de seu próprio domínio 10E, só tem a informação sobre VPNs no próprio domínio prontamente disponível em seus próprios bancos de dados. Porém, o nó de controle de VPN 43 sabe a quais domínios está conectado e remete ao invés o pedido através da conexão de inter-domínio 12A-G para os domínios vizinhos. Isto é ilustrado pelas setas 32. Um nó de controle de VPN 43 recebendo tal pedido através de uma conexão de inter-domínio investiga seus próprios bancos de dados para ver se há quaisquer dados de interesse. Se não, uma nova remessa através de uma conexão de inter-domínio acontecerá até que informação sobre a VPN pedido seja alcançada. Esta informação então será devolvida ao nó de controle de VPN do domínio original 10E.

Esta concretização particular tem a vantagem que o sistema 1 inteiro não tem que ser atualizado em todo único nó de controle de VPN 43. Porém, ao invés, a procura da VPN será algo mais complicada.

Em uma concretização alternativa, o pedido de conexão de VPN é enviado diretamente a um, vários ou todos dos outros nós de controle de VPN nos outros domínios no sistema total, não restringido aos domínios vizinhos. Isto significa que o pedido não é remetido em uma cadeia como na outra concretização, mas meramente radiodifundido pelo sistema. A disponibilidade de tal remessa de pedido direta pode ser regulada por SLAs de domínio.

Figura 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. 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 casamento 49 investigando se uma identidade de uma VPN pedida casa com informação de VPN de domínio, é provida. O pedido de VPN pode ser recebido de outro domínio, de outro nó do próprio domínio ou um pedido de conexão de VPN 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. Uma seção de operação de VPN interna 41 tem funcionalidades para configurar conexões internas dentro do próprio domínio.

Figura 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. A informação de VPN

de domínio interna é nesta concretização particular armazenada em uma memória de dados 52. Esta informação é nesta concretização particular provida, como ilustrada 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 interna 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 internos 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. O banco de dados de entrada 58 atualiza o 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 também 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 vizinhos diferentes e armazenada em um 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.

Uma unidade de casamento 49 investigando se uma identidade de uma VPN pedida casa com informação de VPN de domínio, é provida. O pedido de VPN pode ser recebido de outro domínio, de outro nó do próprio domínio ou um pedido de conexão de VPN pode ser iniciado dentro do próprio nó de controle de VPN. Quando um casamento entre uma VPN pedida e a informação de VPN dos nós de controle de VPN é alcançado, uma reconfiguração de uma VPN de inter-domínio tem que ser executada. A implementação pode ser executada de muitos modos diferentes, usando procedimentos típicos conhecidos como tais na arte anterior. Uma concretização exemplificante será descrita abaixo, que assume que toda a informação de VPN está espalhada pelo sistema inteiro, isto é, semelhante ao que está ilustrado na Figura 4.

Depois de casamento do pedido de conexão de VPN para um usuário, a suposição é que todos os nós de controle de VPN em todos os domínios tem um banco de dados de VPN de onde achar VPNs no sistema. Em cada banco de dados de domínio há informação de "próximo salto" para cada ID de VPN não presentemente no domínio, que mostra o ID de domínio vizinho, onde este ID de VPN pode ser achado. No domínio vizinho, há tanto uma VPN já configurada para este ID de VPN, ou nova informação de

"próximo salto", onde achar o ID de VPN. Os bancos de dados diferentes nos domínios podem assim ser interpretados como "tabelas de roteamento de VPN", que mostram como achar trajetos para VPNs já configuradas. Para cada informação de "próximo salto" pode haver regras de política diferentes associadas. Dependendo das regras de política, o nó de controle de VPN em cada domínio pode escolher estabelecer conexões de VPN para um ou vários dos domínios de "próximo salto".

Um exemplo, ilustrado na Figura 7, mostra como a configuração de uma VPN de inter-domínio pode ser automatizada. Um novo local de cliente 20' no domínio 10E deverá ser conectado a 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 adquire um pedido, de algum modo, do cliente para 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, um casamento é achado entre o pedido de conexão e informação de VPN originada de outros domínios. O banco de dados mostra que a VPN 22A pode ser achada no "próximo salto" 10B, 10C e 10D, presentemente configurado e correndo em domínio 10A, 10C e 10D.

O nó de controle de VPN em domínio 10E escolhe só estabelecer a VPN pelo "próximo salto" 10B somente. 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 estabelece um envelope de VPN 72 para VPN 22A através da ligação 12D a nó de fronteira 18:2. Como a VPN 22A não está presente em domínio 10B, a

nó de controle de VPN em domínio 10B verifica seu banco de dados de VPN e vê que a VPN 22A pode ser achada no "próximo salto" 10A e 10C. O nó de controle de VPN em domínio 10B escolhe estabelecer a VPN pelo "próximo salto" 10A somente. Estabelece 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 estabelece 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 estabelecer 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, um pedido de conexão é iniciado. Este pedido relaciona-se a conectar um primeiro nó de borda em um primeiro domínio a uma VPN não presentemente disponível no primeiro domínio. Na etapa 212, informação de nó de domínio é coletada. Na etapa 214, uma identidade da primeira VPN é casada a identidades de VPN de informação de nó coletada. Baseado no resultado da etapa de casamento, a primeira VPN é configurada para incluir o primeiro nó de borda, na etapa 216. 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. Em particular, qualquer combinação de tração/impulso, inter/intra-domínio, comunicação radiodifundida/vizinha e informação/pedido é possível aplicar. A extensão da presente invenção está, porém, definida pelas reivindicações anexas.

28

REIVINDICAÇÕES

1. Método para configurar uma rede privada virtual de multi-domínio (22A-C) - VPN - dentro de uma rede de comunicação (1), a rede de comunicação (1) tendo pelo menos dois domínios (10A-E) interconectados um ao outro, e por meio de que os clientes são conectados a VPNs (22A-C) em nós de borda (14; 14') dos pelo menos dois domínios (10A-E), caracterizado pelo fato de que inclui as etapas de:

iniciar um pedido de conexão para conectar um primeiro nó de borda (14') em um primeiro domínio (10E) a uma primeira VPN (22A) não presentemente disponível no primeiro domínio (10E);

prover (24; 62) informação de VPN de domínio dentro dos pelo menos dois domínios;

a informação de VPN de domínio incluindo pelo menos identidade de VPN de VPNs disponíveis em domínio respectivo;

casar uma identidade da primeira VPN (22A) com identidades de VPN de um segundo domínio dos pelo menos dois domínios diferentes do primeiro domínio (10E); e

configurar a primeira VPN (22A) para incluir o primeiro nó de borda (14') baseado no resultado da etapa de casamento.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de casamento por sua vez inclui as etapas de:

enviar (32) um pedido de informação sobre existência da primeira VPN (22A) do primeiro domínio (10E) para um domínio adjacente (10B-D); e

comparar o pedido de informação com informação de VPN de domínio provida em um domínio diferente do primeiro domínio (10E).

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de casamento por sua vez inclui as etapas de:

enviar (32) um pedido de informação sobre a existência da

primeira VPN (22A) do primeiro domínio (10E) para um, vários ou todos os domínios (10B-D); e

comparar o pedido de informação com informação de VPN de domínio provida em um domínio diferente do primeiro domínio (10E).

4. Método de acordo com a reivindicação 2 ou 3, caracterizado pelo fato de que a etapa de casamento por sua vez inclui as etapas de:

retornar um reconhecimento ao primeiro domínio (10E) se uma casamento for achado.

5. Método de acordo com a reivindicação 2 ou 4, caracterizado pelo fato de que a etapa de casamento adicionalmente inclui a etapa de:

remeter o pedido de informação sobre existência da primeira VPN para domínio adjacente adicional se nenhum casamento for achado.

6. Método de acordo com quaisquer das reivindicações 2 a 5, caracterizado pelo fato de que o reconhecimento adicionalmente inclui dados representando pelo menos um de:

ID de domínio de domínio no qual a primeira VPN (22A) está disponível;

ID de nó de borda de nó de borda (14) no qual a primeira VPN (22A) está disponível;

informação sobre quais domínios que têm que ser transitados para alcançar o domínio no qual a primeira VPN (22A) está disponível; e

informação de roteamento para o nó de borda no qual a primeira VPN (22A) está disponível.

7. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de casamento por sua vez inclui as etapas de:

processar a informação de VPN de domínio em informação de VPN processada incluindo pelo menos uma identidade de VPN;

transferir (28) a informação de VPN processada entre domínios adjacentes;

comparar a identidade da primeira VPN (22A) com a informação de VPN processada transferida.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de casamento por sua vez inclui as etapas de:

processar a informação de VPN de domínio em informação de VPN processada incluindo pelo menos uma identidade de VPN;

transferir (28) a informação de VPN processada para um, vários ou todos os domínios;

comparar a identidade da primeira VPN (22A) com a informação de VPN processada transferida.

9. Método de acordo com a reivindicação 7 ou 8, caracterizado pelo fato de que a etapa de casamento inclui a etapa adicional de adicionalmente processar a informação de VPN processada transferida antes da etapa de comparação.

10. Método de acordo com a reivindicação 7 ou 9, caracterizado pelo fato de que a informação de VPN processada a ser transferida para outros domínios adicionalmente inclui informação de VPN processada recebida de domínios adjacentes.

11. Método de acordo com a reivindicação 10, caracterizado pelo fato de que a etapa de processamento inclui adição de informação de trânsito relativa à informação de VPN processada transferida de outros domínios ou informação derivadas dela.

12. Método de acordo com quaisquer das reivindicações 7 a 11, caracterizado pelo fato de que a informação de VPN processada adicionalmente inclui pelo menos um de:

ID de domínio de domínios (10A-E) nos quais VPNs diferentes (22A-C) estão disponíveis;

ID de nó de borda de nós de borda (14, 14') nos quais VPNs diferentes (22A-C) estão disponíveis;

informação sobre quais domínios (10A-E) que tem que ser transitados para alcançar o domínio (10A-E) no qual VPNs diferentes (22A-C) estão disponíveis; e

informação de roteamento para o nó de borda (14, 14') no qual VPNs diferentes (22A-C) estão disponíveis.

13. Método de acordo com quaisquer das reivindicações 7 a 12, caracterizado pelo fato de que a etapa de transferência de informação de VPN processada é executada em uma base regular.

14. Método de acordo com quaisquer das reivindicações 7 a 12, caracterizado pelo fato de que a etapa de transferência de informação de VPN processada é executada como uma resposta em mudanças de informação de domínio de VPN.

15. Método de acordo com quaisquer das reivindicações 7 ou 14, caracterizado pelo fato de que a etapa de transferência de informação de VPN processada é executada como uma resposta do pedido de conexão.

16. Método de acordo com quaisquer das reivindicações 1 a 15, caracterizado pelo fato de que a informação de domínio de VPN adicionalmente inclui identidades de cliente de clientes conectados aos nós de borda (14, 14') respectivos e VPNs associadas (22A-C).

17. Método de acordo com quaisquer das reivindicações 1 a 16, caracterizado pelo fato de que a informação de domínio de VPN adicionalmente inclui propriedades das VPNs (22A-C).

18. Método de acordo com a reivindicação 17, caracterizado pelo fato de que as propriedades da VPNs incluem pelo menos uma de:

propriedades de qualidade de serviço;

propriedades de criptografia;

propriedades de camada de transparência;

propriedades de envelopamento; e

propriedades de topologia.

19. Método de acordo com quaisquer das reivindicações 1 a 18, caracterizado pelo fato de que a etapa de prover informação de VPN de domínio por sua vez inclui coleta de dados de VPN de domínio de nós de borda dentro dos mesmos domínios.

20. Método de acordo com a reivindicação 19, caracterizado pelo fato de que a coleta de dados de VPN de domínio é executada de uma maneira centralizada em pelo menos um domínio.

21. Método de acordo com a reivindicação 19, caracterizado pelo fato de que a coleta de dados de VPN de domínio é executada de uma maneira distribuída em pelo menos um domínio.

22. Método de acordo com quaisquer das reivindicações 19 a 21, caracterizado pelo fato de que a coleta de dados de VPN de domínio é executada por um mecanismo de impulso.

23. Método de acordo com quaisquer das reivindicações 19 a 21, caracterizado pelo fato de que a coleta de dados de VPN de domínio é executada por um mecanismo de tração.

24. Rede de comunicação (1), caracterizada pelo fato de que inclui:

pelo menos dois domínios de rede (10A-E) sendo interconectados por conexões (12A-G) entre nós de fronteira (18);

meio para operar redes privadas virtuais (22A-C) - VPNs - dentro da rede de comunicação (1);

nós de borda (14, 14') conectados pelas VPNs (22A-C), por meio de que locais de cliente (20) das VPNs (22A-C) são conectados aos nós de borda (14, 14');

meio para iniciar um pedido de conexão para conectar um primeiro nó de borda (14') em um primeiro domínio (10E) a uma primeira VPN (22A) não presentemente disponível no primeiro domínio (10E);

nós de controle de VPN (43) em cada um dos pelo menos dois

domínios de rede (10A-E) incluindo meio (41) para prover informação de domínio de VPN;

a informação de domínio de VPN incluindo pelo menos identidade de VPN de VPNs disponíveis no domínio (10A-E);

meio para casar uma identidade da primeira VPN com identidades de VPN de um segundo domínio (10A-D) dos pelo menos dois domínios (10A-E) diferentes do primeiro domínio (10E); e

meio para configurar a primeira VPN (22A) para incluir o primeiro nó de borda (14') baseado na saída do meio para casamento.

25. Rede de comunicação de acordo com a reivindicação 24, caracterizada pelo fato de que o nó de controle de VPN (43) é um nó centralizado em pelo menos um domínio (10A-E).

26. Rede de comunicação de acordo com a reivindicação 24 ou 25, caracterizada pelo fato de que o nó de controle de VPN (43) é um nó distribuído em pelo menos um domínio (10A-E).

27. Rede de comunicação de acordo com a reivindicação 26, caracterizada pelo fato de que pelo menos uma parte do nó de controle de VPN distribuída (43) está em conexão lógica com um nó de borda (18), por meio de que comunicação entre a nó de controle de VPN distribuída (43) e domínios conectados pelo nó de fronteira (18) acontece pelo nó de fronteira (18).

28. Rede de comunicação de acordo com quaisquer das reivindicações 24 a 27, caracterizada pelo fato de que o nó de controle de VPN (43) inclui um armazenamento (54) para informação de VPN.

29. Rede de comunicação de acordo com quaisquer das reivindicações 24 a 28, caracterizada pelo fato de que o meio para casamento é distribuído em todos os domínios (10A-E), quais partes distribuídas por sua vez incluem:

meio de operação de pedido para enviar e receber pedidos de

informação sobre a existência de uma VPN particular para e de um domínio adjacente; e

meio para comparar pedidos de informação recebidos com informação de VPN de domínio provida de seu próprio domínio;

por meio de que, o meio de operação de pedido é adicionalmente arranjado para retornar um reconhecimento se um casamento for achado.

30. Rede de comunicação de acordo com quaisquer das reivindicações 24 a 28, caracterizada pelo fato de que o meio para casamento é distribuído em todos os domínios (10A-E), quais partes distribuídas por sua vez incluem:

meio de operação de pedido para enviar e receber pedidos de informação sobre a existência de uma VPN particular para e de um, vários ou todos os domínios; e

meio para comparar pedidos de informação recebidos com informação de VPN de domínio provida de seu próprio domínio;

por meio de que, o meio de operação de pedido é adicionalmente arranjado para retornar um reconhecimento se um casamento for achado.

31. Rede de comunicação de acordo com a reivindicação 29 ou 30, caracterizada pelo fato de que o meio de operação de pedido é adicionalmente arranjado para remeter um pedido de informação para domínios adjacentes adicionais se nenhum casamento for achado.

32. Rede de comunicação de acordo com quaisquer das reivindicações 24 a 28, caracterizada pelo fato de que o nó de controle de VPN (43) adicionalmente inclui:

primeiro processador (50) para processar a informação de VPN de domínio em informação de VPN processada, conectado ao armazenamento (54); e

meio para transferir a informação de VPN processada para outros domínios, conectado ao primeiro processador (50).

33. Rede de comunicação de acordo com a reivindicação 32, caracterizada pelo fato de que o nó de controle de VPN (43) adicionalmente inclui:

meio para receber informação de VPN processada de outros domínios;

segundo processador (56) para processar a informação de VPN processada recebida, conectado ao meio para receber e o armazenamento (54),

por meio de que a informação de VPN recebida processada pode ser armazenada no armazenamento (54).

34. Rede de comunicação de acordo com quaisquer das reivindicações 24 a 33, caracterizada pelo fato de que os nós de controle de VPN (43) em um domínio de rede (10A-E) incluem meio (41) para coletar informação de VPN de domínio de nós de borda no mesmo domínio.

35. Nó de controle de VPN (43) em um primeiro domínio de uma rede de comunicação (1) tendo pelo menos dois domínios (10A-E) e suportando redes privadas virtuais de multi-domínio (22A-C) - VPNs, clientes sendo conectados às VPNs (22A-C) em nós de borda (14, 14') dos pelos menos dois domínios (10A-E), o nó de controle de VPN (43) caracterizado pelo fato de que inclui:

meio (52, 62) para prover informação de VPN de domínio;

a informação de VPN de domínio incluindo pelo menos identidade de VPN de VPNs disponíveis dentro do primeiro domínio; e

meio para casar uma identidade de uma primeira VPN pedida com as identidades de VPN.

36. Nó de controle de VPN de acordo com a reivindicação 35, caracterizado pelo fato de adicionalmente incluir uma máquina de configuração (46) para conexões de VPN dentro do primeiro domínio.

37. Nó de controle de VPN de acordo com a reivindicação 35 ou 36, caracterizado pelo fato de adicionalmente incluir uma máquina de configuração (60) para conexões de VPN de inter-domínio envolvendo o primeiro domínio.

38. Nó de controle de VPN de acordo com quaisquer das reivindicações 35 a 37, caracterizado pelo fato de que o nó de controle (43) é um nó centralizado.

39. Nó de controle de VPN de acordo com a reivindicação 38, caracterizado pelo fato de compreender meio para comunicar com nós de controle de VPN em outros domínios por nós de fronteira.

40. Nó de controle de VPN de acordo com a reivindicação 38, caracterizado pelo fato de compreender meio para comunicar por conexões de sinal de controle de VPN dedicadas (47) com nós de controle de VPN em outros domínios.

41. Nó de controle de VPN de acordo com quaisquer das reivindicações 35 a 37, caracterizado pelo fato de que o nó de controle (43) é um nó distribuído.

42. Nó de controle de VPN de acordo com a reivindicação 41, caracterizado pelo fato de que pelo menos uma parte do nó de controle distribuído (43) está em conexão lógica com um nó de fronteira (18) por qual comunicação de dados a domínios vizinhos acontece.

43. Nó de controle de acordo com quaisquer das reivindicações 35 a 42, caracterizado pelo fato de que o nó de controle (43) inclui um armazenamento (54) para informação de VPN.

44. Nó de controle de acordo com a reivindicação 43, caracterizado pelo fato de que o armazenamento (54) para informação de VPN é centralizado.

45. Nó de controle de acordo com a reivindicação 43, caracterizado pelo fato de que o armazenamento (54) para informação de

VPN é distribuído.

46. Nó de controle de VPN de acordo com quaisquer das reivindicações 35 a 45, caracterizado pelo fato de compreender meio para comunicar informação de VPN de domínio para e de outros domínios.

47. Nó de controle de VPN de acordo com quaisquer das reivindicações 35 a 45, caracterizado pelo fato de compreender meio para receber um pedido de VPN, por meio do qual o meio para casamento inclui meio para enviar um reconhecimento se um casamento for achado.

48. Nó de controle de VPN de acordo com a reivindicação 47, caracterizado pelo fato de compreender meio para remeter um pedido de VPN para outros domínios se nenhum casamento for achado pelo meio para casamento.

49. Nó de controle de acordo com quaisquer das reivindicações 35 a 45, caracterizado pelo fato de compreender meio (41) para coletar informação de VPN de domínio de nós de borda no mesmo domínio.

50. Nó de controle de acordo com a reivindicação 49, caracterizado pelo fato de que o meio (41) para coletar informação de domínio de VPN é arranjado para operar de acordo com um mecanismo de impulso.

51. Nó de controle de acordo com a reivindicação 49, caracterizado pelo fato de que o meio (41) para coletar informação de domínio de VPN é arranjado para operar de acordo com um mecanismo de tração.

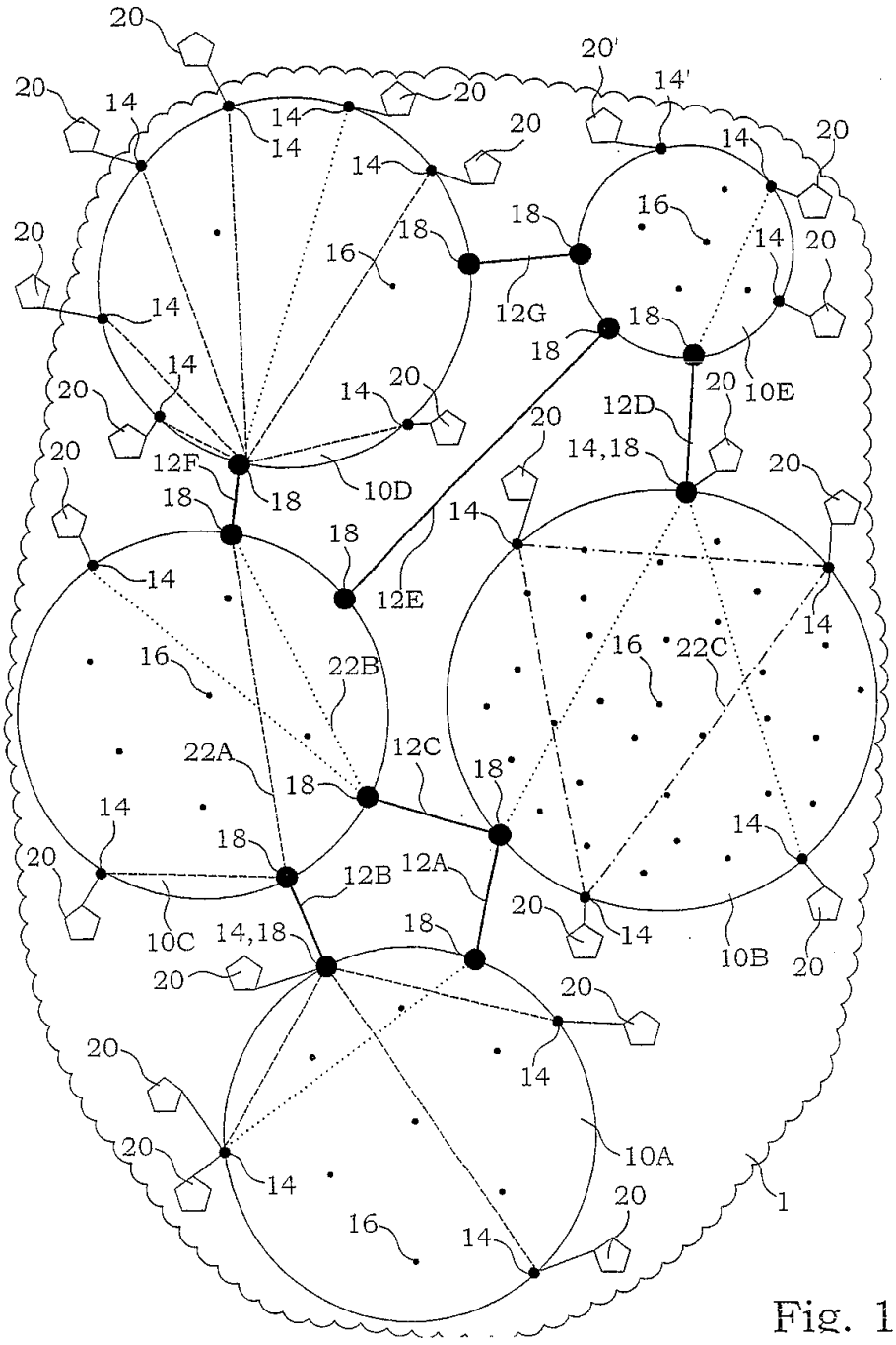

Fig. 1

39

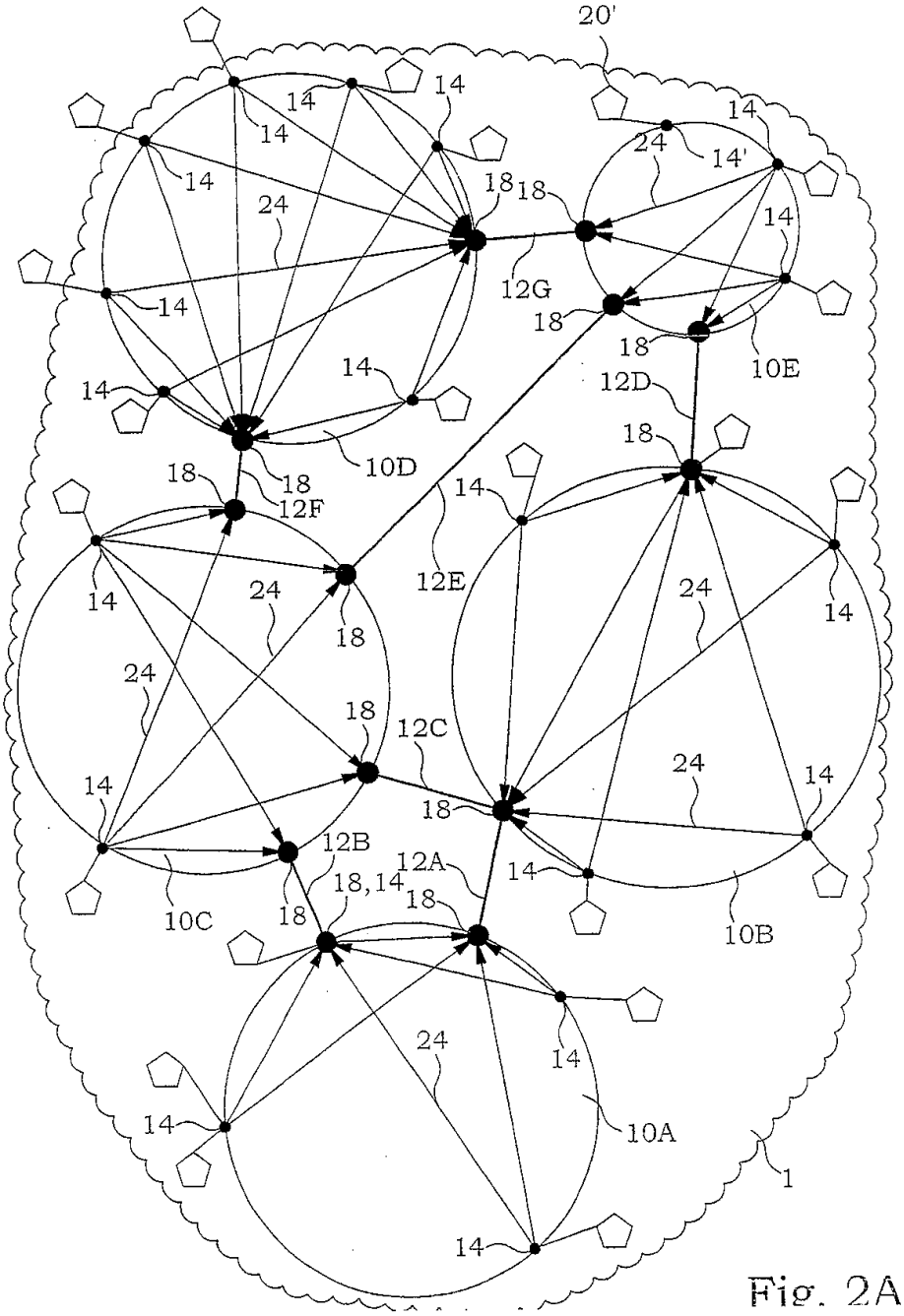
20'
14
24
14'
18
12G
10E
12D
10D
12F
12E
12C
12B
12A
18,14
10C
10B
10A
1

Fig. 2A

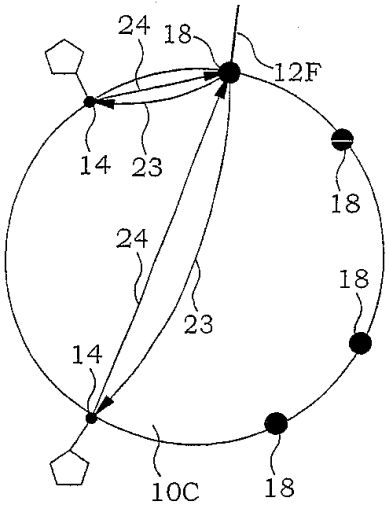

Fig. 2B

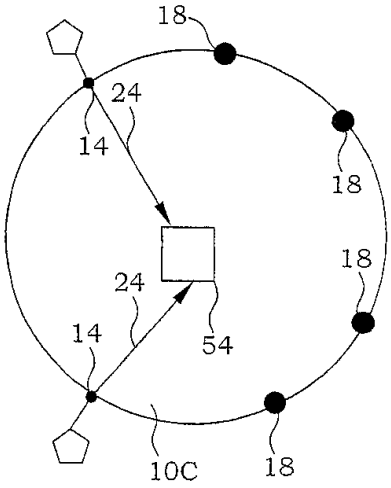

Fig. 2C

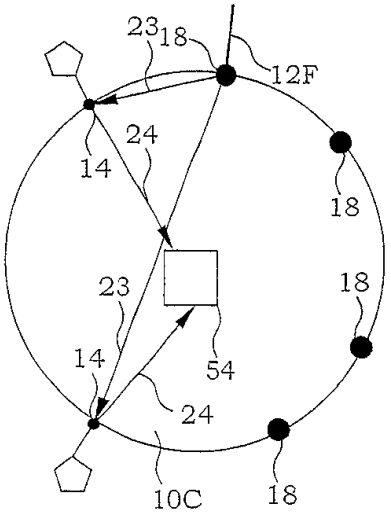

Fig. 2D

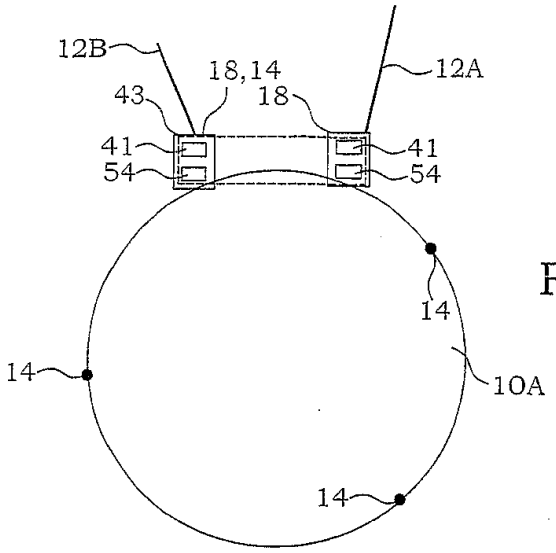
12B
18,14
12A
43
18
41
41
54
54
14
14
10A
14

Fig. 3A

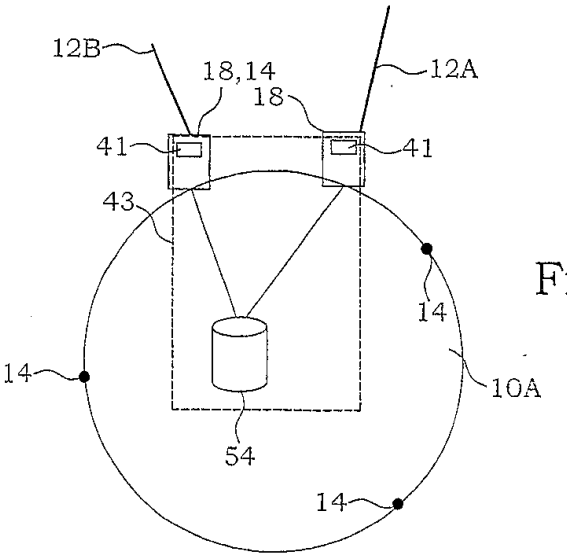
12B
18,14
12A
18
41
41
43
14
14
10A
54
14

Fig. 3B

42

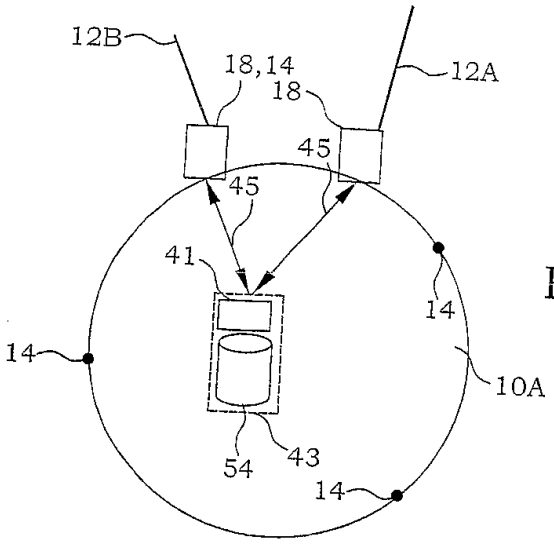

Fig. 3C

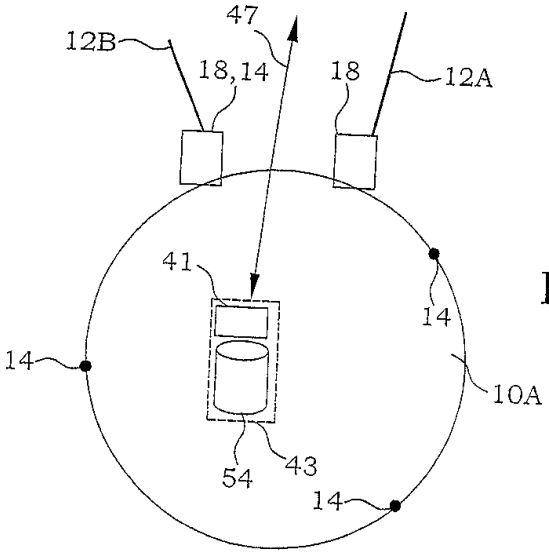

Fig. 3D

43

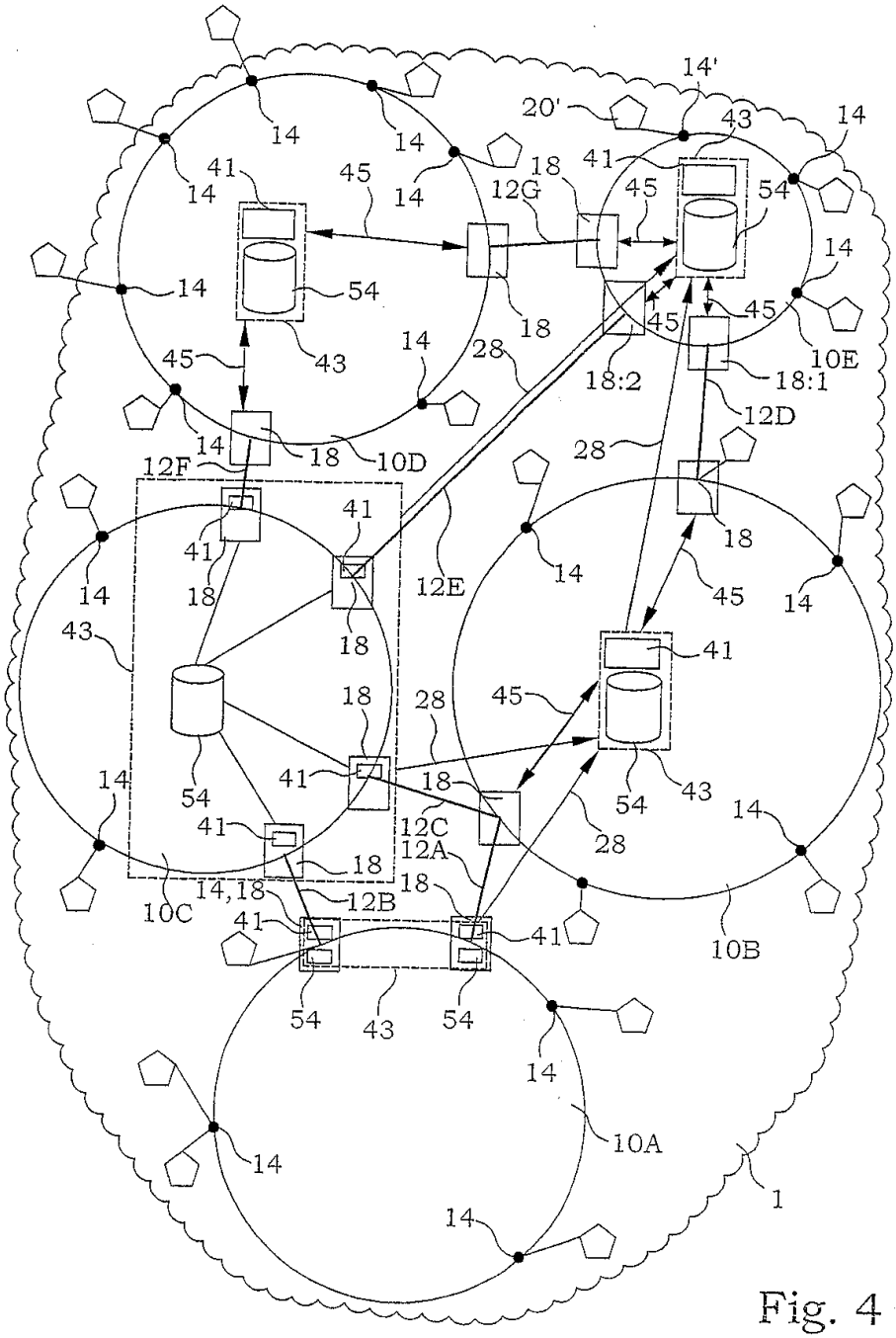
14'
20'
43
14
41
45
18
12G
54
14
28
18:2
18:1
10E
12D
12F
10D
12E
12C
12A
12B
14,18
10C
10B
10A
1

Fig. 4

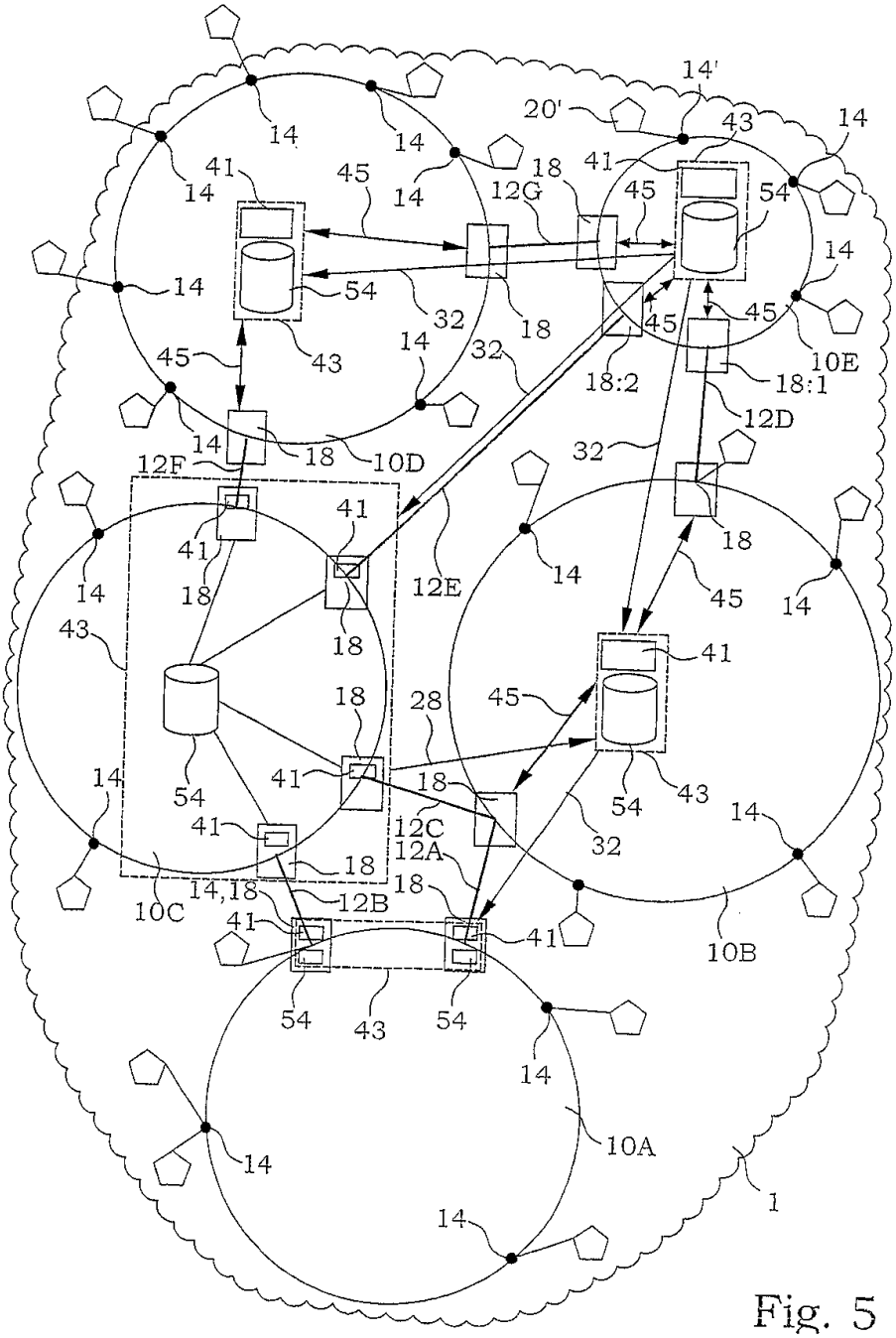
14'
20'
43
14
41
45
14
18
12G
54
32
18:2
18:1
10E
12D
12F
10D
12E
28
12C
12A
12B
14,18
10C
10B
10A
1

Fig. 5

45

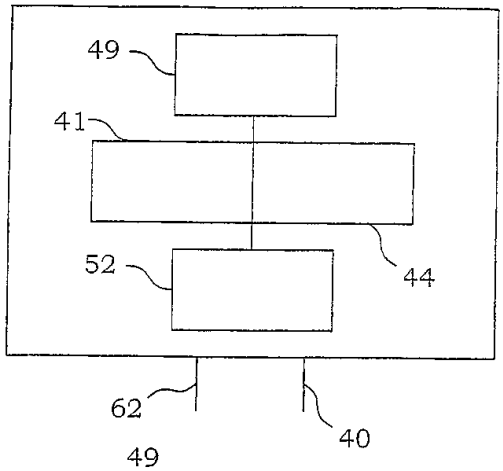

Fig. 6A

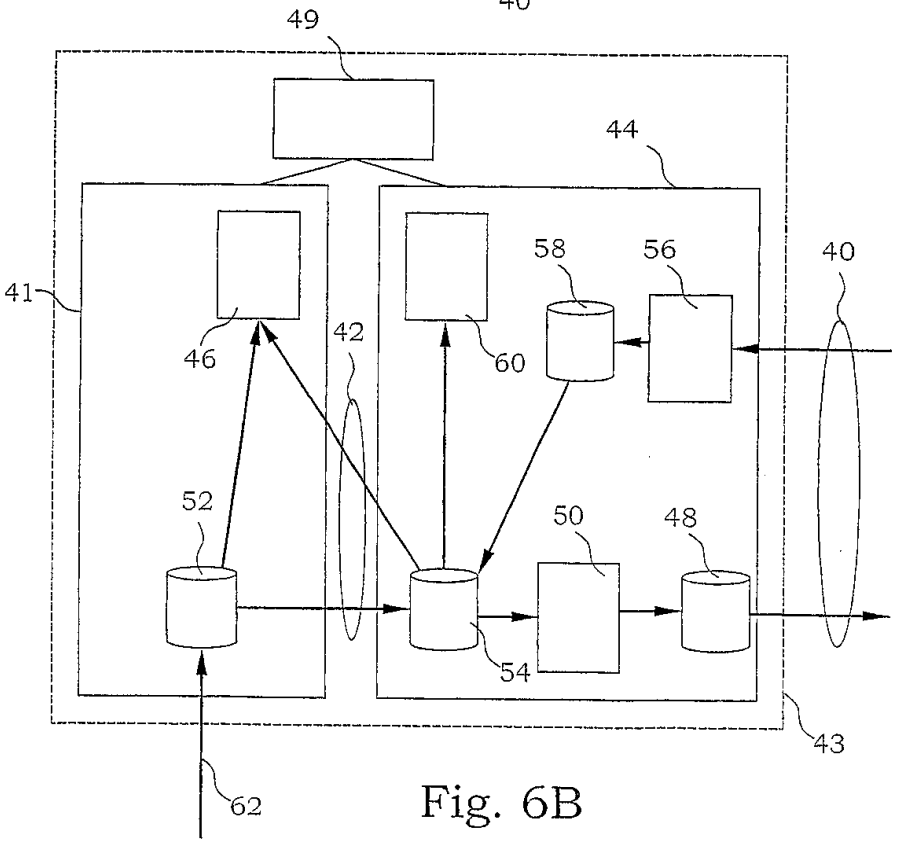

Fig. 6B

46

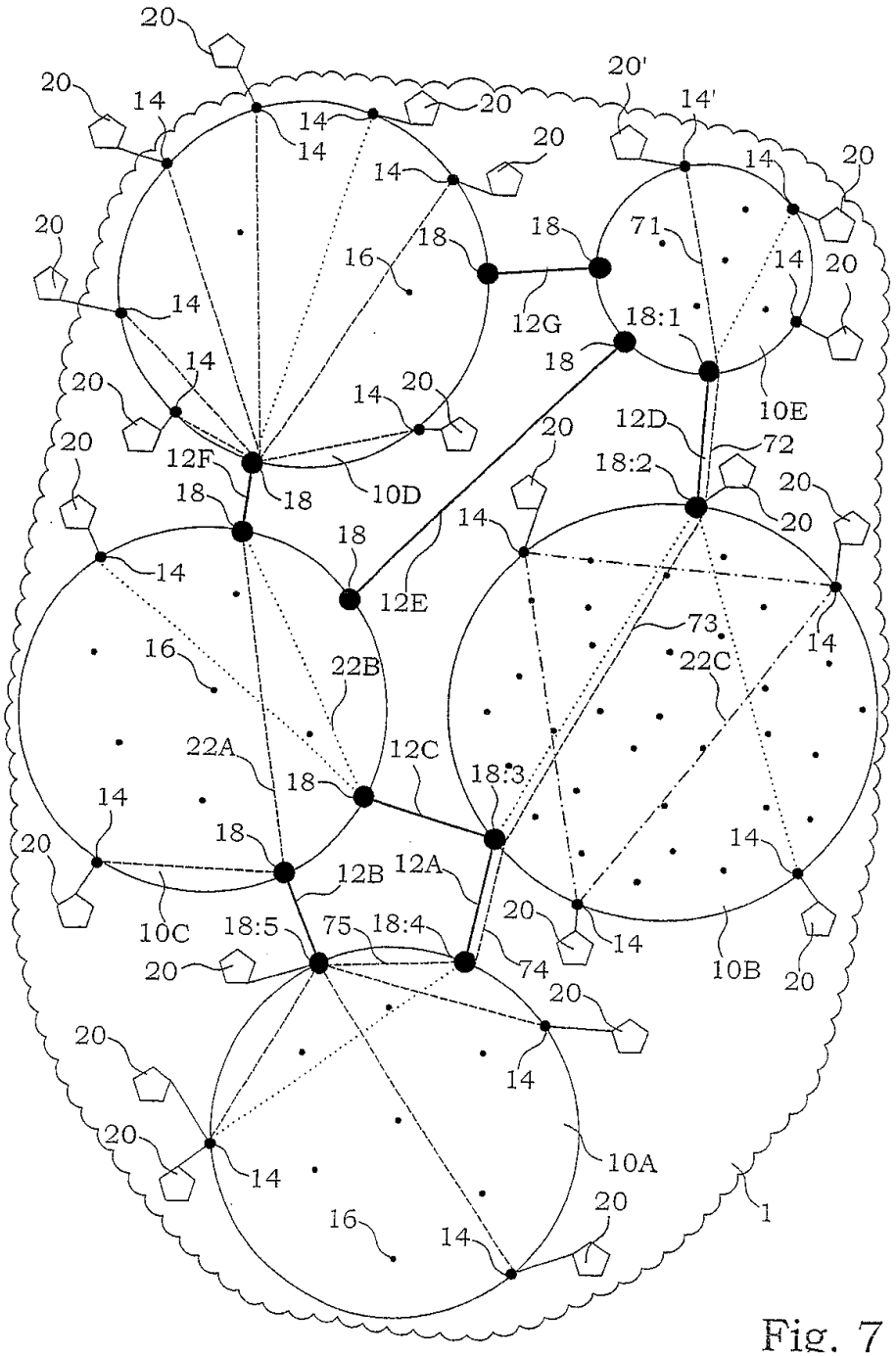
20
20'
14
14'
16
18
18:1
18:2
18:3
18:4
18:5
71
72
73
74
75
12A
12B
12C
12D
12E
12F
12G
10A
10B
10C
10D
10E
22A
22B
22C
1

Fig. 7

47

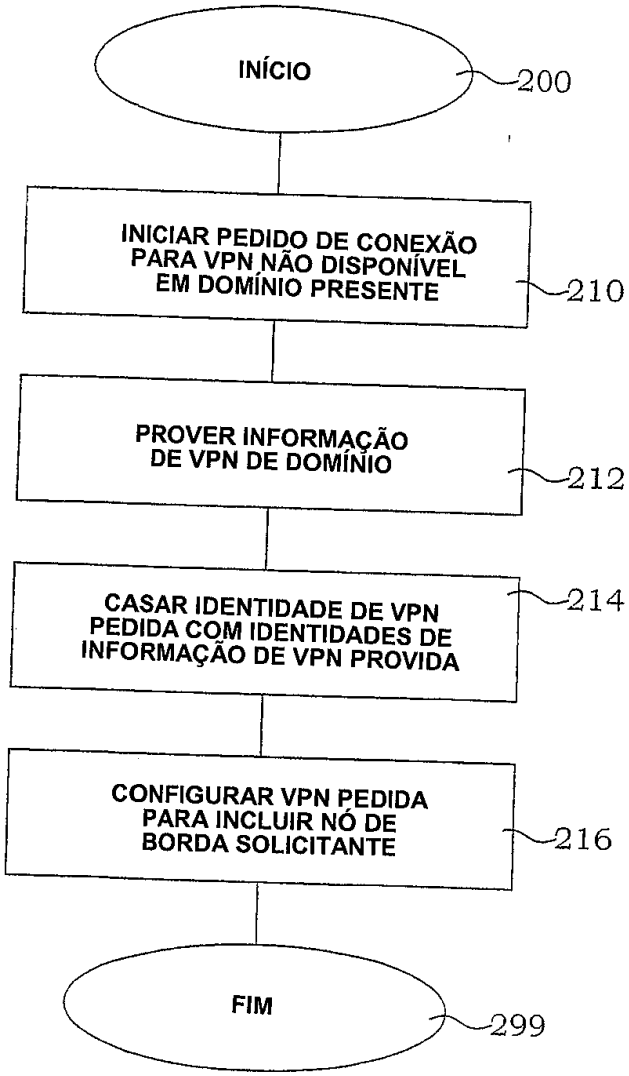
INÍCIO
200
INICIAR PEDIDO DE CONEXÃO PARA VPN NÃO DISPONÍVEL EM DOMÍNIO PRESENTE
210
PROVER INFORMAÇÃO DE VPN DE DOMÍNIO
212
CASAR IDENTIDADE DE VPN PEDIDA COM IDENTIDADES DE INFORMAÇÃO DE VPN PROVIDA
214
CONFIGURAR VPN PEDIDA PARA INCLUIR NÓ DE BORDA SOLICITANTE
216
FIM
299

Fig. 8