



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

(21) **PI 0712204-7 A2**



(22) Data de Depósito: 26/04/2007
(43) Data da Publicação: 10/01/2012
(RPI 2140)

(51) *Int.Cl.:*
G06F 15/16
G06F 21/00
H04L 12/22

(54) **Título:** ZONAS HABILITADAS POR DESAFIO DE NOME

(30) **Prioridade Unionista:** 01/06/2006 US 11/421.641

(73) **Titular(es):** Microsoft Corporation

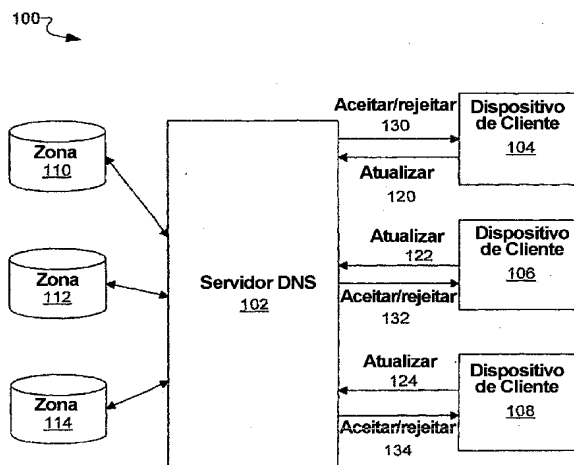
(72) **Inventor(es):** James M. Gilroy, Jeffrey J. Westhead, Kamal Anupama Janardhan, Moon Majumdar

(74) **Procurador(es):** Alexandre Ferreira

(86) **Pedido Internacional:** PCT US2007010298 de 26/04/2007

(87) **Publicação Internacional:** WO 2007/142759de 13/12/2007

(57) **Resumo:** ZONAS HABILITADAS POR DESAFIO DE NOME
São aqui descritos um método e um sistema para implementar zonas habilitadas por desafio de nome. Um servidor DNS recebe uma atualização de um dispositivo de cliente. Se o servidor DNS hospeda uma zona autorizada para a atualização, o servidor DNS determina se há um registro para o nome de hospedeiro. Se houver, então o endereço IP associado ao nome de hospedeiro é determinado. O endereço IP é comparado com o endereço de origem do dispositivo de cliente que envia a atualização. Se os endereços IP corresponde-rem um ao outro, então a atualização é aceita.





“ZONAS HABILITADAS POR DESAFIO DE NOME”

Antecedentes

O Sistema de Nomes de Domínio (DNS) é um sistema que armazena informações associadas a nomes de domínio em um banco de dados distribuído em uma ou mais redes.

5 As informações armazenadas incluem o endereço de Protocolo Internet (IP) associado a um nome de domínio. O espaço de nome de domínio pode ser pensado como uma árvore de nomes de domínio. Cada nó ou folha na árvore é associado a registros de recursos, que guardam informações associadas ao nome de domínio. A árvore é dividida em zonas. Uma zona é uma reunião de nós conectados que são servidos de maneira autorizada por um servidor DSN autorizado. Um servidor autorizado pode hospedar uma ou mais zonas.

10 As zonas podem ser armazenadas utilizando-se arquivos baseados em texto ou utilizando-se um sistema de diretórios. As zonas podem ser configuradas para aceitar atualizações dinâmicas das máquinas de clientes de modo a processarem uma alteração no nome da máquina, no endereço IP ou outras informações de domínio. As atualizações dinâmicas
15 podem ser seguras ou de risco. As atualizações seguras podem exigir uma negociação de contexto de segurança entre uma máquina de cliente e um servidor DNS. O uso de atualizações seguras pode exigir que apenas o proprietário original de um nome registrado faça alterações nesse registro existente. Tentativas de registro por outras máquinas de cliente para o mesmo nome são rejeitadas. As atualizações seguras exigem credenciais de domínio e
20 não estão disponíveis para zonas que estão armazenadas utilizando-se arquivos baseados em texto.

As atualizações de risco permitem que os clientes criem um novo registro ou modifiquem um registro existente. Atualizações de risco para dados existentes não são restritas ao proprietário original. Portanto, outra máquina pode efetuar uma atualização dinâmica para o mesmo nome. Se isto for feito com más intenções, é conhecido como ataque de roubo de nome. As atualizações de risco não exigem credenciais de domínio e podem ser utilizadas independentemente do sistema de armazenamento que é utilizado para a zona. Entretanto, com a utilização das atualizações de risco, os clientes ficam vulneráveis a ataques de roubo de nome e não podem ter garantia de singularidade de nome em uma zona.

Sumário

30 A seguir é apresentado um sumário simplificado da revelação de modo a se proporcionar um entendimento básico ao leitor. Este sumário não é uma vista panorâmica extensiva da revelação e não identifica os elementos-chaves/críticos da invenção nem delineia o alcance da invenção. Sua única finalidade é a de apresentar alguns conceitos aqui revelados sob uma forma simplificada como uma introdução à descrição mais detalhada que é
35 apresentada mais adiante.

São aqui descritas diversas tecnologias e técnicas referentes a métodos e sistemas

para implementar zonas habilitadas por desafio de nome. De acordo com uma implementação das tecnologias descritas, quando um servidor DNS recebe uma atualização para um nome, o servidor DNS verifica se o nome de hospedeiro já existe na zona aplicável. Se já houver um registro para o nome, então o servidor DNS determina se as identidades do registrando original e do dispositivo de cliente que envia a atualização são as mesmas pela comparação de seus endereços IP de origem. Se os endereços IP de origem forem os mesmos, então a atualização é aceita. Se os endereços IP de origem forem diferentes, o servidor DNS pode enviar uma consulta DNS ao registrando original. Se o registrando original responde à consulta DNS, então a atualização é rejeitada. Se o registrando original não responder à consulta DNS, então a atualização pode ser aceita.

Muitos dos aspectos resultantes serão mais prontamente apreciados à medida que os mesmos se tornem melhor entendidos por referência à descrição detalhada seguinte considerada em conjunto com os desenhos anexos.

Descrição dos Desenhos

A presente invenção será melhor entendida com a descrição detalhada seguinte, lida à luz dos desenhos anexos, nos quais:

A Figura 1 é um diagrama de blocos que mostra um sistema exemplar para implementar desafio de nome.

A Figura 2 é um instantâneo de tela que mostra uma interface com usuário exemplar para gerenciar zonas DNS.

A Figura 4 é um diagrama de fluxos que mostra um processo exemplar para implementar desafio de nome.

A Figura 5 mostra um ambiente de computação exemplar no qual determinados aspectos da invenção podem ser implementados.

Os mesmos números de referência são utilizados para designar as mesmas peças nos desenhos anexos.

Descrição Detalhada

A descrição detalhada apresentada a seguir em conexão com os desenhos anexos pretende ser uma descrição dos presentes exemplos e não pretende representar as únicas formas nas quais o presente exemplo pode ser construído ou utilizado. A descrição apresenta as funções do exemplo e a seqüência de etapas para construir e acionar o exemplo. Entretanto, as mesmas, ou equivalentes, funções e seqüências podem ser realizadas por diferentes exemplos.

A Figura 1 é um diagrama de blocos que mostra um sistema 100 exemplar para implementar desafio de nome para uma ou mais zonas em um servidor DNS 102. O servidor DNS 102 é comunicativamente acoplado a um ou mais dispositivos de cliente, tais como 104, 106 ou 108. O servidor DNS 102 hospeda uma ou mais zonas, tais como 110, 112 ou

114. Cada zona inclui um ou mais registros que armazenam informações de domínio, como, por exemplo, um mapeamento de endereços IP nos dispositivos de cliente no domínio. A zona ou zonas podem ser suportadas por arquivo(s) ou integradas com um sistema de diretórios, tal como o sistema Active Directory®. A zona ou zonas podem ser configuradas para

5 aceitar atualizações dinâmicas dos dispositivos de cliente de modo a processarem uma ou mais alterações no nome do dispositivo de cliente, no endereço IP ou em outras informações de domínio. As atualizações dinâmicas podem ser seguras ou de risco. As atualizações seguras podem exigir uma negociação de contexto de segurança entre um dispositivo de cliente e o servidor DNS. As atualizações seguras podem exigir que apenas o dispositivo

10 de cliente original que registrou o nome de domínio pode fazer alterações no registro associado ao nome de domínio. Registros de outros clientes que tentem registrar o mesmo nome de domínio seriam rejeitados.

As atualizações de risco permitem que os clientes criem um novo registro ou modifiquem um registro existente. As atualizações de risco para dados existentes não são restritas ao proprietário original. O sistema 100, conforme mostrado na Figura 1, proporciona atualizações dinâmicas de risco e implementa desafio de nome para atualizações que entram em conflito com registros existentes. Cada dispositivo de cliente, tal como 104, 106 ou 108, podem enviar atualizações, tais como 120, 122 ou 124, ao servidor DNS. Quando o servidor DNS 102 recebe uma atualização, o servidor DNS verifica se o nome de hospedeiro já existe na zona aplicável. Se já houver um registro para o nome de hospedeiro, então o servidor DNS 102 determina se as identidades do registrando original e dos dispositivos de cliente que enviam a atualização são os mesmos comparando seus endereços IP de origem. Se os endereços IP de origem forem os mesmos, então a atualização é aceita. Se os endereços IP de origem forem diferentes, o servidor DNS pode enviar uma consulta DNS ao registrando original. Se o registrando original responder à consulta DNS, então a atualização é rejeitada. Se o registrando original não responder à consulta DNS, então a atualização pode ser aceita. O servidor DNS 102 envia uma resposta, tal como 130, 132 ou 134, de volta ao dispositivo de cliente que solicitou a atualização para notificar o dispositivo de cliente da aceitação ou rejeição da atualização solicitada.

30 Por exemplo, suponha-se que a zona 110 armazene registros para o domínio "corp.contoso.com". A zona 110 tem um registro de endereço (A) para "lab-comp.corp.contoso.com" que foi criado por um registro recebido do dispositivo de cliente 104. O dispositivo de cliente 104 tem o nome de hospedeiro "lab-comp" que foi acrescentado ao domínio "corp.contoso.com".

35 Em um primeiro roteiro, suponha-se que o dispositivo de cliente 104 envie uma atualização dinâmica para "lab-comp.corp.contoso.com" para renovar seu registro A. Quando o servidor DNS autorizado 102 é encontrado, ele verifica se há algum dado existente para o

registro A referente a “lab-comp” na zona “corp.contoso.com”. O registro A para “lab-comp” já existe. Portanto, o servidor DNS verifica se o endereço de origem do registrando original e o endereço de origem do dispositivo de cliente que enviou a atualização são idênticos. Os endereços de origem são o mesmo endereço. Portanto, o servidor DNS 102 aceita a atualização. A atualização é processada e o sucesso da atualização é enviado de volta ao dispositivo de cliente 104.

Em um segundo roteiro, suponha-se que o dispositivo de cliente 105 envie uma atualização dinâmica para “lab-comp.corp.contoso.com” em uma tentativa de registrar seu endereço IP. Quando o servidor DNS 102 autorizado é encontrado, ele verifica se existe algum registro A para “lab-comp” na zona “corp.contoso.com”. O registro A para “lab-comp” já existe. Portanto, o servidor DNS verifica se o endereço de origem do registrando original e o endereço de origem do dispositivo de cliente que enviou são idênticos. O registrando original é o dispositivo de cliente 104, e o dispositivo de cliente 105 está enviando a atualização, de modo que seus endereços de origem não são os mesmos. O servidor DNS 102 pode rejeitar a atualização. O servidor DNS 102 pode enviar uma consulta DNS ao dispositivo de cliente 104. Se uma confirmação for recebida do dispositivo de cliente 104 em resposta à consulta DNS, então o servidor DNS 102 rejeita a atualização. Se nenhuma resposta à consulta DNS for recebida do dispositivo de cliente 104, então o servidor DNS 102 pode aceitar a atualização.

As Figuras 2-3 mostram instantâneos 200 e 300 que mostram uma interface com usuário exemplar para gerenciar zonas DNS. No sistema mostrado na Figura 2, há uma série de zonas DNS, incluindo_msdcs.dnsregression.com 202, bar.com 204, dnsregression.com 206 e a zona de risco 208. O usuário pode selecionar uma zona DNS gerenciada e editar uma ou mais propriedades da zona selecionada. Conforme mostrado na Figura 3, o usuário escolheu ver e/ou editar as propriedades da zona de risco 208. Para cada zona, o usuário pode escolher se ou não habilitar atualizações dinâmicas para a zona. Se o usuário escolher habilitar atualizações dinâmicas, o usuário pode escolher habilitar apenas atualizações seguras, ou o usuário pode escolher habilitar atualizações tanto seguras quanto de risco. No exemplo mostrado na Figura 3, o usuário escolheu habilitar atualizações tanto seguras quanto de risco, conforme mostrado em 302. Quando atualizações de risco são habilitadas, o usuário pode escolher habilitar desafio de nome para as atualizações de risco, conforme mostrado em 304. Uma vez que o desafio de nome é habilitado, o servidor DNS desafiárá quaisquer atualizações para nomes existentes, conforme descrito em detalhe pelo processo exemplar da Figura 4.

A Figura 4 é um diagrama de fluxo que mostra um processo exemplar para zonas habilitadas por desafio de nome. Embora a descrição da Figura 4 possa ser feita com referência a outras figuras, deve ficar entendido que o processo exemplar mostrado na Figura 4

não pretende ser limitado a estar associado aos sistemas ou a outros conteúdos de qualquer figura ou figuras específicas. Além disto, deve ficar entendido que, embora o processo da Figura 4 indique uma ordem específica de execução de operações, em uma ou mais implementações alternativas, as operações podem ser ordenadas de maneira diferentes. Além disto, algumas das etapas e dados mostrados no processo exemplar da Figura 4 podem não ser necessárias e podem ser omitidas em algumas implementações. Finalmente, embora o processo exemplar da Figura 4 contenha várias etapas separadas, deve-se reconhecer que, em alguns ambientes, algumas destas operações podem ser combinadas e executadas ao mesmo tempo.

Em 402, uma atualização para um nome é recebida em um servidor DNS de um primeiro dispositivo de cliente. A atualização inclui um nome de hospedeiro. Em 404, é determinado se o servidor DNS hospeda uma zona autorizada para atualização. Se o fizer, então o processo prossegue em 408. Se não o fizer, então, em 406, a atualização é rejeitada. Quando o servidor DNS que hospeda a zona autoridade para a atualização é encontrado, então, em 408, a zona é verificada de modo a se determinar se já existe um registro para o nome de hospedeiro. Ao se determinar se já existe um registro para o nome de hospedeiro, um ou mais registros de um ou mais tipos de registro podem ser verificados. Tipos de registro exemplares que podem ser verificados incluem, mas não se limitam a, registros de endereço (A), registros de endereço IPv6 e registros de Nome Canônico (NOME).

Se nenhum registro para o nome de hospedeiro for encontrado, então, em 430, a atualização é aceita. Se já houver um registro para o nome de hospedeiro, então, em 412, é determinado o endereço IP de origem associado ao registro de hospedeiro. E, 414, o endereço IP de origem associado ao registro de hospedeiro é comparado com o endereço IP de origem do primeiro dispositivo de cliente. Se os endereços IP correspondem um ao outro, então, em 420, a atualização é aceita. Se os endereços IP não correspondem um ao outro, então, em 416, uma consulta DNS é enviada a um segundo dispositivo de cliente que tem o endereço IP associado ao registro de hospedeiro e, em 418, é determinado se há uma resposta do segundo dispositivo de cliente. Se uma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS, então, em 422, a atualização é rejeitada. Se nenhuma resposta à consulta DNS for recebida do segundo dispositivo de cliente, então, em 422, a atualização pode ser aceita. Se a atualização for aceita e um ou mais servidores DNS tiverem cópias da zona, então a atualização pode ser reproduzida para o outro servidor ou servidores DNS.

A Figura 5 mostra um ambiente de computação exemplar no qual determinados aspectos da invenção podem ser implementados. Deve ficar entendido que o ambiente de computador 500 é apenas um exemplo de ambiente de computação adequado no qual as diversas tecnologias aqui descritas podem ser utilizadas e não pretende sugerir qualquer

limitação ao alcance de uso ou funcionalidade das tecnologias aqui descritas. Nem deve o ambiente de computação 500 ser interpretado como exigindo necessariamente todos os componentes aqui mostrados.

As tecnologias aqui descritas podem ser operacionais com numerosos outros ambientes ou configurações de computação de uso geral ou especial. Exemplos de ambientes e/ou configurações de computação notoriamente conhecidos que podem ser adequados para uso com as tecnologias aqui descritas incluem, mas não se limitam a, computadores pessoais, computadores servidores, dispositivos de mão ou portáteis, dispositivos de mesa gráfica, sistemas microprocessadores, sistemas baseados em microprocessador, conversores set top Box, eletrônicos para consumo programáveis, PCs de rede, minicomputadores, computadores de grande porte, ambientes de computação distribuídos que incluem qualquer um dos sistemas ou dispositivos acima, e semelhantes.

Com referência à Figura 5, o ambiente de computação 500 inclui um dispositivo de computação de uso geral 510. Os componentes do dispositivo de computação 510 podem incluir, mas não se limitam a, uma unidade de processamento 512, uma memória 514, um dispositivo de armazenamento 516, dispositivo(s) de entrada 518, dispositivo(s) de saída 520 e conexão(ões) de comunicação 522.

A unidade de processamento 512 pode incluir um ou mais processadores de uso geral ou especial, ASICs ou chips lógicos programáveis. Dependendo da configuração e do tipo do dispositivo de computação, a memória 514 pode ser volátil (tal como uma RAM) não volátil (tal como uma ROM, memória flash, etc.) ou uma combinação das duas. O dispositivo de computação 510 pode incluir também armazenamento adicional (removível e/ou não removível) que inclui, mas não se limita a, discos ou fita magnética ou óptica. Tal armazenamento adicional é mostrado na Figura pelo armazenamento 516. Os meios de armazenamento em computador incluem meios não voláteis, removíveis e não removíveis implementados em qualquer método ou tecnologia para armazenamento de informações tais como instruções passíveis de leitura por computador, estruturas de dados, módulos de programa ou outros dados. A memória 514 e o armazenamento 516 são exemplos de meios de armazenamento em computador. Os meios de armazenamento em computador incluem, mas não se implementam a, RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, discos versáteis digitais (DVD) ou outro armazenamento óptico, cassetes magnéticos, fita magnética, armazenamento em disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que possa ser utilizado para armazenar as informações desejadas e que possa ser acessado pelo dispositivo de computação 510. Quaisquer meios de armazenamento em computador podem ser parte do dispositivo de computação 510.

O dispositivo de computação 510 pode conter também conexão(ões) de comunica-

ção 522 que permitem que o dispositivo de computação 510 se comunique com outros dispositivos, como, por exemplo, com outros dispositivos de computação, através da rede 530. A conexão(ões) 522 é(são) um exemplo de meios de comunicação. Os meios de comunicação corporificam tipicamente instruções passíveis de leitura por computador, estruturas de dados, módulos de programa ou outros dados em um sinal de dado modulado, tal como uma onda portadora ou outro mecanismo de transporte, e incluem quaisquer meios de entrega de informações. O termo 'sinal de dado modulado' significa um sinal que tem uma ou mais das características fixadas ou alteradas de maneira a codificar as informações no sinal. A título de exemplo, e não de limitação, os meios de comunicação incluem meios cabeados, tal como uma rede cabeada ou conexão cabeada direta, e meios sem fio tais como meios acústicos, de radiofrequência, infravermelhos e outros meios sem fio. O termo meios passíveis de leitura por computador aqui utilizados incluem meios de armazenamento.

O dispositivo de computação 510 pode ter também dispositivo(s) de entrada 518, tais como um teclado, um mouse, uma caneta, um dispositivo de entrada de voz, um dispositivo de entrada sensível ao toque e/ou qualquer outro dispositivo de entrada. Dispositivo(s) de saída 520, tais como um ou mais monitores, alto-falantes, impressoras e/ou qualquer outro dispositivo de saída, podem ser também incluídos.

Embora a invenção tenha sido descrita em termos de várias implementações exemplares, os versados na técnica reconhecerão que a invenção não está limitada às implementações descritas, mas pode ser posta em prática com modificações e alterações dentro do espírito e alcance das reivindicações anexas. A descrição deve assim ser considerada como ilustrativa e não como limitadora.

REIVINDICAÇÕES

1. Método **CARACTERIZADO** por compreender:

receber uma atualização em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização incluindo um nome de hospedeiro;

5 determinar se o servidor DNS hospeda uma zona autorizada para a atualização;
determinar se já existe um registro para o nome de hospedeiro; e se existir,
determinar o endereço de Protocolo

10 Internet (IP) associado ao nome de
hospedeiro;
determinar se o endereço IP
associado ao nome de hospedeiro
corresponde ao endereço IP de origem do
primeiro dispositivo de cliente; e
aceitar a atualização se os

15 endereços IP correspondem um ao outro.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender também aceitar a atualização se não houver registro para o nome de hospedeiro.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender também enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço
20 IP associado ao nome de hospedeiro se o endereço IP associado ao nome de hospedeiro
não corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** por compreender também rejeitar a atualização se uma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS.

25 5. Método, de acordo com a reivindicação 3, **CARACTERIZADO** por compreender
também aceitar a atualização se nenhuma confirmação for recebida do segundo dispositivo
de cliente em resposta à consulta DNS.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender também reproduzir a atualização para outro servidor DNS.

30 7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que
determinar se já existe um registro para o nome de hospedeiro compreende verificar vários
registros de vários tipos.

8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de Endereço (A).

35 9. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que
um dos tipos de registro é um registro de endereço IPv6.

10. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que

um dos tipos de registro é um registro de Nome Canônico (NOME C).

11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a zona é suportada por arquivo.

5 12. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a zona é integrada com um sistema de diretórios.

13. Meio ou meios passíveis de leitura por computador com instruções executáveis por dispositivo(s) para executar etapas, **CARACTERIZADO(s)** por compreender:

10 receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nome de domínio (DNS) que hospeda uma zona autorizada para a atualização, a atualização incluindo um nome de hospedeiro; verificar um ou mais registros na zona de modo a determinar se já há um registro para o
15 nome de hospedeiro, e se houver, verificar o registro para o nome de hospedeiro de modo a determinar o endereço de Protocolo Internet (IP) associado ao nome de hospedeiro de modo a determinar o
20 endereço de Protocolo Internet (IP) associado ao nome de hospedeiro; determinar se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro
25 dispositivo de cliente, e se não corresponder, enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço IP associado ao nome de hospedeiro; e
30 determinar se se vai aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS.

35 14. Meio ou mais passíveis de leitura por dispositivo(s), de acordo com a reivindicação 13, **CARACTERIZADO(s)** pelo fato de que as etapas compreendem também aceitar a atualização se não houver registro para o nome de hospedeiro.

15. Meio ou mais passíveis de leitura por dispositivo(s), de acordo com a reivindicação 13, **CARACTERIZADO**(s) pelo fato de que as etapas compreendem também aceitar a atualização se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente.

16. Meio ou mais passíveis de leitura por dispositivo(s), de acordo com a reivindicação 13, **CARACTERIZADO**(s) pelo fato de determinar se se vai aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS compreende rejeitar a atualização se o segundo dispositivo de cliente responder à consulta DNS e aceitar a atualização se o segundo dispositivo de cliente não responder à consulta DNS.

17. Método **CARACTERIZADO** por compreender:

receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização

incluindo um nome de hospedeiro; determinar se já existe um registro para o nome de hospedeiro; e se existir, determinar o endereço IP de um

registrando do nome de hospedeiro; determinar se o endereço IP de origem do registrando do nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente, e se não corresponder,

enviar uma consulta DNS ao registrando do nome de hospedeiro; e rejeitar a atualização se uma confirmação for recebida do registrando em resposta à consulta DNS.

18. Método, de acordo com a reivindicação 17, **CARACTERIZADO** por compreender também aceitar a atualização se não houver registro para o nome de hospedeiro.

19. Método, de acordo com a reivindicação 17, **CARACTERIZADO** por compreender também aceitar a atualização se o endereço IP de origem do registrando do nome de hospedeiro corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

20. Método, de acordo com a reivindicação 17, **CARACTERIZADO** por compreender também aceitar a atualização se nenhuma resposta for recebida do registrando em resposta à consulta DNS.

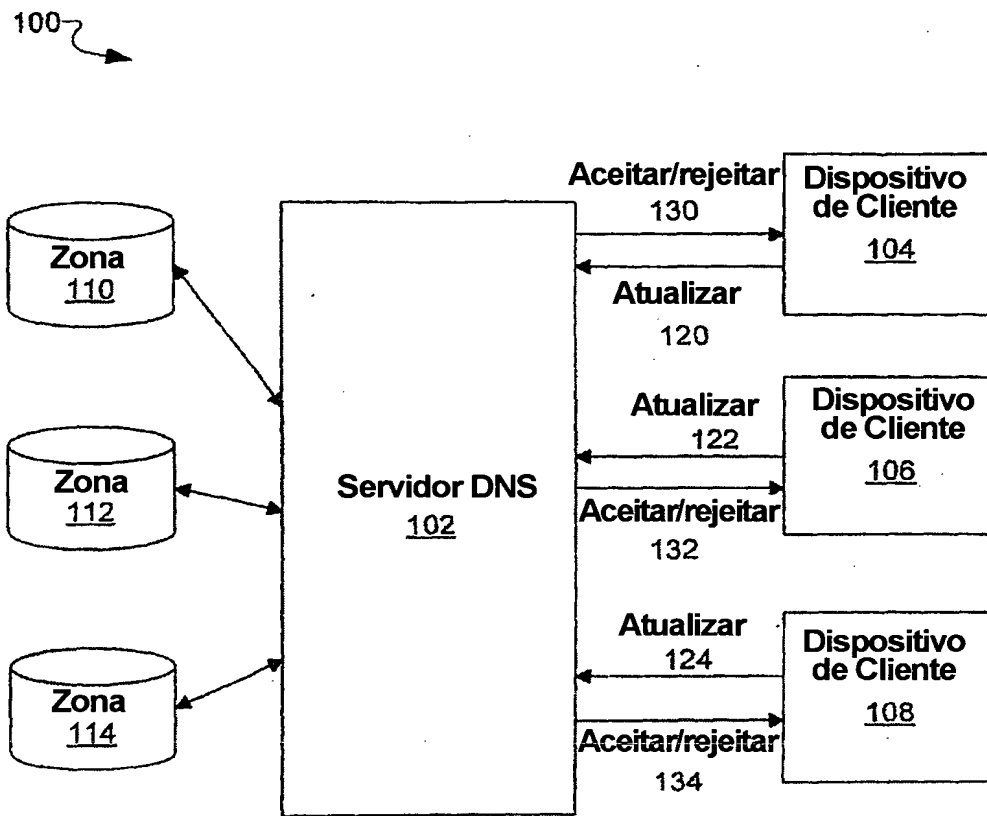


FIG. 1

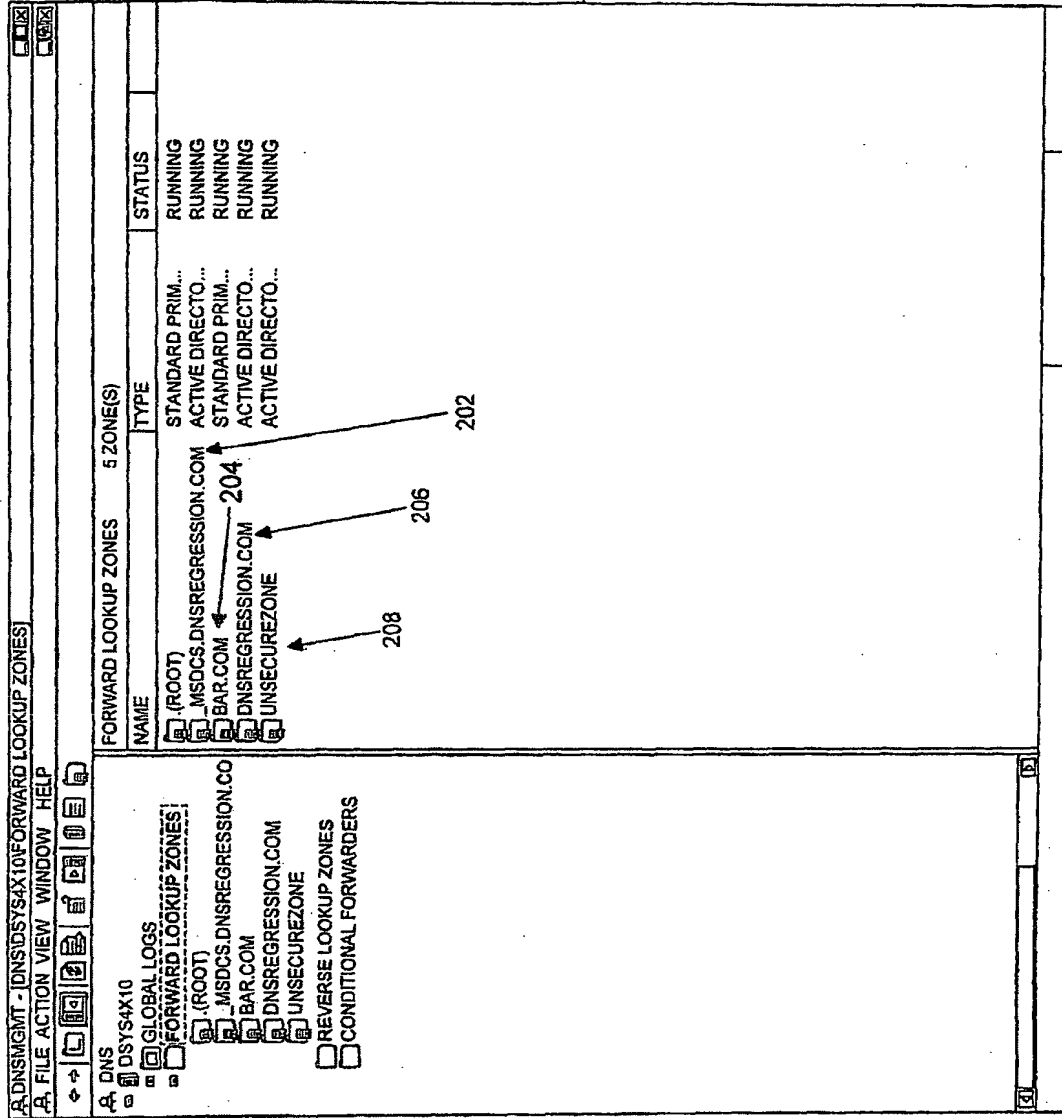


FIG. 2

304

FIG. 3

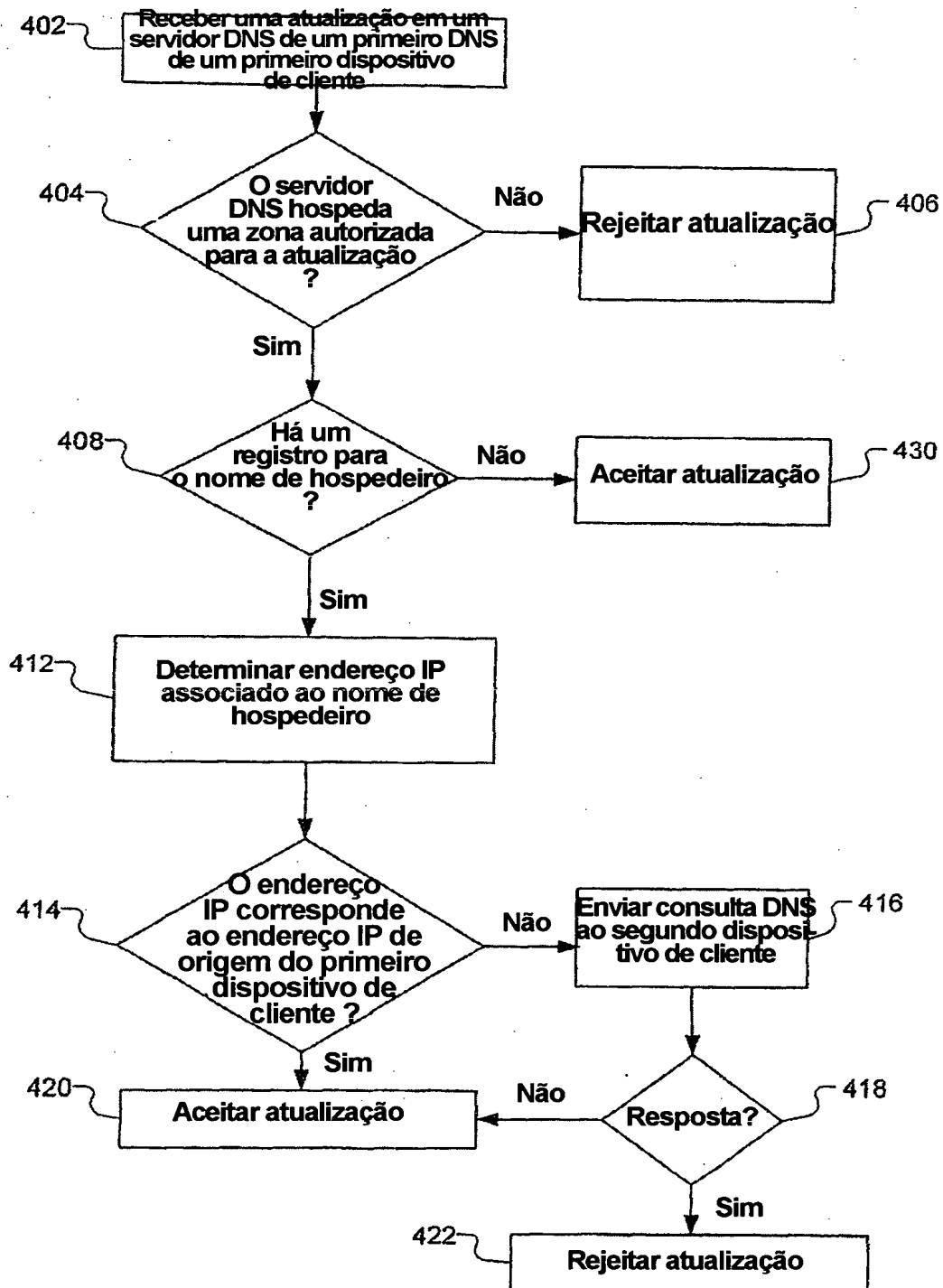


FIG. 4

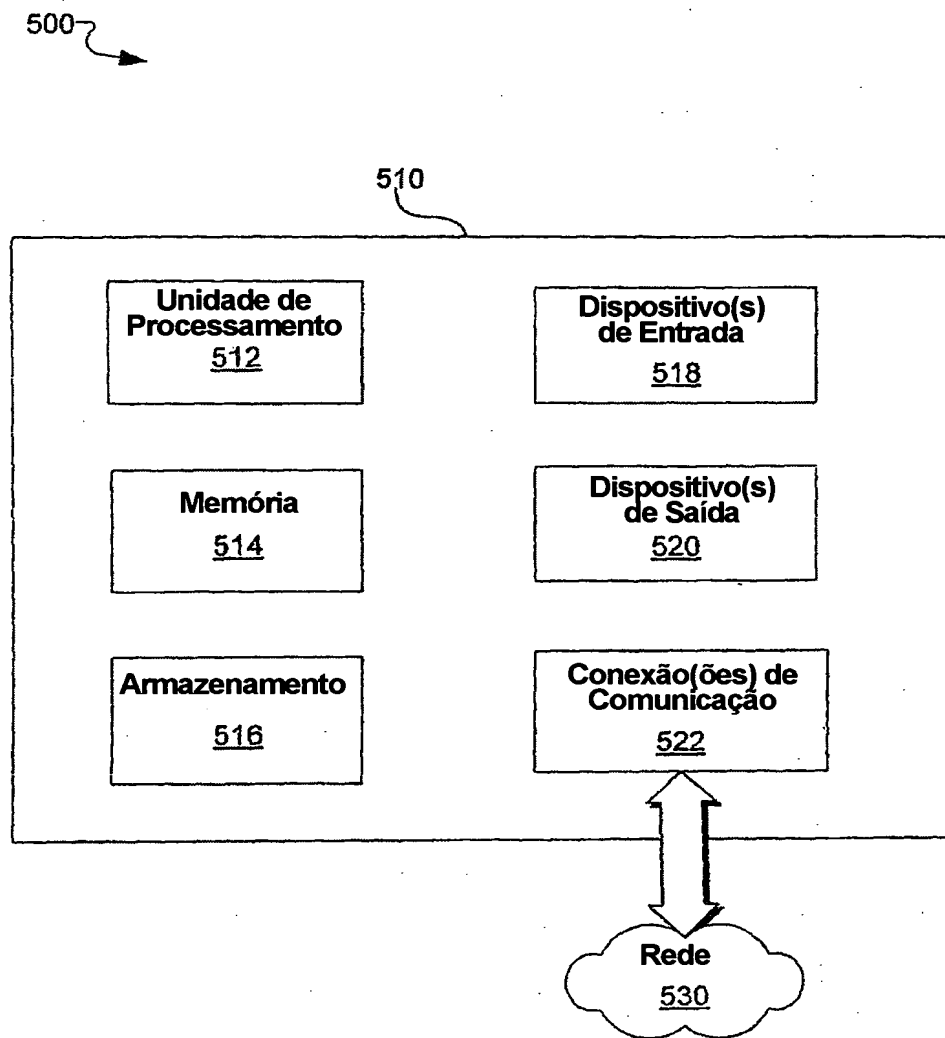


FIG. 5

RESUMO"ZONAS HABILITADAS POR DESAFIO DE NOME"

São aqui descritos um método e um sistema para implementar zonas habilitadas por desafio de nome. Um servidor DNS recebe uma atualização de um dispositivo de cliente.

- 5 Se o servidor DNS hospeda uma zona autorizada para a atualização, o servidor DNS determina se há um registro para o nome de hospedeiro. Se houver, então o endereço IP associado ao nome de hospedeiro é determinado. O endereço IP é comparado com o endereço de origem do dispositivo de cliente que envia a atualização. Se os endereços IP corresponderem um ao outro, então a atualização é aceita.

REIVINDICAÇÕES

1. Método, **CARACTERIZADO** por compreender:

receber uma atualização em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização incluindo um nome de hospedeiro;

5 determinar se o servidor DNS hospeda uma zona autorizada para a atualização;
determinar se já existe um registro para o nome de hospedeiro; e se existir,
determinar um endereço de Protocolo de Internet (IP) associado ao nome de hospedeiro;

10 determinar se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente; e
aceitar a atualização se os endereços IP correspondem um ao outro.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender aceitar a atualização se não houver registro para o nome de hospedeiro.

15 3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço IP associado ao nome de hospedeiro se o endereço IP associado ao nome de hospedeiro não corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

20 4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** adicionalmente por compreender rejeitar a atualização se uma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS.

5. Método, de acordo com a reivindicação 3, **CARACTERIZADO** adicionalmente por compreender aceitar a atualização se nenhuma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS.

25 6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender reproduzir a atualização para outro servidor DNS.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que determinar se já existe um registro para o nome de hospedeiro compreende verificar vários registros de vários tipos.

30 8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de Endereço (A).

9. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de endereço IPv6.

10. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de Nome Canônico (NOME).

35 11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a zona é suportada por arquivo.

12. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que

a zona é integrada com um sistema de diretórios.

13. Meio passível de leitura por dispositivo, **CARACTERIZADO** por ter instruções executáveis por dispositivo para executar etapas compreendendo:

receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nome de domínio (DNS) que hospeda uma zona autorizada para a atualização, a atualização incluindo um nome de hospedeiro;

verificar um ou mais registros na zona, de modo a determinar se já há um registro para o nome de hospedeiro, e se houver,

verificar o registro para o nome de hospedeiro, de modo a determinar o endereço de Protocolo Internet (IP) associado ao nome de hospedeiro;

determinar se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente, e se não corresponder,

enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço IP associado ao nome de hospedeiro; e

determinar se deve-se aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS.

14. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA-RACTERIZADO** pelo fato de que as etapas compreendem também aceitar a atualização se não houver registro para o nome de hospedeiro.

15. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA-RACTERIZADO** pelo fato de que as etapas compreendem também aceitar a atualização se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente.

16. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA-RACTERIZADO** pelo fato de determinar se deve-se aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS compreende rejeitar a atualização se o segundo dispositivo de cliente responder à consulta DNS e aceitar a atualização se o segundo dispositivo de cliente não responder à consulta DNS.

17. Método, **CARACTERIZADO** por compreender:

receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização incluindo um nome de hospedeiro;

determinar se já existe um registro para o nome de hospedeiro; e se existir,

determinar o endereço IP de um registrante do nome de hospedeiro;

determinar se o endereço IP de origem do registrando do nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente, e se não corresponder,

enviar uma consulta DNS ao registrando do nome de hospedeiro; e
rejeitar a atualização se uma confirmação for recebida do registrando em resposta à consulta DNS.

5 18. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se não houver registro para o nome de hospedeiro.

19. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se o endereço IP de origem do registrando do nome de hospedeiro corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

10 20. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se nenhuma resposta for recebida do registrando em resposta à consulta DNS.

REIVINDICAÇÕES

1. Método, **CARACTERIZADO** por compreender:

receber uma atualização em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização incluindo um nome de hospedeiro;

5 determinar se o servidor DNS hospeda uma zona autorizada para a atualização;
determinar se já existe um registro para o nome de hospedeiro; e se existir,
determinar um endereço de Protocolo de Internet (IP) associado ao nome de hospedeiro;

10 determinar se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente; e

aceitar a atualização se os endereços IP correspondem um ao outro.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender aceitar a atualização se não houver registro para o nome de hospedeiro.

15 3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço IP associado ao nome de hospedeiro se o endereço IP associado ao nome de hospedeiro não corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

20 4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** adicionalmente por compreender rejeitar a atualização se uma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS.

5. Método, de acordo com a reivindicação 3, **CARACTERIZADO** adicionalmente por compreender aceitar a atualização se nenhuma confirmação for recebida do segundo dispositivo de cliente em resposta à consulta DNS.

25 6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente por compreender reproduzir a atualização para outro servidor DNS.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que determinar se já existe um registro para o nome de hospedeiro compreende verificar vários registros de vários tipos.

30 8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de Endereço (A).

9. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de endereço IPv6.

10. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que um dos tipos de registro é um registro de Nome Canônico (NOME).

35 11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a zona é suportada por arquivo.

12. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que

a zona é integrada com um sistema de diretórios.

13. Meio passível de leitura por dispositivo, **CARACTERIZADO** por ter instruções executáveis por dispositivo para executar etapas compreendendo:

5 receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nome de domínio (DNS) que hospeda uma zona autorizada para a atualização, a atualização incluindo um nome de hospedeiro;

verificar um ou mais registros na zona, de modo a determinar se já há um registro para o nome de hospedeiro, e se houver,

10 verificar o registro para o nome de hospedeiro, de modo a determinar o endereço de Protocolo Internet (IP) associado ao nome de hospedeiro;

determinar se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente, e se não corresponder,

enviar uma consulta DNS a um segundo dispositivo de cliente que tem o endereço IP associado ao nome de hospedeiro; e

15 determinar se deve-se aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS.

14. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA- RACTERIZADO** pelo fato de que as etapas compreendem também aceitar a atualização se não houver registro para o nome de hospedeiro.

20 15. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA- RACTERIZADO** pelo fato de que as etapas compreendem também aceitar a atualização se o endereço IP associado ao nome de hospedeiro corresponde ao endereço IP de origem do primeiro dispositivo de cliente.

25 16. Meio passível de leitura por dispositivo, de acordo com a reivindicação 13, **CA- RACTERIZADO** pelo fato de determinar se deve-se aceitar a atualização com base em se o segundo dispositivo de cliente responder à consulta DNS compreende rejeitar a atualização se o segundo dispositivo de cliente responder à consulta DNS e aceitar a atualização se o segundo dispositivo de cliente não responder à consulta DNS.

17. Método, **CARACTERIZADO** por compreender:

30 receber uma atualização de um primeiro dispositivo de cliente em um servidor de sistema de nomes de domínio (DNS) de um primeiro dispositivo de cliente, a atualização incluindo um nome de hospedeiro;

determinar se já existe um registro para o nome de hospedeiro; e se existir,

determinar o endereço IP de um registrante do nome de hospedeiro;

35 determinar se o endereço IP de origem do registrando do nome de hospedeiro cor- responde ao endereço IP de origem do primeiro dispositivo de cliente, e se não correspon- der,

enviar uma consulta DNS ao registrando do nome de hospedeiro; e
rejeitar a atualização se uma confirmação for recebida do registrando em resposta à consulta DNS.

5 18. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se não houver registro para o nome de hospedeiro.

19. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se o endereço IP de origem do registrando do nome de hospedeiro corresponder ao endereço IP de origem do primeiro dispositivo de cliente.

10 20. Método, de acordo com a reivindicação 17, **CHARACTERIZADO** adicionalmente por compreender aceitar a atualização se nenhuma resposta for recebida do registrando em resposta à consulta DNS.