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

(11) **PI 0505394-3 B1**

(22) Data do Depósito: 06/12/2005

(45) Data de Concessão: 16/01/2018

(54) Título: "MÉTODO E SISTEMA PARA PROPORCIONAR UM DISPOSITIVO DE COMPUTAÇÃO DO CLIENTE COM UM ENDEREÇO DE REDE USADO EM UM AMBIENTE DE COMPUTAÇÃO DO CLIENTE/SERVIDOR"

(51) Int.Cl.: G06F 17/30

(30) Prioridade Unionista: 08/12/2004 US 11/007.122

(73) Titular(es): MICROSOFT TECHNOLOGY LICENSING, LLC

(72) Inventor(es): CALVIN C. CHOE; VIVEK P. KAMATH

Relatório Descritivo da Patente de Invenção para **"MÉTODO E SISTEMA PARA PROPORCIONAR UM DISPOSITIVO DE COMPUTAÇÃO DO CLIENTE COM UM ENDEREÇO DE REDE USADO EM UM AMBIENTE DE COMPUTAÇÃO DO CLIENTE/SERVIDOR".**

ÁREA TÉCNICA

[001] A presente invenção refere-se, de maneira geral, a comunicações via computador e, de maneira particular, ao provisionamento remoto de um dispositivo de cliente.

ANTECEDENTES DA INVENÇÃO

[002] No passado, após um computador ser configurado para seu ambiente de trabalho, essa configuração raramente ou nunca se alterava. Porém, no ambiente dinâmico de computação atual, um computador pode precisar ter sua configuração alterada com freqüência. Quando, por exemplo, um computador portátil se move de uma rede sem fio para outra, ele pode alterar seu endereço de rede para um mais compatível com a nova rede. Além disto, quando um computador se une temporariamente a um grupo de comunicação entre redes ad hoc, políticas administrativas e de segurança podem demandar que o computador altere sua configuração para uma mais aceitável ao grupo ad hoc. Em um terceiro exemplo, alguns computadores alteram sua configuração, pelo menos seu endereço de rede, a cada vez que eles acessam a Internet através do Provedor de Serviços da Internet (ISP).

[003] Protocolos têm sido desenvolvidos para prestar suporte a vários aspectos da configuração dinâmica. Como um exemplo, DHCP, o Protocolo de Configuração Dinâmica do Hospedeiro, fornece, dentre outras informações de configuração de rede, um endereço IP (Protocolo da Internet) a um computador solicitante. O DHCP usa um modelo de cliente/ servidor, onde um computador de cliente, precisando de um endereço IP, solicita o mesmo a um servidor DHCP. O servidor DHCP,

em alguns casos fornecido por um ISP, controla um conjunto de endereços IP. Após receber o pedido do cliente, o servidor DHCP executa um dentre três modos de alocação de endereços. No modo de "alocação automática", o servidor DHCP escolhe um endereço IP não usado a partir de seu conjunto e o atribui permanentemente ao cliente solicitante. No modo de "alocação manual", um administrador de rede escolhe o endereço. De maneira mais interessante para a configuração dinâmica, no modo de "alocação dinâmica", o servidor DHCP atribui um endereço IP atualmente não usado ao cliente, mas este endereço dinâmico é válido somente por um período limitado de tempo, conforme definido pelo servidor DHCP, ou até que o cliente renuncie explicitamente ao uso do endereço. Qualquer que seja o modo de alocação usado, o servidor DHCP responde ao pedido do cliente, informando ao cliente o endereço IP a ele atribuído juntamente com, no caso da alocação dinâmica, o período de tempo da atribuição. Se o servidor DHCP não puder fornecer um endereço IP (possivelmente porque todos os endereços no seu conjunto estão atualmente em uso), então o servidor DHCP informa ao cliente este fato, e o cliente precisa aguardar até mais tarde para acessar a rede.

[004] Em qualquer sistema dinâmico de computação, a facilidade de configuração deve ser equilibrada com preocupações de segurança. Muitas instituições estabelecem uma rede dinâmica para realizar o trabalho interno (a saber, privado) na instituição, e a instituição pode ficar comprometida, caso seja permitido que um computador não autorizado seja configurado dinamicamente, e se conecte à rede. Embora sendo úteis, protocolos de configuração dinâmica, incluindo o DHCP, são em geral deficientes na área de segurança. Por dependerem intensamente de processos de pós-configuração (tais como mecanismos de autenticação baseados em chave de criptografia) para proteger a sua rede, alguns servidores de configuração permitem inadvertidamen-

te clientes invasores. Embora os esquemas de pós-configuração normalmente operem, como divulgado, para limitar o acesso e o possível danos de clientes invasores, ainda assim um certo dano pode ser causado por um invasor, mesmo antes dele ser forçado a se submeter, e presumivelmente fracassar, a um esquema de proteção de pós-configuração.

Sumário da Invenção

[005] Com vistas ao anterior, a presente invenção fornece um mecanismo para provisionar com segurança um cliente, por meio de autenticação daquele cliente durante um processo de configuração dinâmica. Ao invés de depender de esquemas de autenticação de pós-configuração, a presente invenção combina segurança e configuração dinâmica em um esquema unificado.

[006] Qualquer dispositivo de cliente tentando acessar uma rede pode solicitar informações de configuração por parte de um servidor de configuração associado àquela rede, mas o servidor não atende ao pedido, até que o cliente tenha sido autenticado com sucesso como um dispositivo autorizado para receber informações de configuração para a rede. Em uma modalidade, o servidor de configuração pode provisionar o cliente com informações de configuração temporárias, por exemplo, um endereço de rede temporário, que permita ao cliente prosseguir com o processo de autenticação, mas que negue pleno acesso do cliente à rede. Após autenticação bem sucedida, o servidor pode dar ao cliente novas informações de configuração não-temporária, ou pode alterar o estado das informações já fornecidas, de temporário a um estado fornecendo pleno acesso.

[007] Em uma modalidade, a presente invenção usa um protocolo de configuração dinâmica existente, tal como o DHCP, sem a necessidade de alterar esse protocolo. Mensagens usadas no processo de autenticação são transportadas dentro das mensagens de configura-

ção existentes, por exemplo dentro do campo das opções nas mensagens DHCP.

[008] Em outra modalidade, a presente invenção aplica protocolos de segurança existentes a um ambiente de configuração dinâmica. O Protocolo de Autenticação Extensível (EAP), por exemplo, pode ser usado sem modificação como uma estrutura de autenticação para muitas das tarefas de segurança da presente invenção.

[009] Combinando as modalidades dos dois parágrafos anteriores, mensagens EAP podem ser transportadas no campo das opções das mensagens DHCP. Quando um cliente solicita informações de configuração, ele inclui dentro de sua mensagem DHCP uma opção de capacitação do EAP. O EAP é continuado, até que o cliente tenha sido autenticado no servidor DHCP (e, em alguns cenários, o servidor tenha sido autenticado no cliente). Neste momento, o servidor DHCP pode responder ao pedido inicial, fornecendo as informações de configuração solicitadas.

[0010] Fazendo parte de um mecanismo de provisionamento dinâmico e seguro, um servidor de configuração pode aplicar políticas definidas para a rede por ele servida. Por exemplo, as informações de configuração fornecidas podem ser limitadas em duração ou em âmbito.

Breve Descrição dos Desenhos

[0011] Embora as reivindicações apensas descrevam os aspectos da presente invenção em detalhes, a invenção, em conjunto com seus objetivos e vantagens, pode ser mais bem compreendida a partir da descrição detalhada a seguir tomada em conjunto com os desenhos anexos, onde:

a Fig. 1 é um diagrama de blocos mostrando um dispositivo de cliente tentando se conectar a uma rede que é "protegida" por um servidor de configuração segura;

A Fig. 2 é um diagrama esquemático ilustrando, de um modo geral, um dispositivo de computação exemplificante, que dá suporte à presente invenção;

As Figs. 3a a 3c, em conjunto, constituem um fluxograma lógico, mostrando uma comunicação exemplificante entre um cliente e um servidor de configuração segura;

As Figs 4a e 4b, em conjunto, constituem um fluxograma de comunicações mostrando como mensagens DHCP e EAP podem ser usadas para implementar um esquema de configuração segura; e

A Fig. 5 é um diagrama da estrutura de dados de uma mensagem EAP transportada dentro do campo das opções de uma mensagem DHCP.

Descrição Detalhada da Invenção

[0012] Com relação aos desenhos, onde algarismos de referência semelhantes se referem a elementos semelhantes, a presente invenção é ilustrada, como sendo implementada em um ambiente de computação adequado. A descrição a seguir é baseada em modalidades da invenção, e não deve ser considerada como limitadora da invenção, com vistas a modalidades alternativas, que não sejam aqui explicitamente descritas.

[0013] Na descrição a seguir, o ambiente envolvendo a presente invenção é descrito com referência a atos e representações simbólicas que são realizadas por um ou mais dispositivos de computação, salvo se de outro modo indicado. Neste sentido, deverá ficar claro que tais atos e operações, que são algumas vezes citados, como sendo executados por computador, incluem a manipulação pela unidade de processamento do dispositivo de computação de sinais elétricos representando dados de uma forma estruturada. Essa manipulação transforma os dados, ou os mantém em locais no sistema de memória do dispositivo de computação, que configura ou, de outra forma, altera a

operação do dispositivo, de uma maneira óbvia para as pessoas versadas na técnica. As estruturas de dados, onde os dados são mantidos, são posições físicas da memória que possuem propriedades específicas definidas pelo formato dos dados. Porém, embora a invenção esteja sendo descrita no contexto anterior, ela não pretende ser limitadora, conforme as pessoas versadas na técnica deverão perceber que vários atos e operações aqui a seguir descritos podem ser também implementados em hardware.

[0014] A Fig. 1 é útil para apresentar um panorama de vários aspectos da presente invenção. Uma discussão mais detalhada se segue com referência às outras figuras. Uma rede segura 100 é mostrada na Fig. 1. Aqui, *segura* significa simplesmente que a rede 100 é vedada a usuários não autorizados. A segurança é garantida por um conjunto de parâmetros de configuração. Os dispositivos 102 já na rede 100 possuem os corretos parâmetros de configuração e podem, assim, se comunicar livremente entre si. Um elemento estranho, como o cliente de configuração 106, não possui um conjunto correto de parâmetros de configuração e, assim, não pode se comunicar com esses dispositivos 102. Devido ao fato do cliente de configuração 106 querer se conectar à rede 100, ele busca admissão através do servidor de configuração segura 104 que está "protegendo" a rede 100. Como uma porta de comunicação para a rede 100, qualquer dispositivo externo pode se comunicar livremente com o servidor de configuração segura 104.

[0015] Após a recepção do pedido do cliente de configuração 106 para se conectar à rede 100, mas antes de provisionar o cliente de configuração 106 com um conjunto correto de parâmetros de configuração, o servidor de configuração segura 104 força o cliente de configuração 106 a se autenticar, isto é, a provar que ele é um dispositivo autorizado a se conectar à rede 100. Como essa autenticação é inicialmente definida está além do escopo da presente invenção, mas nu-

merosos processos são bastante conhecidos na técnica.

[0016] O cliente de configuração 106 prossegue comprovando a sua identidade ao servidor de configuração segura 104. Exemplos detalhados deste processo de autenticação acompanham as Figs. 3a a 3c, 4a, 4b, e 5. Em algumas redes, o servidor de configuração segura também comprova a sua identidade ao cliente de configuração solicitante. Esta autenticação bidirecional, ou mútua, aumenta a segurança dessas redes, impedindo que um dispositivo invasor represente o servidor de configuração segura da rede.

[0017] Se o processo de autenticação for concluído com sucesso, então o servidor de configuração segura 104 sabe que o cliente de configuração 106 está autorizado a se conectar à rede 100. O servidor de configuração segura 104, então, fornece um conjunto apropriado de parâmetros de configuração ao cliente de configuração 106, e o cliente de configuração 106 usa esses parâmetros para se conectar à rede 100 e para se comunicar livremente com os outros dispositivos 102 já na rede 100.

[0018] De modo eventual, o cliente de configuração 106 sai da rede 100. Isto pode ser a critério do cliente de configuração 106, ou um conjunto de parâmetros de configuração a ele fornecido pode expirar. Neste caso, esses parâmetros de configuração não são mais válidos e, sempre que o cliente de configuração 106 quiser se reconectar à rede 100, ele repete o processo acima.

[0019] O cenário da Fig. 1 é intencionalmente simplificado, a fim de enfocar aspectos relevantes da presente invenção. O servidor de configuração segura 104 da Fig. 1 pode, em algumas redes, ser na verdade um servidor de configuração operando com um servidor de segurança distinto. Além disto, o servidor de configuração segura 104 (de qualquer descrição), na verdade, pode não residir na rede 100: Um agente de relé situado na rede 100 pode transferir mensagens de con-

figuração e autenticação a um servidor de configuração segura, localizado a distância. Agentes de relé eliminam a necessidade de ter um servidor de configuração segura em cada segmento de rede segura.

[0020] O cliente de configuração 106 e o servidor de configuração segura 104 da Fig. 1 podem ser de qualquer arquitetura. A Fig. 2 é um diagrama de blocos ilustrando, de maneira geral, um sistema de computador exemplificante que presta suporte à presente invenção. O sistema de computador da Fig. 2 é somente um exemplo de um ambiente adequado, e não pretende sugerir qualquer limitação quanto ao escopo de uso ou funcionalidade da invenção. O cliente 106 e o servidor de configuração segura 104 também não devem ser interpretados, como tendo qualquer dependência ou exigência a qualquer um ou combinação de componentes ilustrados na Fig. 2. A invenção é operacional em diversos outros ambientes ou configurações de computação para uso geral ou especial. Exemplos de sistemas, ambientes e configurações de computação bastante conhecidos e apropriados para uso com a invenção, incluem, mas não são limitados a, computadores pessoais, servidores, dispositivos portáteis ou laptops, sistemas multiprocessadores, sistemas baseados em microprocessador, dispositivos de interface Internet/ TV, eletrônicos programáveis por consumidor, PCs de rede, minicomputadores, computadores de grande porte, e ambientes computacionais distribuídos, que incluem qualquer um dos sistemas ou dispositivos acima. Nas suas configurações mais básicas, o cliente 106 e o servidor de configuração segura 104 incluem, tipicamente, pelo menos uma unidade de processamento 200 e memória 202. A memória 202 pode ser volátil (tal como RAM), não-volátil (tal como ROM ou memória *flash*), ou uma combinação das duas. Essa configuração mais básica é ilustrada na Fig. 2 pela linha tracejada 204. O cliente 106 e o servidor de configuração segura 104 podem ter aspectos e funcionalidades adicionais. Por exemplo, eles podem ainda possuir

armazenagem adicional (removível e/ou não removível) incluindo, mas não limitado a, fitas e discos magnéticos e óticos. Essa armazenagem adicional é ilustrada na Fig. 2 pela armazenagem removível 206 e armazenagem não-removível 208. A mídia de armazenagem em computador inclui mídia volátil e não-volátil, removível e não-removível, implementada em qualquer processo ou tecnologia para armazenagem de informações, tais como instruções legíveis por computador, estrutura de dados, módulos de programa, ou outros dados. A memória 202, armazenagem removível 206 e armazenagem não-removível 208, todas elas são exemplos de mídia de armazenagem em computador. A mídia de armazenagem em computador inclui, mas não é limitada à, RAM, ROM, EEPROM, memória *flash*, outra tecnologia de memória, CD-ROM, discos digitais versáteis (DVD), outra armazenagem ótica, cassetes magnéticos, fita magnética, armazenagem em disco magnético, outros dispositivos de armazenagem magnética, e qualquer outra mídia que possa ser usada para armazenar as informações desejadas e que possa ser acessada pelo cliente 106 ou pelo servidor de configuração segura 104. Qualquer uma dessas mídias de armazenagem em computador pode fazer parte do cliente 106 ou do servidor de configuração segura 104. O cliente 106 e o servidor de configuração segura 104 podem ainda conter canais de comunicação 210, que permitam a eles se comunicar com outros dispositivos, incluindo dispositivos em uma rede 100. Os canais de comunicação 210 são exemplos de mídia de comunicação. A mídia de comunicação incorpora tipicamente instruções legíveis por computador, estruturas de dados, módulos de programa, ou outros dados em um sinal modulado de dados, tal como uma onda portadora, ou outro mecanismo de transporte, e inclui qualquer mídia para transmissão de informações. O termo “sinal modulado de dados” significa um sinal que possui uma ou mais de suas características definidas ou alteradas, de modo a codificar informações no si-

nal. Para fins de exemplo, e não de limitação, a mídia de comunicação inclui mídia óptica, mídia ligada por fio, tal como redes ligadas por fio e conexões diretas com fio, e mídia sem fio, tal como mídia acústica, RF, infravermelha, e outras sem fio. O termo "*mídia legível por computador*", conforme aqui usado, inclui mídia de armazenagem e mídia de comunicação. O cliente 106 e o servidor de configuração segura 104 podem ainda possuir dispositivos de entrada 212, tais como uma tela sensível a toque, teclado, mouse, dispositivo para entrada de voz etc.. Dispositivos de saída 214 incluem os dispositivos propriamente ditos, tais como a tela sensível a toque, alto-falantes, e uma impressora, e módulos de processamento (muitas vezes chamados de "adaptadores") para acionamento desses dispositivos. Todos esses dispositivos são bastante conhecidos na técnica e não precisam ser aqui discutidos em detalhes. O cliente 106 e o servidor de configuração segura 104, cada um deles possui uma fonte de alimentação 216.

[0021] Nos aprofundando mais do que o panorama da Fig. 1, as Figs. 3a a 3c apresentam detalhes de esquemas de configuração segura exemplificantes, de acordo com a presente invenção. Para fins de ilustração, o fluxograma lógico dessas figuras inclui opções e variações que podem não se aplicar a uma determinada modalidade. De modo particular, as etapas nas figuras representam tarefas lógicas, e não correspondem necessariamente às mensagens individuais. Detalhes mais específicos de uma modalidade particular, incluindo trocas e formatos de mensagens, são discutidos com relação às Figs. 4a, 4b e 5.

[0022] A lógica da Fig. 3a começa na etapa 300, quando o cliente de configuração 106 solicita ao servidor de configuração segura 104 um conjunto de parâmetros de configuração que são válidos para uso na rede 100. Ao invés de atender imediatamente ao pedido, o servidor de configuração segura 104, na etapa 302, pede para que o cliente de

configuração 106 se autentique. Em algumas modalidades (ver especificamente a etapa 400 da Fig. 4a), o cliente de configuração 106 não espera que o servidor de configuração segura 104 solicite autenticação; ao invés disso, o cliente de configuração 106 inicia o processo de autenticação simultaneamente com seu pedido de configuração inicial.

[0023] Existem algumas configurações de rede, onde o cliente de configuração 106 precisa usar um conjunto válido de parâmetros de configuração, a fim de continuar a se comunicar com o servidor de configuração segura 104. Isto é parecido com um dilema: Por motivos de segurança, o servidor de configuração segura 104 não deseja prestar informações de configuração válidas ao cliente de configuração 106, até que o cliente 106 tenha se autenticado como um dispositivo autorizado para receber tais informações, mas o procedimento de autenticação não pode prosseguir, até que o cliente 106 possua um conjunto de parâmetros válidos. As etapas 304 e 306 apresentam uma solução para esse dilema, para algumas modalidades da presente invenção. Na etapa 304, o servidor de configuração segura 104 fornece um conjunto válido de parâmetros de configuração ao cliente de configuração 106, a fim de que o cliente 106 possa prosseguir no processo de autenticação. Porém, as informações de configuração prestadas, apesar de válidas, são “temporárias”, e são somente úteis durante a autenticação. Por exemplo, as informações de configuração podem incluir um endereço IP que indique o usuário do endereço, como não inteiramente autenticado. Na etapa 306, o cliente de configuração 106 recebe as informações de configuração temporárias e irá usá-las durante o restante do processo de autenticação. Em alguns casos, as informações de configuração temporárias impedem ao cliente de configuração 106 de conversar com qualquer dispositivo na rede 100, que não com o servidor de configuração segura 104. O cliente de configuração 106 é dito, como estando em “quarentena”.

[0024] Na etapa 308, o cliente de configuração 106 e o servidor de configuração segura 104 prosseguem no processo de autenticação. Muitos desses processos de autenticação são bastante conhecidos na técnica, e qualquer um deles pode ser aqui usado. Em algumas modalidades, o processo de autenticação particular a ser usado é negociado entre o cliente de configuração 106 e o servidor de configuração segura 104. Como acima citado com relação à Fig. 1, o processo de autenticação pode ser mútuo com o cliente de configuração 106 e o servidor de configuração segura 104, cada um autenticando-se ao outro.

[0025] Se o processo de autenticação falhar, então, é obvio que o acesso à rede 100 é negado ao cliente de configuração 106. Se o cliente de configuração 106 recebeu informações de configuração temporárias na etapa 306, a rede 100 está ainda protegida, devido ao uso limitado, ao qual essas informações podem ser colocadas. Se o processo de autenticação tiver sucesso, então na etapa 310 da Fig. 3b, o servidor de configuração segura 104 aplica políticas em vigor na rede 100, caso existentes, para decidir como prestar as informações de configuração solicitadas. Essas políticas podem, por exemplo, limitar a duração ou o escopo de uso das informações de configuração (por exemplo, que as informações sejam somente válidas para um "arrendamento" de uma hora).

[0026] Se possível, em seguida na etapa 312, o servidor de configuração segura 104 presta as informações de configuração solicitadas ao cliente de configuração 106, juntamente com informações sobre quaisquer limitações acerca do uso definido pela política na etapa 310. É obvio que, se a rede 100 tiver esgotado os recursos necessários para atender o pedido (por exemplo, todos os endereços IP atribuíveis já se encontram em uso), então o processo de configuração falha, muito embora o processo de autenticação tenha sido bem sucedido. Em algumas modalidades, a disponibilidade de recursos é checada, antes

de avançar com o processo de autenticação, e o servidor de configuração segura 104 pode negar o pedido de configuração nestas bases, ao invés de iniciar o processo de autenticação na etapa 302. Porém, isto não é preferido, porque ele presta informações confidenciais (de que a rede 100 está baixa em recursos) a um cliente de configuração 106, que não foi autenticado, e possa ser capaz de usar as informações em detrimento da rede 100.

[0027] A etapa 314 observa que se o cliente de configuração 106 for dotado de informações de configuração temporárias na etapa 304, então, em algumas modalidades, o servidor de configuração segura 104 pode optar por alterar simplesmente o estado dessas informações para não temporárias, ao invés de enviar um novo conjunto de parâmetros de configuração. O efeito é o mesmo em qualquer um dos casos.

[0028] Com a autenticação concluída e com as informações de configuração não temporárias em mãos, o cliente de configuração 106 é agora um dispositivo na rede 100 e, na etapa 316 da Fig. 3c, pode se comunicar com os outros dispositivos 102 (sujeito a quaisquer limitações de política impostas sobre as informações de configuração prestadas). Isto prossegue até a etapa 318, onde o cliente de configuração 106 opta por abrir mão das informações de configuração prestadas, ou um arrendamento das informações expira. No último caso, o servidor de configuração segura 104 identifica as informações de configuração prestadas como inválidas. Em qualquer um dos casos, o cliente 106 sai da rede 100 e, se ele quiser continuar a se comunicar, repete o processo de configuração segura (etapa 320).

[0029] A discussão acompanhando as Figs. 3a a 3c é mantida em um alto nível, para ilustrar a amplitude de aplicação da presente invenção (que é, porém, finalmente definida pelo escopo das reivindicações, e não por quaisquer ilustrações neste relatório descritivo). Para apro-

fundar a discussão, as Figs. 4a e 4b apresentam uma modalidade específica da invenção.

[0030] Embora, de uma maneira geral, qualquer parte possa iniciar o processo de configuração segura, na etapa 400 da Fig. 4a, o cliente de configuração 106 inicia o processo, enviando uma mensagem de Descobrir DHCP ao servidor de configuração segura 104. Essa mensagem DHCP contém o pedido do cliente de configuração 106 para informações de configuração. Transportada dentro do campo de opções da mensagem Descobrir DHCP, existe uma comunicação de que o cliente de configuração 106 está preparado para usar EAP para se autenticar. Esses dois protocolos, DHCP e EAP, são bastante conhecidos na técnica, e assim seus detalhes não precisam ser aqui discutidos. Eles são definidos, respectivamente, nos Pedidos de Comentários 2131 e 3748 da Força Tarefa de Engenharia da Internet, que são aqui incorporados na sua totalidade para fins de referência.

[0031] Devido ao fato do servidor de configuração segura 104 não prestar informações de configuração a um cliente não-autenticado, ele responde na etapa 402 com uma mensagem de Oferecer DHCP contendo dentro do seu campo de opções uma mensagem EAP solicitando a identidade do cliente de configuração 106. O cliente de configuração 106 responde na etapa 404, através do envio de uma mensagem EAP contendo a sua identidade. A mensagem EAP, é, uma vez mais, contida no campo de opções de uma mensagem DHCP.

[0032] O EAP permite ao cliente de configuração 106 e ao servidor de configuração segura 104 negociar e usar qualquer um de uma variedade de mecanismos de autenticação. Nas etapas 406 e 408, as duas partes prosseguem através dos detalhes do EAP e do mecanismo de autenticação por elas escolhidos. Em algumas modalidades, o EAP não precisa ser alterado de nenhuma maneira para os objetivos da presente invenção e, assim, os detalhes do EAP conhecidos na técni-

ca também se aplicam aqui. Nas etapas 406 e 408, como nas etapas anteriores da Fig. 4a, mensagens EAP são transportadas dentro dos campos de opções das mensagens DHCP.

[0033] Se o processo de autenticação avançar até uma conclusão bem sucedida, então o servidor de configuração segura 104 aceita a autenticidade do cliente de configuração 106 e, na etapa 410 da Fig. 4b, envia uma mensagem de Sucesso do EAP transportada no campo de opções de uma mensagem de reconhecimento do DHCP. Essa mensagem DHCP inda inclui as informações de configuração solicitadas.

[0034] Quando o cliente de configuração 106 tiver concluído o seu trabalho na rede 100, ele abre mão das informações de configuração, por meio do envio de uma mensagem de Liberar DHCP na etapa 412.

[0035] A Fig. 5 é um diagrama da estrutura de dados exemplificante de uma mensagem DHCP 500 contendo, dentro de seu campo de opções 502, uma mensagem EAP 204. O núcleo da mensagem EAP é seu campo de dados 506. Através da combinação de um protocolo de configuração bastante conhecido, DHCP, com um protocolo da estrutura de autenticação bastante conhecido, EAP, modalidades da presente invenção fornecem segurança ao processo de configuração, sem demandar quaisquer mudanças em qualquer um dos protocolos.

[0036] Com vistas às muitas modalidades possíveis, às quais os princípios da presente invenção podem ser aplicados, deve ficar claro que as modalidades aqui descritas com respeito às figuras e desenhos pretendem ser somente ilustrativas, e não devem ser consideradas como limitadoras do escopo da invenção. As pessoas versadas na técnica deverão perceber que alguns detalhes de implementação, tais como protocolos de configuração e autenticação, são determinados por situações específicas. Embora o ambiente da invenção seja descrito em termos de módulos ou componentes de software, alguns pro-

cessos podem ser executados, de maneira equivalente, por componentes de hardware. Assim, a invenção aqui descrita contempla todas essas modalidades, conforme possam incidir no escopo das reivindicações a seguir e seus equivalentes.

REIVINDICAÇÕES

1. Método para proporcionar seguramente um dispositivo de computação do cliente (106) com um endereço de rede usado em um ambiente de computação do cliente/ servidor compreendendo:

solicitando, pelo dispositivo de computação cliente (106), um endereço de rede (300);

receber, por um dispositivo de computação do servidor (104), a solicitação do cliente para um endereço de rede;

tentar autenticar o dispositivo de computação do cliente (106) no dispositivo de computação (308) do servidor (104), **caracterizado pelo fato de que** um endereço de rede temporário é usado pelo dispositivo de computação do cliente (106) durante a tentativa de autenticação, em que a solicitação compreende o uso de DHCP, na qual a tentativa de autenticação compreende o uso de mensagens carregadas nos campos da opção DHCP (502);

colocar em quarentena o dispositivo de computação cliente (106), em que o endereço de rede temporário evita que o dispositivo de computação do cliente (106) converse com qualquer dispositivo em uma rede diferente do dispositivo de computação do servidor (104); e

se o dispositivo de computação do cliente (106) for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor, então:

identificar, por parte do dispositivo de computação do servidor (104), um endereço de rede que seja apropriado ao ambiente de computação do cliente/servidor e que não seja atualmente atribuído a um dispositivo de computação;

atribuir, por parte do dispositivo de computação do servidor (104), o endereço de rede identificado ao dispositivo de computação do cliente (106);

proporcionar, por parte do dispositivo de computação do

servidor (104), o endereço de rede atribuído ao dispositivo de computação do cliente (312); e

receber, por parte do dispositivo de computação do cliente (106), o endereço de rede atribuído.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** o endereço de rede atribuído é um endereço de Protocolo da Internet (IP).

3. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a tentativa de autenticar compreende usar o Protocolo de Autenticação Extensível (EAP).

4. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a solicitação compreende usar o DHCP, na qual a tentativa de autenticar compreende usar o EAP, e na qual as mensagens EAP são transportadas em campos de opções (502) do DHCP.

5. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a tentativa de autenticar é iniciada pelo dispositivo de computação do cliente (106).

6. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a tentativa de autenticar é iniciada pelo dispositivo de computação do servidor (104).

7. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a identificação de um endereço de rede é realizada mesmo se o dispositivo de computação do cliente (106) não for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor.

8. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** o endereço de rede temporário é atribuído pelo dispositivo de computação do servidor (104) ao dispositivo de computação do cliente (106) para um uso limitado.

9. Método, de acordo com a reivindicação 1, **caracteriza-**

do pelo fato de que, se o dispositivo de computação do cliente (106) for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor, então o endereço de rede atribuído é igual ao endereço de rede temporário.

10. Método, de acordo com a reivindicação 4, **caracterizado pelo fato de que** cada campo de opções (502) é parte de uma estrutura de dados, a estrutura de dados compreendendo:

um primeiro campo de dados contendo dados que representam uma mensagem DHCP (500), a mensagem DHCP compreendendo um segundo campo de dados;

o segundo campo de dados contendo dados que representam um campo de opções DHCP (502), o campo de opções DHCP compreendendo um terceiro campo de dados; e

o terceiro campo de dados contendo dados que representam uma mensagem EAP (504).

11. Método, de acordo com a reivindicação 10, **caracterizado pelo fato de que** a mensagem DHCP no primeiro campo de dados é selecionada a partir do grupo que consiste em: DHCPDISCOVER, DHCPOFFER e DHCPREQUEST.

12. Método, de acordo com a reivindicação 10, **caracterizado pelo fato de que** a mensagem EAP no terceiro campo de dados é selecionada a partir do grupo que consiste em: Solicitação, Resposta, Sucesso e Falha.

13. Método para proporcionar seguramente um dispositivo de computação do cliente (106) com um endereço de rede por parte de um dispositivo de computação do servidor (104), usado em um ambiente de computação do cliente/servidor compreendendo:

receber um pedido DHCP do cliente para um endereço de rede (300);

tentar autenticar o dispositivo de computação do cliente

para o dispositivo de computação de servidor (308), **caracterizado pelo fato de que** um endereço de rede temporário é atribuído ao dispositivo de computação do cliente (106) para uso durante a tentativa de autenticação, na qual a tentativa de autenticação compreende usar as mensagens transportadas nos campos de opção DHCP (502);

colocar em quarentena o dispositivo de computação do cliente (106), em que o endereço de rede temporário evita que o dispositivo de computação do cliente (106) converse com qualquer dispositivo em uma rede diferente do dispositivo de computação do servidor (104); e

se o dispositivo de computação do cliente (106) for autenticado conforme permitido para receber um endereço de rede no ambiente de computação do cliente/servidor, então:

identificar um endereço de rede que seja apropriado ao ambiente de computação do cliente/ servidor e que não seja atualmente atribuído a um dispositivo de computação;

atribuir o endereço de rede identificado ao dispositivo de computação do cliente (106); e

proporcionar o endereço de rede atribuído ao dispositivo de computação do cliente (106).

14. Método, de acordo com a reivindicação 13, **caracterizado pelo fato de que** o endereço de rede atribuído é um endereço IP.

15. Método, de acordo com a reivindicação 13, **caracterizado pelo fato de que** a tentativa de autenticar compreende o uso do EAP.

16. Método, de acordo com a reivindicação 15, **caracterizado pelo fato de que** as mensagens EAP são transportadas em campos de opções (502) do DHCP.

17. Método, de acordo com a reivindicação 13, **caracteri-**

zado pelo fato de que a tentativa de autenticar é iniciada pelo dispositivo de computação do servidor (104).

18. Método, de acordo com a reivindicação 13, **caracterizado pelo fato de que** a identificação de um endereço de rede é realizada, mesmo se o dispositivo de computação do cliente (106) não for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor.

19. Método, de acordo com a reivindicação 13, **caracterizado pelo fato de que**, se o dispositivo de computação do cliente (106) for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor, então o endereço de rede atribuído é igual ao endereço de rede temporário.

20. Método, de acordo com a reivindicação 15, **caracterizado pelo fato de que** cada campo de opções (502) é parte de uma estrutura de dados, a estrutura de dados compreendendo:

um primeiro campo de dados contendo dados que representam uma mensagem DHCP (500), a mensagem DHCP compreendendo um segundo campo de dados;

o segundo campo de dados contendo dados que representam um campo de opções DHCP (502), o campo de opções DHCP compreendendo um terceiro campo de dados; e

o terceiro campo de dados contendo dados que representam uma mensagem EAP (504).

21. Método, de acordo com a reivindicação 20, **caracterizado pelo fato de que** a mensagem DHCP no primeiro campo de dados é selecionada a partir do grupo que consiste em: DHCPDISCOVER, DHCPOFFER e DHCPREQUEST.

22. Método, de acordo com a reivindicação 20, **caracterizado pelo fato de que** a mensagem EAP no terceiro campo de dados é selecionada a partir do grupo que consiste em: Solicitação, Respos-

ta, Sucesso e Falha.

23. Sistema para proporcionar seguramente, em um ambiente de computação do cliente/servidor, um dispositivo de computação do cliente (106) com um endereço de rede compreendendo:

dispositivo de computação do cliente (106) configurado para solicitar um endereço de rede (300), para tentar autenticar o dispositivo de computação do cliente (106) em um dispositivo de computação do servidor (308), em que a solicitação compreende usar o DHCP, no qual a tentativa de autenticação compreende usar mensagens transportadas nos campos de opção (502) DHCP e, se o dispositivo de computação do cliente (106) for autenticado conforme permitido para receber um endereço de rede no ambiente de computação de cliente/servidor, então para receber um endereço de rede atribuído; e

dispositivo de computação do servidor (104) configurado para receber a solicitação do cliente para um endereço de rede, para tentar autenticar o dispositivo de computação do cliente (106) no dispositivo de computação do servidor (308) **caracterizado pelo fato de que** uma rede temporária é atribuída ao dispositivo de computação do cliente (106) para uso durante a tentativa de autenticação, colocando em quarentena o dispositivo de computação do cliente, em que o endereço de rede temporário evita que o dispositivo de computação do cliente converse com qualquer dispositivo em uma rede diferente do dispositivo de computação do servidor e, se o dispositivo de computação do cliente for autenticado, como permitido para receber um endereço de rede no ambiente de computação do cliente/servidor, então para identificar um endereço de rede que seja apropriado ao ambiente de computação do cliente/servidor e que não seja atualmente atribuído a um dispositivo de computação, para atribuir o endereço de rede identificado ao dispositivo de computação do cliente, e para proporcionar o endereço de rede atribuído ao dispositivo de computação do cli-

ente (312).

24. Sistema, de acordo com a reivindicação 23, **caracterizado pelo fato de que** o endereço de rede atribuído é um endereço de IP.

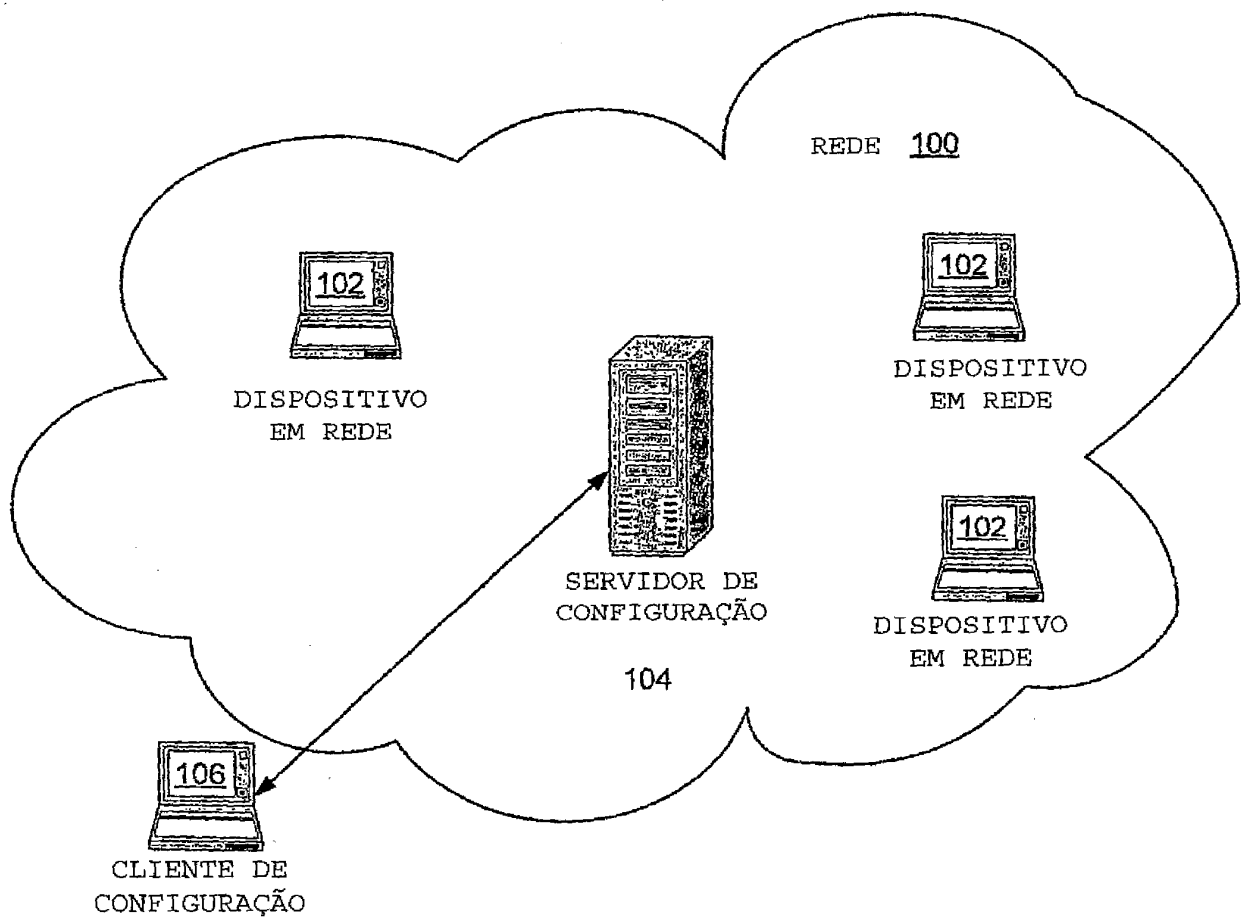

REDE 100
102
DISPOSITIVO EM REDE
102
DISPOSITIVO EM REDE
SERVIDOR DE CONFIGURAÇÃO
104
102
DISPOSITIVO EM REDE
106
CLIENTE DE CONFIGURAÇÃO

FIG. 1

FIG. 2

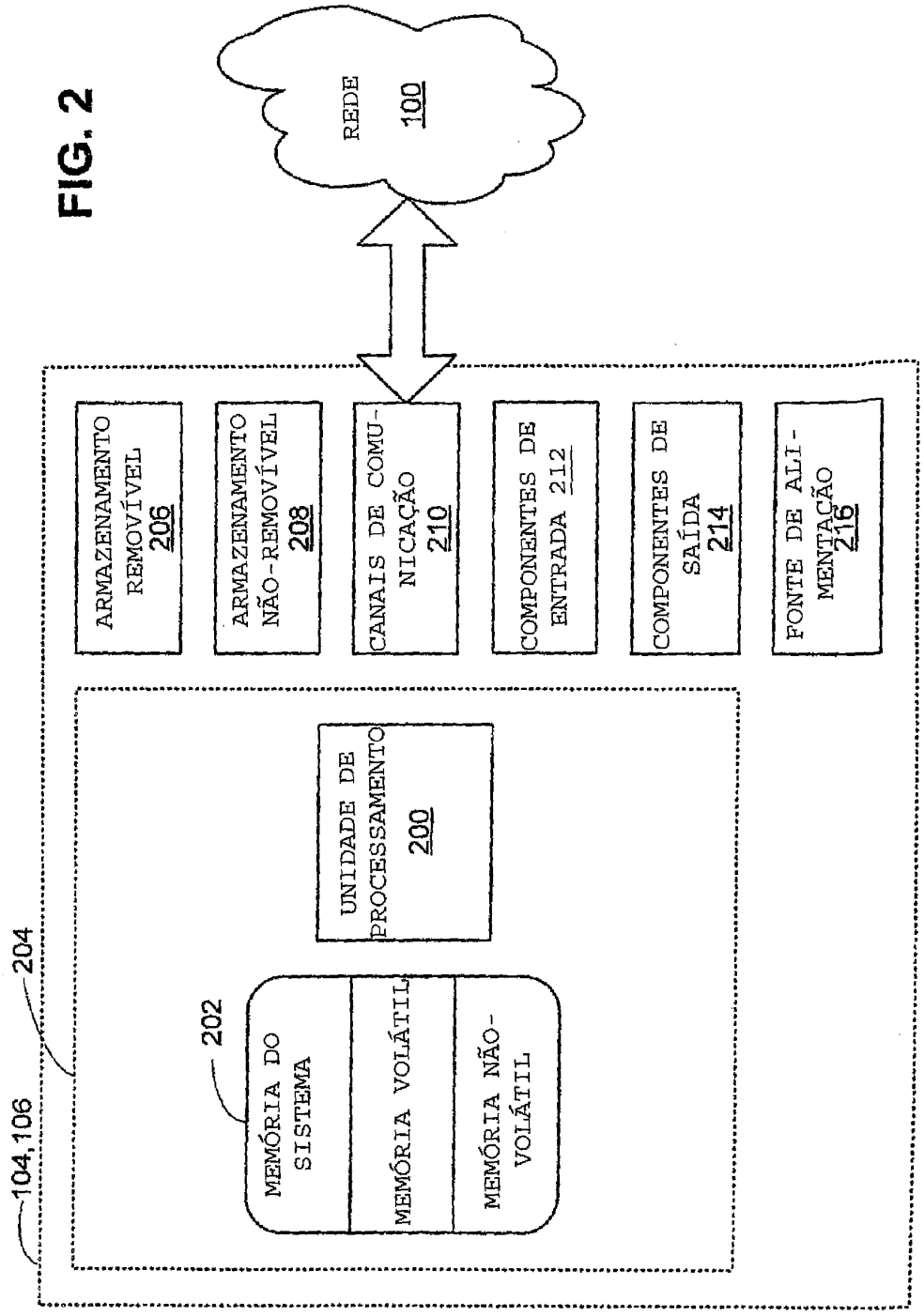

REDE
100
ARMAZENAMENTO REMOVÍVEL 206
ARMAZENAMENTO NÃO-REMOVÍVEL 208
CANAIS DE COMUNICAÇÃO 210
COMPONENTES DE ENTRADA 212
COMPONENTES DE SAÍDA 214
FONTE DE ALIMENTAÇÃO 216
UNIDADE DE PROCESSAMENTO 200
MEMÓRIA DO SISTEMA
MEMÓRIA VOLÁTIL
MEMÓRIA NÃO-VOLÁTIL
202
204
104,106

FIG. 3a

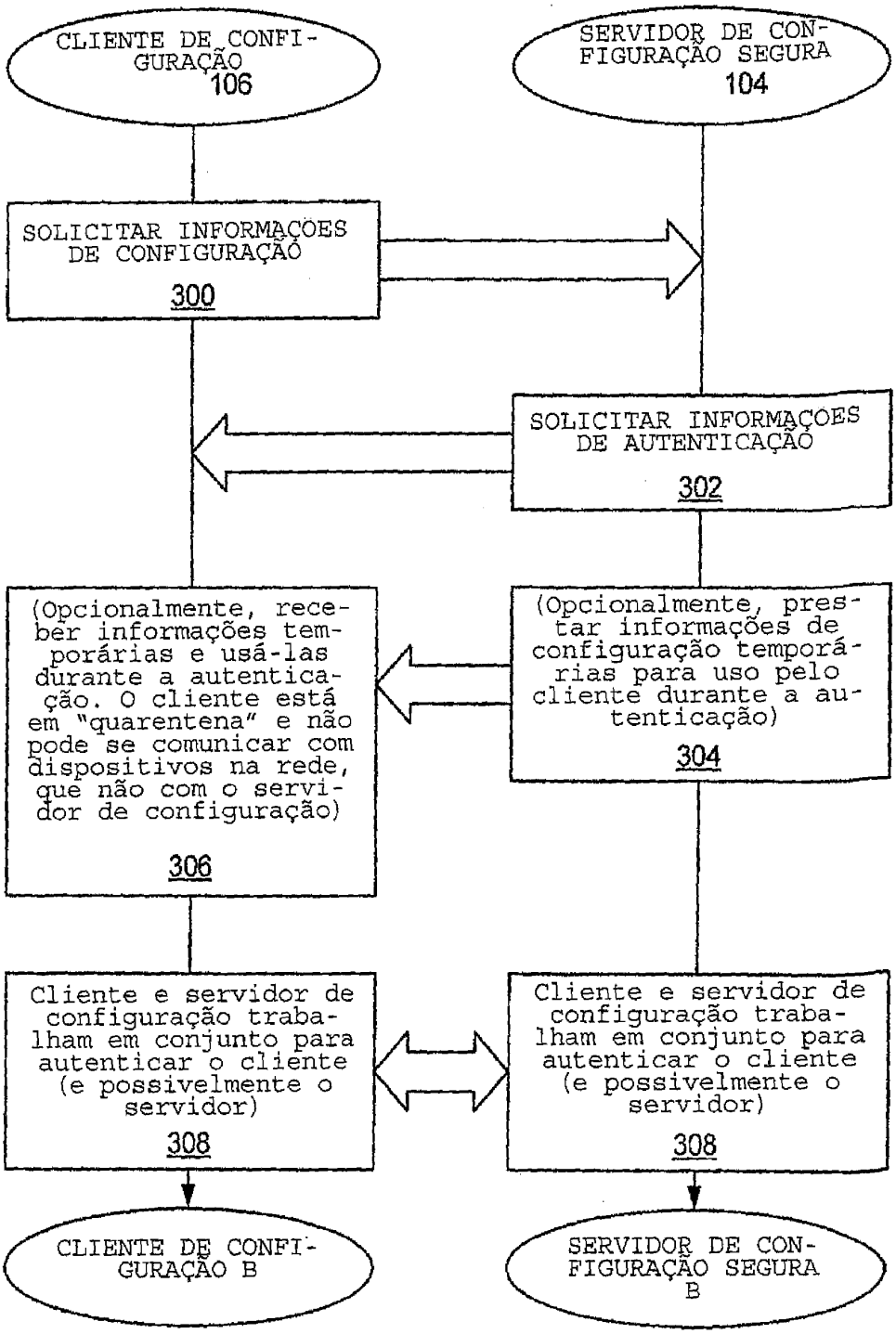

CLIENTE DE CONFIGURAÇÃO 106
SERVIDOR DE CONFIGURAÇÃO SEGURA 104
SOLICITAR INFORMAÇÕES DE CONFIGURAÇÃO 300
SOLICITAR INFORMAÇÕES DE AUTENTICAÇÃO 302
(Opcionalmente, receber informações temporárias e usá-las durante a autenticação. O cliente está em "quarentena" e não pode se comunicar com dispositivos na rede, que não com o servidor de configuração) 306
(Opcionalmente, prestar informações de configuração temporárias para uso pelo cliente durante a autenticação) 304
Cliente e servidor de configuração trabalham em conjunto para autenticar o cliente (e possivelmente o servidor) 308
Cliente e servidor de configuração trabalham em conjunto para autenticar o cliente (e possivelmente o servidor) 308
CLIENTE DE CONFIGURAÇÃO B
SERVIDOR DE CONFIGURAÇÃO SEGURA B

FIG. 3b

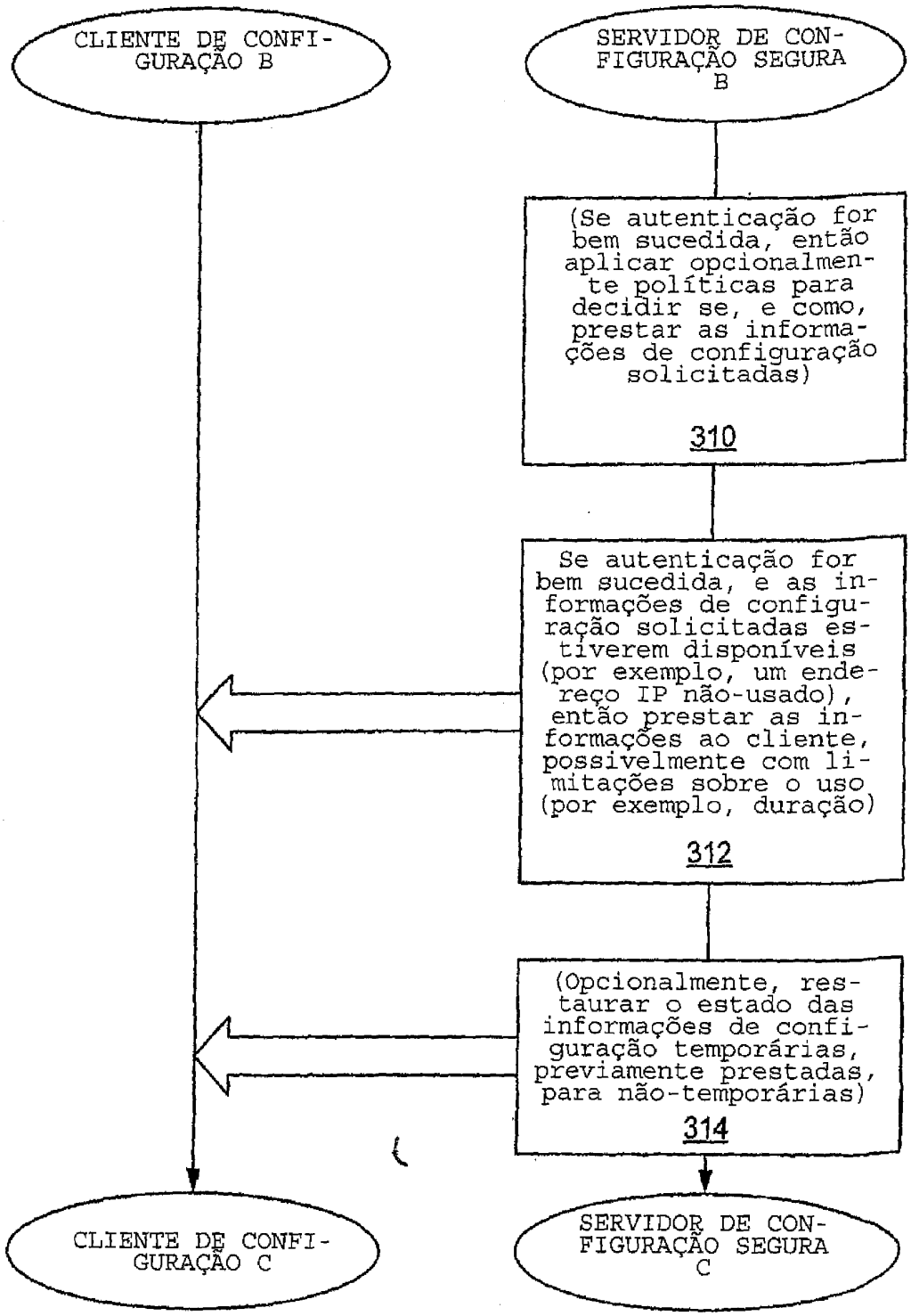

CLIENTE DE CONFIGURAÇÃO B
SERVIDOR DE CONFIGURAÇÃO SEGURA B
(Se autenticação for bem sucedida, então aplicar opcionalmente políticas para decidir se, e como, prestar as informações de configuração solicitadas)
310
Se autenticação for bem sucedida, e as informações de configuração solicitadas estiverem disponíveis (por exemplo, um endereço IP não-usado), então prestar as informações ao cliente, possivelmente com limitações sobre o uso (por exemplo, duração)
312
(Opcionalmente, restaurar o estado das informações de configuração temporárias, previamente prestadas, para não-temporárias)
314
CLIENTE DE CONFIGURAÇÃO C
SERVIDOR DE CONFIGURAÇÃO SEGURA C

FIG. 3c

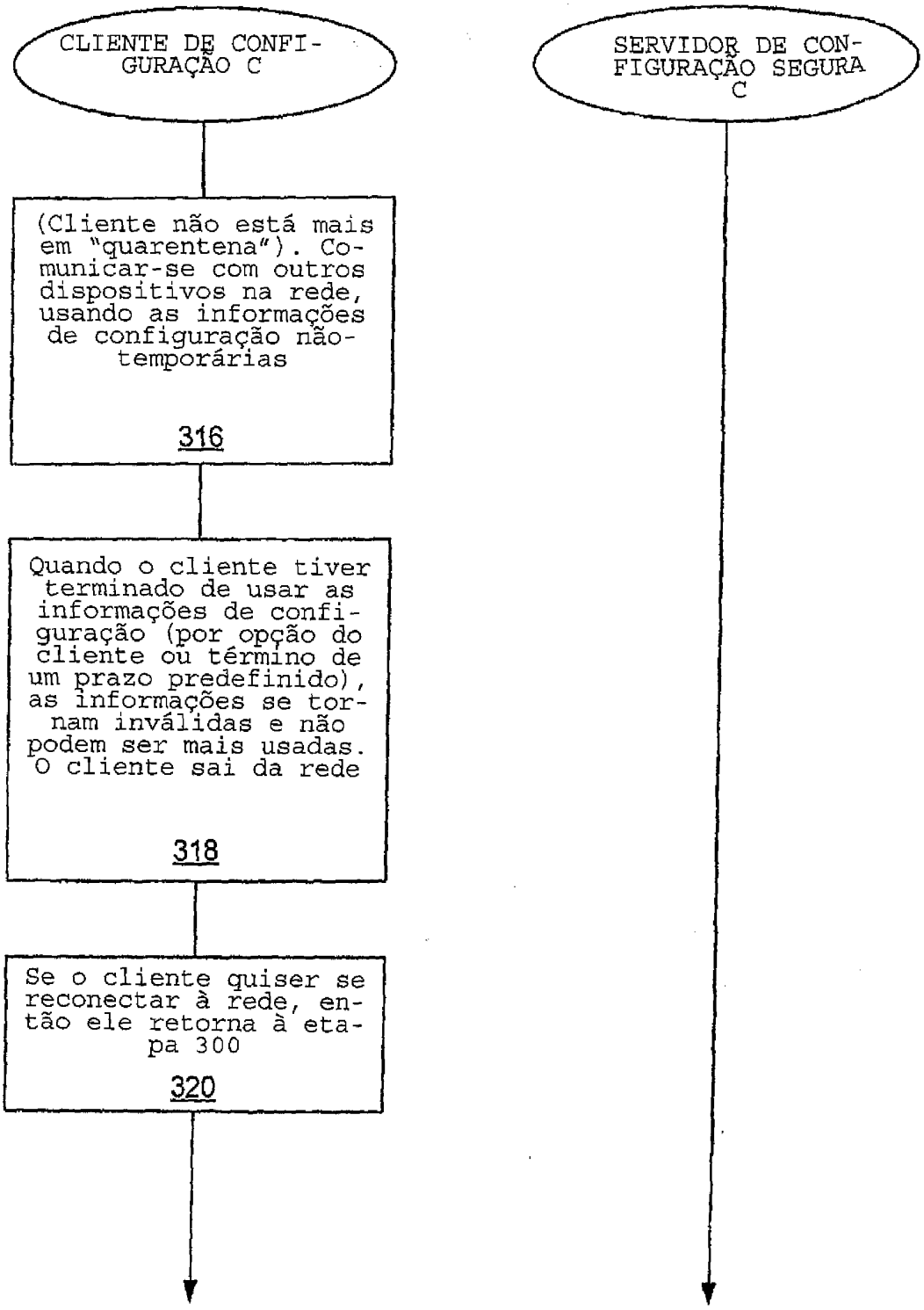

CLIENTE DE CONFIGURAÇÃO C
SERVIDOR DE CONFIGURAÇÃO SEGURA C
(Cliente não está mais em "quarentena"). Comunicar-se com outros dispositivos na rede, usando as informações de configuração não-temporárias
316
Quando o cliente tiver terminado de usar as informações de configuração (por opção do cliente ou término de um prazo predefinido), as informações se tornam inválidas e não podem ser mais usadas. O cliente sai da rede
318
Se o cliente quiser se reconectar à rede, então ele retorna à etapa 300
320

FIG. 4a

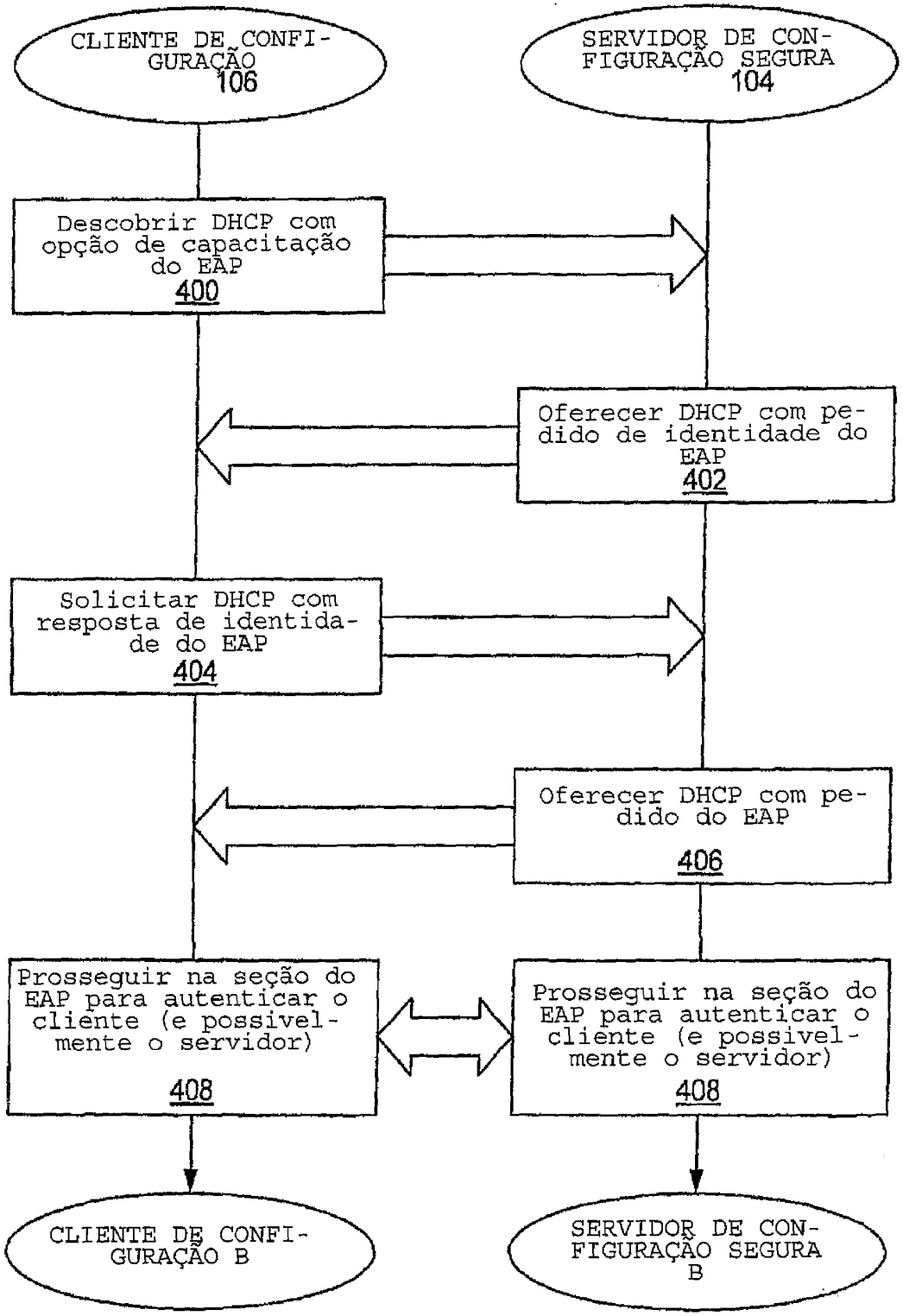

CLIENTE DE CONFIGURAÇÃO 106
SERVIDOR DE CONFIGURAÇÃO SEGURA 104
Descobrir DHCP com opção de capacitação do EAP 400
Oferecer DHCP com pedido de identidade do EAP 402
Solicitar DHCP com resposta de identidade do EAP 404
Oferecer DHCP com pedido do EAP 406
Prosseguir na seção do EAP para autenticar o cliente (e possivelmente o servidor) 408
Prosseguir na seção do EAP para autenticar o cliente (e possivelmente o servidor) 408
CLIENTE DE CONFIGURAÇÃO B
SERVIDOR DE CONFIGURAÇÃO SEGURA B

FIG. 4b

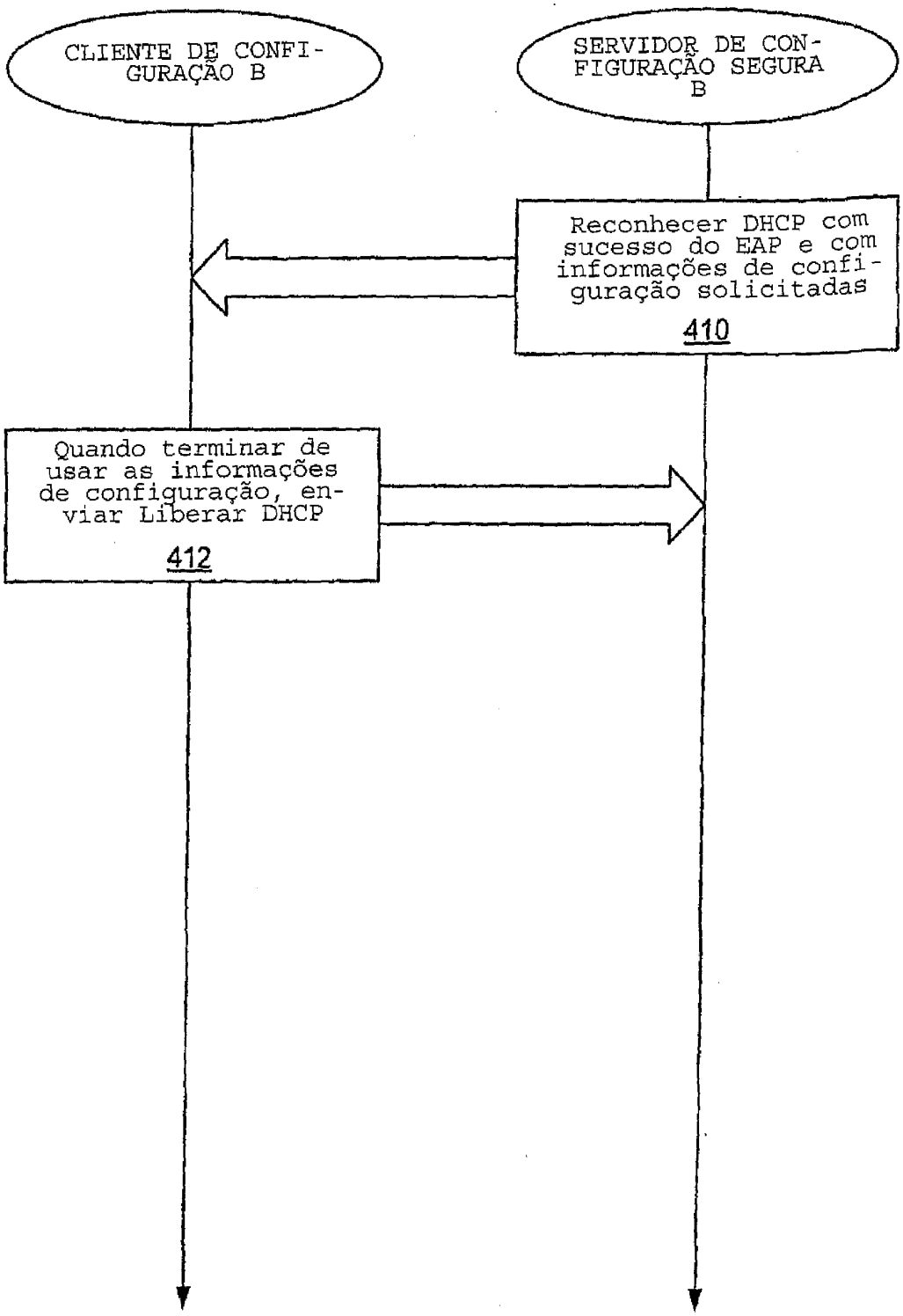
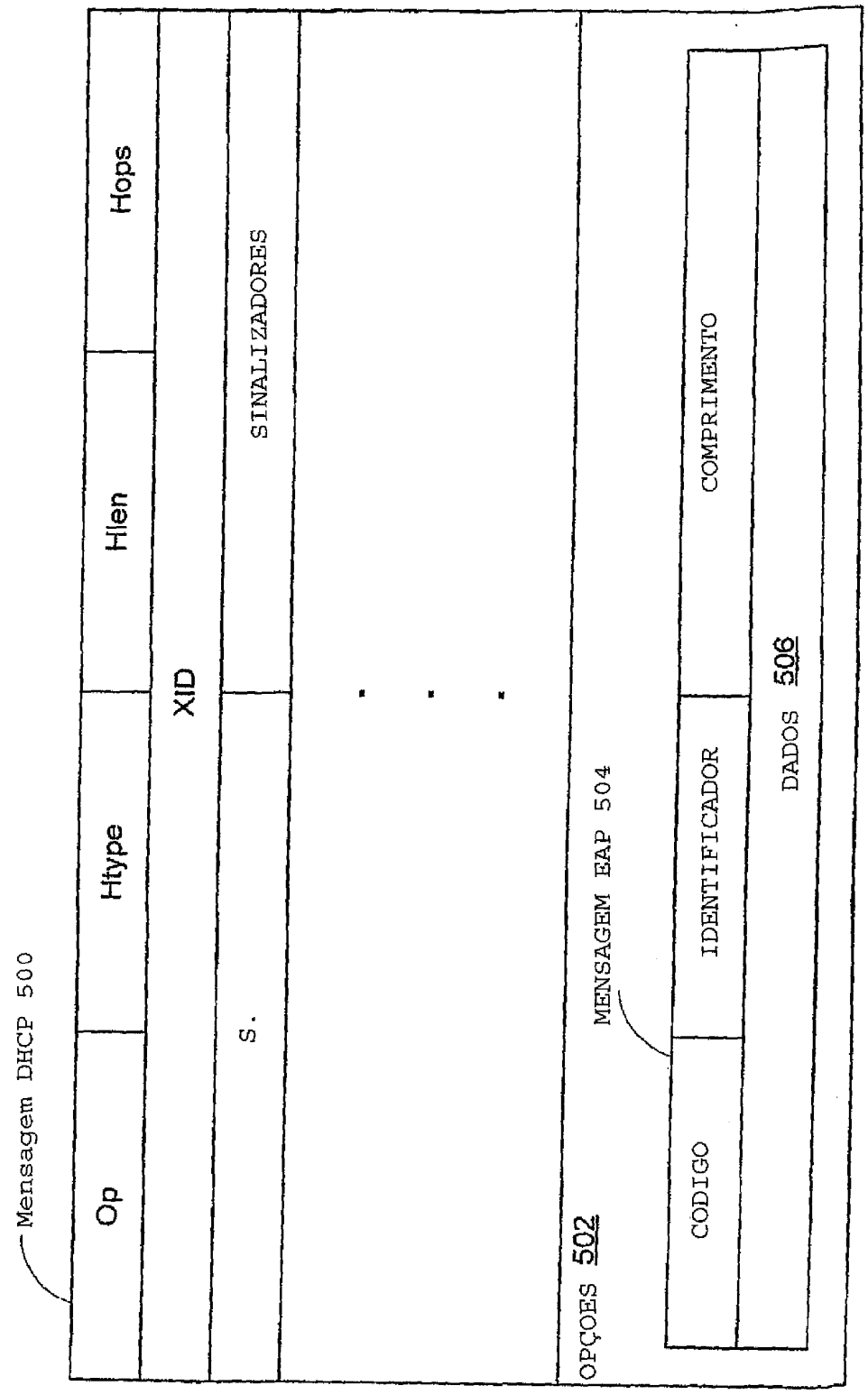

CLIENTE DE CONFIGURAÇÃO B
SERVIDOR DE CONFIGURAÇÃO SEGURA B
Reconhecer DHCP com sucesso do EAP e com informações de configuração solicitadas
410
Quando terminar de usar as informações de configuração, enviar Liberar DHCP
412

FIG. 5


Mensagem DHCP 500
Op
Htype
Hlen
Hops
XID
S.
SINALIZADORES
OPÇOES 502
MENSAGEM EAP 504
CODIGO
IDENTIFICADOR
COMPRIMENTO
DADOS 506