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

(21) **PI0710927-0 A2**

*BRPI0710927A2*

(22) Data de Depósito: 30/04/2007
**(43) Data da Publicação: 31/05/2011**
**(RPI 2108)**

***(51) Int.Cl.:***
**G06F 15/16 2006.01**
**H04Q 7/20 2006.01**

(54) Título: **OFERTA E FORNECIMENTO DE SERVIÇOS DE REDE PRIVADA VIRTUAL SEM FIO PROTEGIDOS**

(30) Prioridade Unionista: 28/04/2006 US 11/413.573

(73) Titular(es): Microsoft Corporation

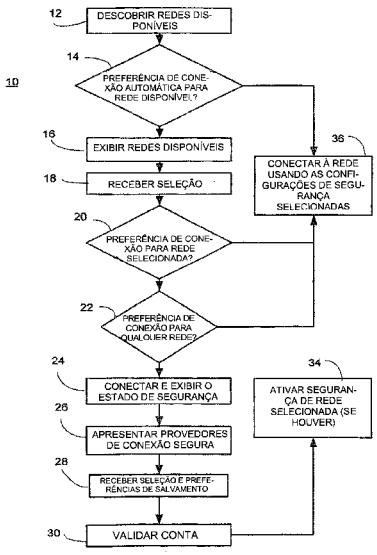
(72) Inventor(es): David Jones, Thomas W. Kuehnel

(74) Procurador(es): Nellie Anne Daniel Shores

(86) Pedido Internacional: PCT US2007010568 de 30/04/2007

(87) Publicação Internacional: WO 2007/127483de 08/11/2007

(57) Resumo: OFERTA E FORNECIMENTO DE SERVIÇOS DE REDE PRIVADA VIRTUAL SEM FIO PROTEGIDOS Um dispositivo eletrônico pode apresentar uma interface de usuário para fazer seleções relacionadas a conexão a uma rede ou seleção de uma rede a partir de uma pluralida- de de redes disponíveis. Adicionalmente, uma interface de usuário pode dar ao usuário uma oportunidade de proteger a uma conexão aberta e não segura, por exemplo, uma conexão ad-hoc sem fio, tal como pode ser encontrado em uma cafeteria. Uma seleção de ofertas de segurança pode ser feita a partir de uma tela de interface de usuário que inclui provedores de serviço pré-povoados. Pode ser permitido ao usuário salvar as preferências para se co- nectar a novas redes, bem como as preferências relacionadas às redes previamente usa- das. Ademais, o usuário pode salvar as preferências para convocar serviços de segurança em uma base por rede ou de panorama de rede. O serviço de segurança pode ser um pro- tocolo de tunelamento conhecido (isto é VPN), tal como o L2TP ou PPTP.



"OFERTA E FORNECIMENTO DE SERVIÇOS DE REDE PRIVADA VIRTUAL SEM FIO PROTEGIDOS"

Fundamentos da Invenção

A segurança do computador e a segurança das comunicações de dados com um computador têm sido uma preocupação por algum tempo. A proliferação de dispositivos de computação portáteis, laptops, PDAs, e similares, tem aumentado as oportunidades de brechas na segurança. Adicionalmente, a disponibilidade expandida de pontos de acesso de rede aberta, particularmente de pontos de acesso sem fio, tem também aumentado as oportunidades de brechas na segurança. Os funcionários móveis rotineiramente usam dispositivos eletrônicos portáteis em cafeterias, salas de espera de aeroportos, estacionamentos, ou mesmo quando visitam outras redes da corporação durante uma viagem de negócios. Freqüentemente, tais funcionários móveis são defrontados com uma escolha de não completar seu trabalho ou expor com risco dados confidenciais ou valiosos. Dada tal escolha, os funcionários móveis freqüentemente escolhem a última e esperam ser a melhor.

As tomadas seguras (SSL ou SSL2) podem ser usadas em um nível de aplicação para proteger as comunicações entre dois aplicativos, por exemplo, um navegador de rede e um servidor de pagamento. Entretanto, uma conexão SSL é somente efetiva para a única sessão de nível de aplicativo.

Os serviços de rede seguros ou redes privadas virtuais (VPN), tal protocolo de tunelamento de duas camadas (L2TP) e o protocolo de tunelamento ponto a ponto (PPTP), permitem proteger todas as comunicações entre os pontos finais pelas redes abertas (isto é, redes inseguras). Mas, a configuração e a manutenção de tais comunicações são incomodativas e freqüentemente solicitam ou conhecimento específico ou acesso do administrador.

Sumário da Invenção

Os dispositivos eletrônicos podem ser equipados com um gerenciador de conexão para gerenciar as conexões às redes disponíveis, especialmente as redes sem fio. O gerenciador de conexão pode monitorar as redes disponíveis e avaliar sua segurança relativa. Uma interface de usuário que apresenta as seleções de rede a um usuário pode indicar a natureza da conexão com relação à segurança. Quando uma seleção de uma rede aberta é feita, o usuário pode ser apresentado com uma opção para estabelecer uma conexão de rede segura que usa um serviço de rede segura, por exemplo, VPN.

Uma ou mais ofertas de serviços de rede segura podem ser programadas no dispositivo eletrônico para seleção pelo usuário. O gerenciador de conexão pode ser capaz de ativar o serviço de rede segura selecionado, resultando em uma conexão segura com pouca ou nenhuma ação da parte do usuário. As seleções de usuário com relação a uma rede particular podem ser armazenadas e solicitadas automaticamente quando subseqüentemente encontrando esta rede. Similarmente, as seleções de usuário com relação às conexões de

rede segura podem ser armazenadas e solicitadas automaticamente quando usando a rede particular novamente ou podem ser automaticamente solicitadas por qualquer rede subseqüentemente selecionada.

Por exemplo, um dispositivo eletrônico pode sempre conectar a sua própria rede de negócios quando disponível e não usará outras opções de rede. A rede de negócios pode não exigir um serviço de rede segura, enquanto o dispositivo eletrônico pode preferir uma rede particular de cafeteria a uma rede do posto de gasolina quando ambas estão disponíveis, mas pode optar em usar um serviço de rede segura quando conectando a qualquer uma.

Breve Descrição dos Desenhos

A Fig. 1 representa um diagrama de bloco representativo e simplificado de um dispositivo eletrônico;

A Fig. 2 representa uma topologia de rede que mostra uma variedade de conexões de rede;

A Fig. 3 representa um diagrama de bloco simplificado que mostra conexões lógicas e físicas entre um dispositivo eletrônico e um servidor;

A Fig. 4 representa uma tela de interface de usuário representativa para selecionar uma rede;

A Fig. 5 representa uma tela de interface de usuário representativa que apresenta informação de rede;

A Fig. 6 representa uma tela de interface de usuário representativa que mostra o estado da conexão;

A Fig. 7 representa uma tela de interface de usuário representativa que mostra o estado adicional;

A Fig. 8 representa uma tela de interface de usuário representativa que mostra o estado e a oferta de uma opção segura;

A Fig. 9 representa uma tela de interface de usuário representativa que oferece as seleções para serviços de rede segura;

A Fig. 10 representa uma tela de interface de usuário representativa para conectar a um serviço de rede segura;

A Fig. 11 representa uma tela de interface de usuário representativa para ativar uma conta com um serviço de rede segura;

A Fig. 12 representa uma tela de interface de usuário representativa para armazenar as configurações do serviço de rede segura;

A Fig. 13 representa uma tela de interface de usuário representativa para armazenar as configurações de conexão de rede; e

A Fig. 14 representa um fluxograma de um método exemplificado para selecionar e

proteger conexões de rede e armazenar as preferências relacionadas.

Descrição Detalhada da Invenção

Embora o texto seguinte apresente uma descrição detalhada de inúmeras modalidades diferentes, dever-se-ia entender que o escopo legal da descrição é definido pelas palavras das reivindicações apresentadas no fim desta descrição. A descrição detalhada é construída como exemplificada somente e não descreve cada possível modalidade visto que descrever cada possível modalidade seria impraticável, para não dizer impossível. Inúmeras modalidades alternativas poderiam ser implementadas, usando ou tecnologia atual ou tecnologia desenvolvida após a data de depósito desta patente, que ainda estaria dentro do escopo das reivindicações.

Dever-se-ia também entender que, a menos que um termo seja expressamente definido nesta patente usando a sentença "Como usado aqui, o termo '_____' é aqui definido como significando..." ou uma sentença similar, não existe a intenção de limitar o significado deste termo, ou expressamente ou por implicação, além de seu significado pleno e ordinário, e tal termo não deveria ser interpretado como sendo limitado em escopo baseado em qualquer determinação feita em qualquer seção desta patente (exceto a linguagem das reivindicações). No tocante a qualquer termo citado nas reivindicações no fim desta patente referido nesta patente de uma forma consistente com um único significado, isto é feito com o objetivo de esclarecimento para não confundir o leitor, e não se pretende que tal termo da reivindicação seja limitado, pela implicação ou de outra forma, a este único significado. Finalmente, a menos que um elemento de reivindicação seja definido citando a palavra "significa" e uma função sem citar qualquer estrutura, não se pretende que o escopo de qualquer elemento de reivindicação seja interpretado com base no pedido de 35 U.S.C. § 112, sexto parágrafo.

A maior parte da funcionalidade inventiva e dos princípios inventivos é melhor implementada com ou em programas de software ou instruções e circuitos integrados (CIs) tal como os CIs específicos de aplicativo. Espera-se que um versado na técnica, apesar do esforço possivelmente significativo e muitas escolhas de projetos motivadas, por exemplo, pelo tempo disponível, tecnologia atual, e considerações econômicas, quando guiadas pelos conceitos e princípios descritos aqui, seja prontamente capaz de gerar tais instruções de software e programas e CIs com experimentação mínima. Então, no interesse de brevidade e minimização de qualquer risco de obscurecer os princípios e conceitos de acordo com a presente invenção, a discussão adicional de tal software e tal CIs, se houver, será limitada ao essencial com relação aos princípios e conceitos das modalidades preferidas.

A Fig. 1 fornece uma base estrutural para um dispositivo eletrônico adequado para executar os métodos e hospedar os meios legíveis por computador relacionados à descrição. O dispositivo eletrônico 110 pode ser um computador padrão, porém também pode ser

um dispositivo portátil adequado para uso por um funcionário móvel. Os dispositivos eletrônicos exemplificados podem incluir um computador laptop, um computador portátil, um assistente digital pessoal (PDA), um telefone inteligente, e uma ferramenta de protocolo de internet por voz (VoIP).

A Fig. 1 ilustra um dispositivo de computação na forma de um dispositivo eletrônico 110. Os componentes do dispositivo eletrônico 110 podem incluir, porém não são limitados a uma unidade de processamento 120, a uma memória de sistema 130, e a um barramento de sistema 121 que acopla vários componentes de sistema incluindo a memória de sistema à unidade de processamento 120. O barramento de sistema 121 pode ser qualquer um dos vários tipos de estruturas de barramento incluindo um barramento de memória ou um controlador de memória, um barramento periférico, e um barramento local que usa qualquer uma das variedades de arquiteturas de barramento. A título de exemplo, e não limitação, tais arquiteturas incluem o barramento de Arquitetura Padrão de Indústria (ISA), barramento de Arquitetura de Micro-canal (MCA), barramento ISA Aperfeiçoado (EISA), barramento local de Associação de Padrões Eletrônicos de Vídeo (VESA), e barramento de Componentes Periféricos Interconectados (PCI), mas também conhecido como barramento Mezzanine.

O dispositivo eletrônico 110 tipicamente inclui uma variedade de meios legíveis por computador. Esses podem ser quaisquer meios disponíveis que podem ser acessados pelo dispositivo eletrônico 110 e incluem ambos os meios voláteis e não voláteis, removíveis e não removíveis. A título de exemplo, e não limitação, meios legíveis por computador podem compreender meios de armazenamento por computador e meios de comunicação. Os meios de armazenamento por computador incluem meios voláteis e não voláteis, removíveis e não removíveis implementados em qualquer método ou tecnologia para armazenamento de informação tal como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados. Os meios de armazenamento por computador incluem, mas não estão limitados a, RAM, ROM, EEPROM, memória rápida ou outra tecnologia de memória, CD-ROM, discos versáteis digitais (DVD) ou outro armazenamento em disco óptico, cassetes magnéticos, fita magnética, armazenamento em disco magnético ou outros dispositivos de armazenamento magnéticos, ou qualquer outro meio que pode ser usado para armazenar a informação desejada e que pode ser acessado pelo dispositivo eletrônico 110. Os meios de comunicação tipicamente incorporam 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 incluem quaisquer meios de entrega de informação. O termo "sinal modulado de dados" significa um sinal que tem uma ou mais de suas características ajustadas ou alteradas de tal maneira a codificar informação no sinal. A título de exemplo, e não limitação, os meios de comunicação incluem meios por fios tais como uma rede por fios ou conexão direta por fios, e meios sem fio tais como acús-

ticos, radiofreqüência, infravermelhos e outros meios sem fio. Combinações de qualquer um dos acima deveriam ser também incluídas no escopo dos meios legíveis por computador.

A memória de sistema 130 inclui meios de armazenamento por computador na forma de memória volátil e/ou não volátil, tal como memória somente de leitura (ROM) 131 e memória de acesso aleatório (RAM) 132. Um sistema de entrada/saída básico (BIOS) 133, contendo as rotinas básicas que ajudam a transferir informação entre elementos no computador 110, tal como durante a inicialização, é tipicamente armazenado na ROM 131. A RAM 132 tipicamente contém dados e/ou módulos de programa que são imediatamente acessíveis e/ou estão presentemente sendo operados pela unidade de processamento 120. A título de exemplo, e não limitação, a FIG. 1 ilustra o sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137.

O dispositivo eletrônico 110 pode também incluir outros meios de armazenamento por computador removíveis/não removíveis, voláteis/não voláteis. A título de exemplo somente, a Fig. 1 ilustra uma unidade de disco rígido 141 que lê a partir de e escreve em meios magnéticos não removíveis e não voláteis, uma unidade de disco magnético 151 que lê a partir de e escreve em discos magnéticos removíveis e não voláteis 152, e uma unidade de disco óptico 155 que lê a partir de e escreve em um disco óptico removível e não volátil 156, tal como um CD-ROM, DVD ou outro meio óptico. Outros meios de armazenamento por computador removíveis/não removíveis, voláteis/não voláteis que podem ser usados no ambiente operacional exemplificado incluem, mas não estão limitados a, fitas cassetes magnéticas, cartões de memória rápida, discos versáteis digitais, fita de vídeo digital, RAM de estado sólido, ROM de estado sólido, e seus similares. A unidade de disco rígido 141 é tipicamente conectada ao barramento de sistema 121 através de uma interface de memória não removível tal como a interface 140, e a unidade de disco magnético 151 e a unidade de disco óptico 155 são tipicamente conectadas ao barramento de sistema 121 por uma interface de memória removível, tal como a interface 150.

As unidades e seus meios de armazenamento por computador associados discutidos acima e ilustrados na Fig. 1, fornecem armazenamento de instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o dispositivo eletrônico 110. Na Fig. 1, por exemplo, a unidade de disco rígido 141 é ilustrada como armazenando o sistema operacional 144, programas de aplicação 145, outros módulos de programa 146, e dados de programa 147. Nota-se que esses componentes podem ou ser os mesmos ou diferentes do sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137. Ao sistema operacional 144, aos programas de aplicação 145, a outros programas 146 e aos dados de programa 147 são atribuídos números diferentes aqui para ilustrar que, no mínimo, eles são cópias diferentes. Um usuário pode inserir comandos e informação no dispositivo eletrônico 110 através de dispo-

sitivos de entrada, tais como um teclado 162 e um dispositivo de controle de cursor 161, comumente referido como um mouse, mouse estacionário ("trackball") ou mesa sensível ao toque. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, um comando de jogos, mesa de jogos, antena de satélite, digitalizador, ou seus similares. Esses e outros dispositivos de entrada são freqüentemente conectados à unidade de processamento 120 através de uma interface de entrada de usuário 160 que está acoplada ao barramento de sistema, mas pode estar conectada por outra interface e estruturas de barramento, tais como uma porta paralela, porta de jogos ou um barramento serial universal (USB). Um dispositivo de exibição 191 é também conectado ao barramento de sistema 121 via uma interface, tal como um controlador de gráficos 190. Em adição à tela 191, os dispositivos eletrônicos externos ou periféricos podem ser conectados ao dispositivo eletrônico 110 via a interface periférica de saída 195. Tais dispositivos periféricos de saída podem incluir alto-falantes ou uma impressora (não descrita), embora eles não sejam geralmente usados durante a operação móvel.

O dispositivo eletrônico 110 pode operar em um ambiente de rede usando conexões lógicas a um ou mais computadores remotos, tal como um computador remoto 180. O computador remoto 180 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo não hierárquico ou outro nó de rede comum, e tipicamente inclui muitos ou todos os elementos descritos acima em relação ao dispositivo eletrônico 110. As conexões lógicas representadas na Fig. 1 incluem uma rede de área local (LAN) 171, mas podem também incluir outras redes, tal como uma rede de área ampla ou a internet. Tais ambientes de rede são comuns em escritórios, redes de computador de grandes empresas, intranets, e redes não hierárquicas.

Quando usado em um ambiente de rede LAN, o dispositivo eletrônico 110 pode ser conectado à LAN 171 através de uma interface de rede ou adaptador 170. Em um ambiente de rede, os módulos de programa (não descritos) relevantes ao dispositivo eletrônico 110, ou partes desse, podem ser armazenados no dispositivo de armazenamento remoto em memória.

A conexão de comunicações 170 permite que o dispositivo se comunique com outros dispositivos. A conexão de comunicações 170 é um exemplo de meios de comunicação. Os meios de comunicação tipicamente incorporam 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 incluem quaisquer meios de entrega de informação. Um "sinal modulado de dados" pode ser um sinal que tem uma ou mais de suas características ajustadas ou mudadas de tal forma a codificar a informação no sinal. A título de exemplo, e não limitação, os meios de comunicação incluem meios por fio tal como rede por fio ou conexão direta por fio, e meios sem fio tais como acústico, RF,

infravermelho e outros meios sem fio. Os meios legíveis por computador podem incluir ambos os meios de armazenamento e meios de comunicação.

A Fig. 2 representa uma topologia de rede que mostra uma variedade de conexões de rede. Um dispositivo eletrônico 202 é mostrado acoplado através de um número de redes, protocolos, e meios a uma rede de área ampla 204, tal como a internet, um rede corporativa, ou um provedor de serviço de Internet (ISP). O dispositivo eletrônico 202 pode ser o mesmo ou similar ao dispositivo eletrônico 110 da Fig. 1. As conexões ilustradas não estão necessariamente disponíveis ao mesmo tempo, nem o dispositivo eletrônico 202 está necessariamente conectado a mais de uma rede por vez, se conectado a todas.

A Fig. 2 mostra o dispositivo eletrônico 202 conectado a uma rede doméstica 206 via uma conexão por fio 208, embora as conexões sem fio em ambientes domésticos sejam cada vez mais comuns. Uma cafeteria 212 ilustra outra localização de acesso de rede, nesta modalidade exemplificada, a conexão entre o dispositivo eletrônico 202 e a cafeteria 212 está sobre conexão sem fio 214. A cafeteria pode ser conectada à rede de área ampla 204 pela conexão 216. Outro ponto de acesso pode ser representado pelo aeroporto 218. Uma conexão sem fio 220 pode ser usada para acoplar o dispositivo eletrônico 202 ao aeroporto 218 e subseqüentemente, à rede de área ampla 204 pela conexão 222.

Quando o dispositivo eletrônico 202 está no alcance de uma rede sem fio, por exemplo, as redes 214 e 220, ou está fisicamente conectado a uma rede por fio, por exemplo, a rede 208, uma interface de usuário pode ser apresentada no dispositivo eletrônico 202 para convidar um usuário a selecionar uma rede e, quando a rede selecionada não é segura, adicionar segurança à rede. A interface de usuário e os processos de seleção são discutidos em mais detalhes abaixo com relação às Figs. 4 a 13. A segurança de rede pode incluir um ou todos os elementos de AAA, ou seja, a autenticação, autorização e contabilidade. Por exemplo, uma conexão de rede segura ou VPN pode garantir que os pacotes não são adulterados ou sorvidos enquanto encaminhados entre pontos finais.

A Fig. 3 é diagrama de bloco representativo e simplificado que mostra conexões físicas e lógicas entre um dispositivo eletrônico e uma rede. Um dispositivo eletrônico 302 pode conectar a um computador 304 por uma conexão de rede 306. O computador 304 pode ser um ponto de acesso, um servidor de acesso local (LAS), porta de comunicação, ou similares. A conexão de rede 306 pode ser por fio ou sem fio, como mostrado na Fig. 2. O computador 304 pode ser conectado a uma rede de área ampla 308, tal como a internet, ou conexão de rede 310. A rede de área ampla 308, tal como a internet, ou conexão de rede 310. A rede de área ampla 308, por sua vez, pode ser conectada a um provedor de serviços 312 e adicionalmente a um computador de ponto final 314. Em algumas modalidades, o provedor de serviços 312 pode não estar presente e as conexões lógicas e físicas podem diretamente se acoplar ao computador de ponto final 314.

Uma conexão lógica 316 pode ser feita entre o dispositivo eletrônico 302 e o computador de ponto final 314, embora a conexão física seja via as redes 306 e 310 e os pontos intermediários 304 e 308 e, opcionalmente 312. A conexão lógica 316 pode usar um dos vários protocolos especializados para proteger a conexão entre os pontos finais. Por exemplo, um protocolo de tunelamento de duas camadas (L2TP), conhecido na técnica, encapsula os dados oriundos ou do ponto final 302 ou 314 e os passa através das várias redes físicas e em um modelo seguro até que eles alcancem o outro ponto final e é o encapsulado apresentado à pilha de protocolos do ponto final de recebimento. Outro tal protocolo é o protocolo de tunelamento ponto a ponto (PPTP).

Em uma modalidade, um cliente pode ser instalado no dispositivo eletrônico 302 para suportar a configuração, operação e destruição do lado do cliente do protocolo de tunelamento quando o provedor de serviço está presente e uma conexão confiável e segura entre o computador de ponto final 314 e o provedor de serviço 312 existe, a conexão de comunicação segura 316 pode terminar no provedor de serviço 312. O provedor de serviço 312 pode ser um serviço comercial, um serviço livre, ou um serviço oferecido por uma empresa associada a seus próprios usuários. O software de aplicação de lado de cliente de mais de um provedor de serviço pode ser pré-instalado em um dispositivo eletrônico 302 e apresentado para seleção pelo usuário no momento de uma conexão de rede ser feita. Como será discutido, ambas a seleção de rede e preferências de serviço seguro podem ser armazenadas para uso futuro.

Em outra modalidade, uma série de módulos de software pode suportar as operações associadas com ambas conectar-se a uma rede, monitorar a segurança da conexão, e ativar os serviços necessários para suportar uma conexão VPN. Um módulo de monitor de rede pode ser implementado para determinar a disponibilidade de uma rede, especialmente uma rede sem fio. Um módulo gerenciador de apresentação pode operar em conjunto com o monitor de rede e apresentar as redes disponíveis. O gerenciador de apresentação pode também apresentar as ofertas de segurança de rede. Um módulo gerenciador de ligação pode ser usado para ativar uma oferta de segurança selecionada quando o gerenciador de apresentação recebe as seleções a partir de um usuário. As seleções podem incluir ambas uma seleção de uma rede e uma oferta de segurança de seleção (por exemplo, fornecedor) ou exigência de segurança (por exemplo, uma exigência por uma VPN).

Um módulo gerenciador de configuração para salvar as configurações correspondentes para repetir os comportamentos selecionados quando o monitor de rede determina a disponibilidade subseqüente da rede sem fio. Um módulo gerenciador de pré-carga pode armazenar uma ou mais ofertas de segurança de rede. Como discutido abaixo, uma implementação do gerenciador de pré-carga pode ser um kit de pré-instalação OEM. Um módulo gerenciador de configuração pode operar em conjunto com o gerenciador de apresentação

para salvar as configurações correspondentes para proteger automaticamente todas as futuras conexões de rede, quando uma resposta coletada pelo gerenciador de apresentação indica que o usuário prefere usar um serviço de segurança para as conexões de rede não seguras.

A Fig. 4 representa uma tela de interface de usuário para selecionar uma rede. A janela 400 mostra que uma série de redes foram detectadas como estando disponíveis, especificamente, uma rede 402 com uma indicação 404 de que a conexão pode não ser segura, uma rede 406 com uma indicação 408 de que o disponível eletrônico principal, tal como o dispositivo eletrônico 302 da Fig. 3, já está conectado, e uma rede 410, por exemplo, um grupo de redes não hierárquicas ad hoc, com uma indicação 412 de que a rede está disponível e possui segurança habilitada. As seleções adicionais podem incluir uma opção por outras conexões para cem 14 e uma opção para gerenciar a rede sem fio 416. Os botões de cancelar 420 e de conectar 418 podem ser usados para navegar a partir da janela 400. Para o propósito de exemplo, o usuário seleciona a rede do HotelFiat 402.

A Fig. 5, uma tela de interface de usuário representativa 500 apresentando a informação de rede é discutida e descrita. Depois de receber uma seleção de rede, por exemplo, na Fig. 4, um gerenciador de conexão no dispositivo eletrônico 302 pode apresentar informação sobre a rede selecionada. A tela de interface 500 pode notificar um usuário via a mensagem 502 de que a rede selecionada, neste caso o HotelFiat, não é segura. As opções podem ser apresentadas, por exemplo, uma oferta para proteger a rede 504, uma opção para conectar-se sem segurança 506, e uma oferta para conectar a outra rede 508. Selecionando a oferta para conectar a outra rede 508 pode, de fato, retornar o usuário à tela da Fig. 4. Para continuar o exemplo, a primeira seleção 504 é escolhida.

A Fig. 6 representa uma tela de interface de usuário representativa 600 mostrando o estado 602. Similarmente, a Fig. 7 representa uma tela de interface de usuário representativa 700 mostrando o estado adicional 702.

A Fig. 8 mostra uma tela de interface de usuário representativa 800 mostrando o estado 802 indicando que a conexão de rede foi completada. Como na Fig. 5, a seleção 504 foi feita solicitando a auxílio na segurança da conexão, a seleção 804 pode ser apresentada. A seleção 804 permite que o usuário continue a proteger a rede. Para esta modalidade exemplificada, a seleção 804 é escolhida.

A Fig. 9 mostra uma tela de interface de usuário representativa 900 que oferece as seleções para proteger a conexão de rede. Como discutido acima, o software de cliente pode ser instalado no dispositivo eletrônico 302 suportando as conexões seguras. O software de cliente pode ser pré-instalado no momento da fabricação ou na programação inicial, pode ser transferido pós-fabricação, ou mesmo na pós-entrega a um consumidor. Três seleções de segurança de rede exemplificadas são mostradas na Fig. 9, o primeiro provedor 902, o

segundo provedor 904, e o terceiro provedor 906. No mínimo um botão 908 pode ser usado para prosseguir.

Quando o software de cliente é pré-instalado, ele pode ser pré-instalado através de um kit de pré-instalação do fabricante de equipamento original (OEM), tal como uma ferramenta disponível através da Microsof™, ou uma ferramenta equivalente. O kit de pré-instalação OEM permite que um fornecedor de produto especifique o tipo de oferta que está sendo feita a um usuário, bem como um texto específico e gráfico associados à oferta. As categorias exemplificadas para oferecer a pré-instalação são mostradas abaixo.

Para fornecer aos OEMs a capacidade de alterar o comportamento padrão das redes seguras, eles podem fornecer um objeto grande binário XML (blob) que contém a seguinte informação, ou similar.

VPNOffer padrão: Determina a(s) opções para apresentação ao usuário. Quando configurado para 1, a oferta é apresentada, quando configurado para 0, a oferta não é apresentada.

VPNTitleText padrão: Personaliza a descrição da seqüência de textos para a página de oferta VPN (substitui a seqüência padrão "Para registrar agora, selecionar um provedor de segurança sem fio").

VPNIconPath padrão: Localização do ícone do serviço VPN padrão (um para cada entrada).

VPNdescription padrão: Personaliza a descrição da seqüência de texto/informação de oferta.

VPNlocation padrão: Configura um caminho de execução de programa padrão para inicializar o instalador do serviço VPN sem fio/sítio da rede padrão.

A Fig. 10 representa uma tela de interface de usuário representativa 1000 para conectar-se a um serviço de rede segura que permite a apresentação de detalhes adicionais 1002 pelo provedor de oferta e confirmação 1004 do serviço selecionado pelo usuário.

A Fig. 11 representa uma tela de interface de usuário representativa 1100 para ativar uma conta com um serviço de rede segura. Após a confirmação da seleção do serviço na Fig. 10, a tela de interface 1100 pode ser apresentada para permitir que o usuário complete os campos de registro 1102 e selecione uma linguagem usando a janela suspensa 1104. Quando completado, o botão 1106 permite prosseguir para a próxima tela.

A Fig. 12 representa uma tela de interface de usuário representativa 1200 para armazenar as configurações de serviço de rede segura. Várias seleções podem ser escolhidas por um usuário para uso subseqüente quando conectando às redes, incluindo redes sem fio. A seleção 1202 permite que um usuário automaticamente proteja todas as futuras conexões de rede. Quando a seleção 1202 é escolhida, a seleção 1024 permite que o usuário solicite a apresentação de avisos relacionados à proteção de redes que não foram previamente a-

cessadas. A seleção 1206 permite que o serviço seguro particular execute as atualizações automáticas. Quando as seleções forem completadas, o botão de seleção 1208 pode ser usado para fechar a janela e prosseguir.

A Fig. 13 é uma tela de interface de usuário representativa 1300 para armazenar as configurações de conexão de rede para uma rede particular. A seleção 1302 especifica que a rede atualmente selecionada, na modalidade exemplar, a rede 'HotelFiat' deveria ser automaticamente conectada sempre que estiver disponível no futuro. A seleção 1304 permite que o usuário especifique que outros usuários do mesmo dispositivo eletrônico 302 podem também se conectar à rede selecionada. A seleção 1306 permite que um usuário especifique automaticamente a proteção futura de todas as conexões com a rede selecionada, neste exemplo, 'HotelFiat'. O botão 1308 pode ser usado para fechar a janela e continuar a operação normal. As seleções feitas nas Figs. 12 e 13 podem ser usadas pelas sessões futuras para determinar como manipular as redes conhecidas à medida que elas se tornam disponíveis.

A Fig. 14 representa um fluxograma de um método exemplificado 10 para selecionar e proteger as conexões de rede e armazenar as preferências relacionadas. No bloco 12, um gerenciador de conexão, ou componente similar, pode descobrir uma ou mais redes e determinar quando no mínimo uma rede está disponível para uma conexão. No bloco 14, um valor correspondente às configurações de rede pode ser lido para determinar se as instruções ou preferências estão disponíveis relacionadas a qualquer uma das redes descobertas no bloco 12. Se as instruções ou preferências anteriores são encontradas, elas podem ser seguidas e podem especificar que uma das redes é automaticamente conectada e talvez automaticamente protegida.

Se nenhuma instrução está disponível no bloco 14, uma interface de usuário pode ser solicitada no bloco 16 para exibir as redes disponíveis e, no bloco 18, para receber uma seleção de uma rede com que se conectar, ou para receber uma seleção para não conectar com qualquer rede.

Quando uma rede é selecionada, as preferências podem novamente ser verificadas no bloco 20 para determinar se uma preferência de conexão foi feita para essa rede selecionada particular, por exemplo, para proteger sempre uma conexão com essa rede particular. Quando nenhuma preferência é encontrada para a rede selecionada particular, no bloco 22 uma determinação pode ser feita se existe uma preferência de conexão para qualquer rede em geral, obviamente, incluindo a rede atualmente selecionada. Quando nenhuma preferência de conexão geral é encontrada, a rede selecionada pode ser conectada e o estado de segurança exibido no bloco 24.

Se o usuário solicitou ajuda na proteção da conexão de rede ou no bloco 18 ou no bloco 24, uma interface de usuário pode ser exibida no bloco 26 oferecendo para proteger a

conexão de rede. Quando mais de um provedor de serviço de rede segura for fornecido, o usuário pode fazer uma seleção das escolhas disponíveis e da seleção recebida no bloco 28. Quando indicado pelo usuário, as seleções feitas no bloco 28 podem ser salvas para referência futura quando se conectando subseqüentemente à mesma rede, ou para uso adicional quando determinando para proteger as conexões a outras novas redes.

Quando solicitado, um processo de validação de conta pode ser completado no bloco 30 e a rede pode ser protegida, por exemplo, usando um protocolo de tunelamento L2TP ou PPTP no bloco 34.

Quando as preferências para conexão de rede são encontradas nos blocos 14, 20, ou 22, uma conexão à rede preferencial pode ser feita no bloco 36, e, quando assim indicado, a conexão protegida.

Embora o texto anterior apresente uma descrição detalhada de inúmeras diferentes modalidades da invenção, dever-se-ia entender que o escopo da invenção é definido pelas palavras das reivindicações apresentadas no fim desta patente. A descrição detalhada é construída como exemplificada somente e não descreve cada possível modalidade da invenção porque descrever cada possível modalidade seria impraticável, se não impossível. Inúmeras modalidades alternativas poderiam ser implementadas, usando ou a tecnologia atual ou a tecnologia desenvolvida após a data de depósito desta patente, que ainda estaria no escopo das reivindicações que definem a invenção.

Assim, muitas modificações e variações podem ser feitas nas técnicas e estruturas descritas e ilustradas aqui sem abandonar o espírito e escopo da presente invenção. Conseqüentemente, dever-se-ia entender que os métodos e aparelhos descritos aqui são somente ilustrativos e não são limitantes do escopo desta invenção.

## REIVINDICAÇÕES

1. Método para proteger uma conexão de rede, **CARACTERIZADO** pelo fato de que compreende:

determinar quando pelo menos uma das redes (214, 220) está disponível para uma conexão;

apresentar uma interface de usuário (400) para fazer uma seleção correspondente a pelo menos uma rede;

receber uma indicação de uma rede selecionada (214);

determinar quando a rede selecionada (214) não é segura;

apresentar uma interface de usuário (900) correspondente a um serviço para proteger a conexão de rede;

receber uma resposta para oferecer o serviço; e

armazenar um valor correspondente a um do serviço e da rede selecionada (214) para uso durante uma sessão de rede subseqüente.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente pelo fato de que compreende ler um valor correspondente às configurações de rede após determinar quando no mínimo uma conexão de rede está disponível, onde o valor corresponde às instruções para um de conectar e proteger no mínimo uma conexão de rede.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente pelo fato de que compreende instalar um gerenciador de conexão de rede.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente pelo fato de que compreende proteger a conexão de rede quando o recebimento de uma resposta à oferta do serviço é afirmativa.

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que proteger a conexão de rede compreende proteger a conexão de rede usando um de um protocolo de tunelamento de duas camadas (L2TP) e um protocolo de tunelamento ponto a ponto (PPTP).

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que armazenar o valor correspondente a um dos serviços e no mínimo uma sessão de rede compreende armazenar um primeiro valor para proteger qualquer conexão de rede usando o serviço.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que armazenar o valor correspondente a um dos serviços e no mínimo uma sessão de rede compreende armazenar um primeiro valor para replicar o gerenciamento da conexão de rede quando no mínimo uma rede está disponível em uma sessão subseqüente.

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que armazenar o valor correspondente a um dos serviços e no mínimo uma sessão de rede

compreende armazenar um primeiro valor para usar o serviço quando selecionando subseqüentemente no mínimo uma rede.

9. Meio legível por computador (130, 141) para armazenar as instruções executáveis por computador para implementar um gerenciador de conexão sem fio em um dispositivo eletrônico, **CARACTERIZADO** pelo fato de que compreende:

um módulo monitor de rede para determinar a disponibilidade de uma rede sem fio (214);

um módulo gerenciador de apresentação acoplado ao monitor de rede para apresentar a disponibilidade da rede sem fio (214) e para apresentar as ofertas de segurança de rede;

um módulo gerenciador de ligação para ativar uma oferta de segurança responsiva ao gerenciador de apresentação que recebe uma seleção da rede sem fio e a oferta de segurança.

10. Meio legível por computador, de acordo com a reivindicação 9, **CARACTERIZADO** adicionalmente pelo fato de que compreende um módulo gerenciador de configuração para salvar as configurações correspondentes para repetir os comportamentos selecionados quando o monitor de rede determina a disponibilidade da rede sem fio.

11. Meio legível por computador, de acordo com a reivindicação 9, **CARACTERIZADO** adicionalmente pelo fato de que compreende um módulo gerenciador de pré-carga para armazenar uma ou mais ofertas de segurança de rede.

12. Meio legível por computador, de acordo com a reivindicação 9, **CARACTERIZADO** adicionalmente pelo fato de que compreende um módulo gerenciador de configuração para salvar as configurações correspondentes para proteger automaticamente todas as conexões de rede sem fio, responsivas a uma instrução para proteger automaticamente todas as conexões de rede sem fio.

13. Método para gerenciar conexões sem fio, (214, 220) aos provedores de rede não segura (212, 218) em um dispositivo eletrônico (202), **CARACTERIZADO** pelo fato de que compreende:

instalar um gerenciador de conexão segura no dispositivo eletrônico (202);

instalar um cliente para um serviço de segurança de rede (902, 904, 906);

apresentar uma interface de usuário (500) para receber uma preferência para proteger uma conexão a um selecionado dos provedores de rede não segura (212);

armazenar a preferência para proteger a conexão a um provedor de rede não segura selecionado (212);

anexar ao provedor de rede não segura selecionado (212) usando uma conexão não segura;

solicitar que o gerenciador de conexão segura se conecte ao serviço de segurança

de rede (902, 904, 906) de acordo com a preferência armazenada.

14. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o serviço de segurança de rede é um serviço seguro de protocolo de tunelamento de duas camadas.

15. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o serviço de segurança de rede é um protocolo de tunelamento de ponto a ponto.

16. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que instalar um cliente para um serviço de segurança de rede compreende instalar uma oferta de serviço usando um kit de pré-instalação OEM no momento da fabricação do dispositivo eletrônico (202).

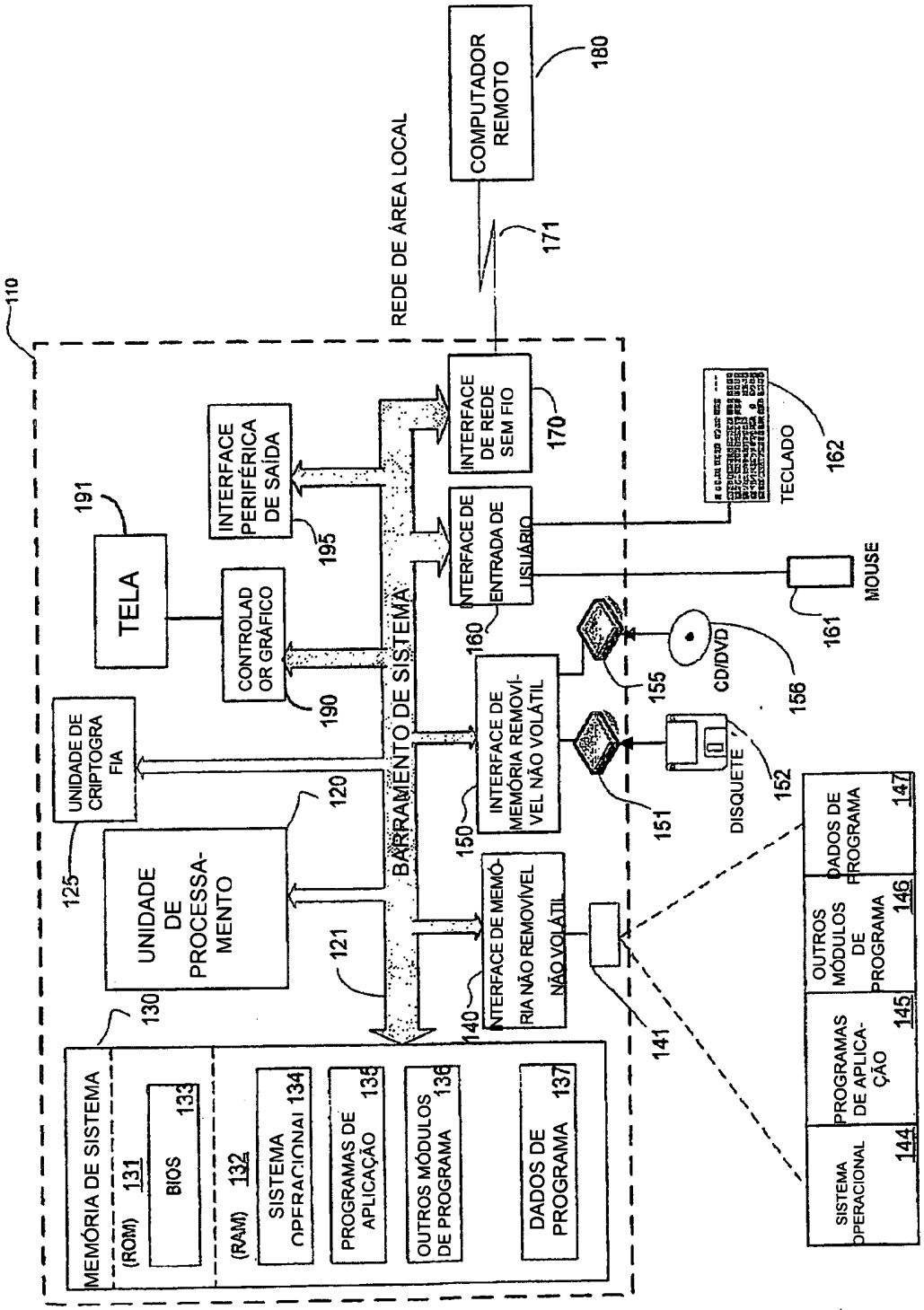

110
REDE DE ÁREA LOCAL
COMPUTADOR REMOTO
180
171
INTERFACE DE REDE SEM FIO
170
INTERFACE PERIFÉRICA DE SAÍDA
195
191
TELA
CONTROLADOR GRÁFICO
190
INTERFACE DE ENTRADA DE USUÁRIO
160
TECLADO
162
MOUSE
161
BARRAMENTO DE SISTEMA
UNIDADE DE CRIPTOGRAFIA
125
UNIDADE DE PROCESSAMENTO
120
INTERFACE DE MEMÓRIA REMOVÍVEL NÃO VOLÁTIL
150
155
CD/DVD
156
DISQUETE
152
151
INTERFACE DE MEMÓRIA NÃO REMOVÍVEL NÃO VOLÁTIL
140
121
130
MEMÓRIA DE SISTEMA
(ROM) 131
BIOS 133
(RAM) 132
SISTEMA OPERACIONAL 134
PROGRAMAS DE APLICAÇÃO 135
OUTROS MÓDULOS DE PROGRAMA 136
DADOS DE PROGRAMA 137
141
DADOS DE PROGRAMA 147
OUTROS MÓDULOS DE PROGRAMA 146
PROGRAMAS DE APLICAÇÃO 145
SISTEMA OPERACIONAL 144

Fig. 1

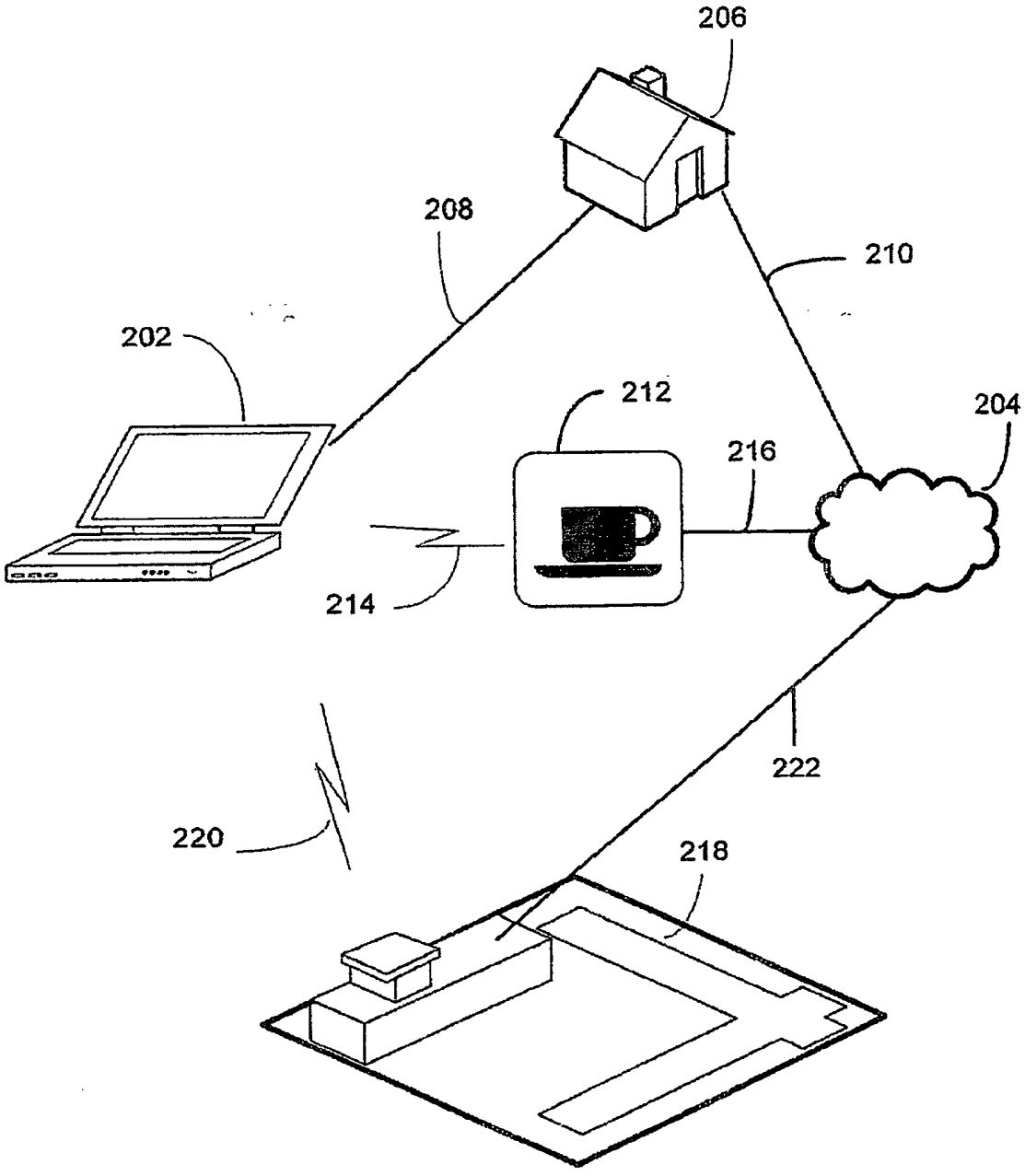



Fig. 2

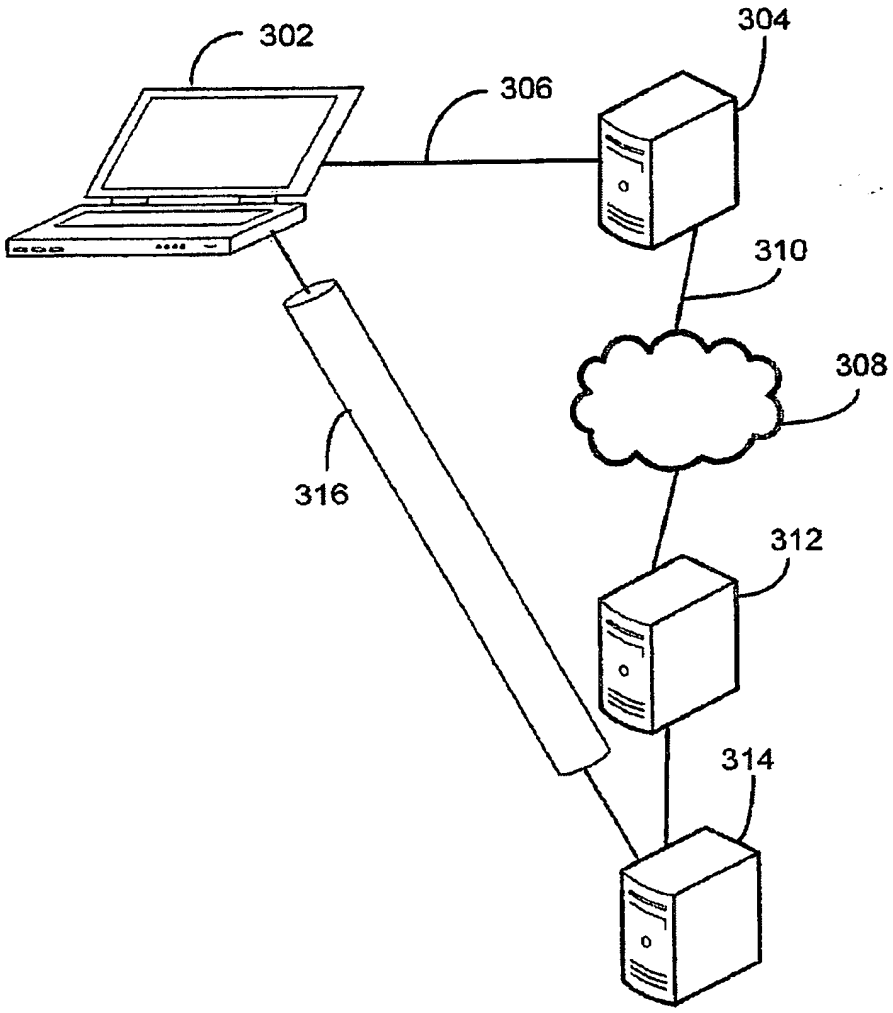



Fig. 3

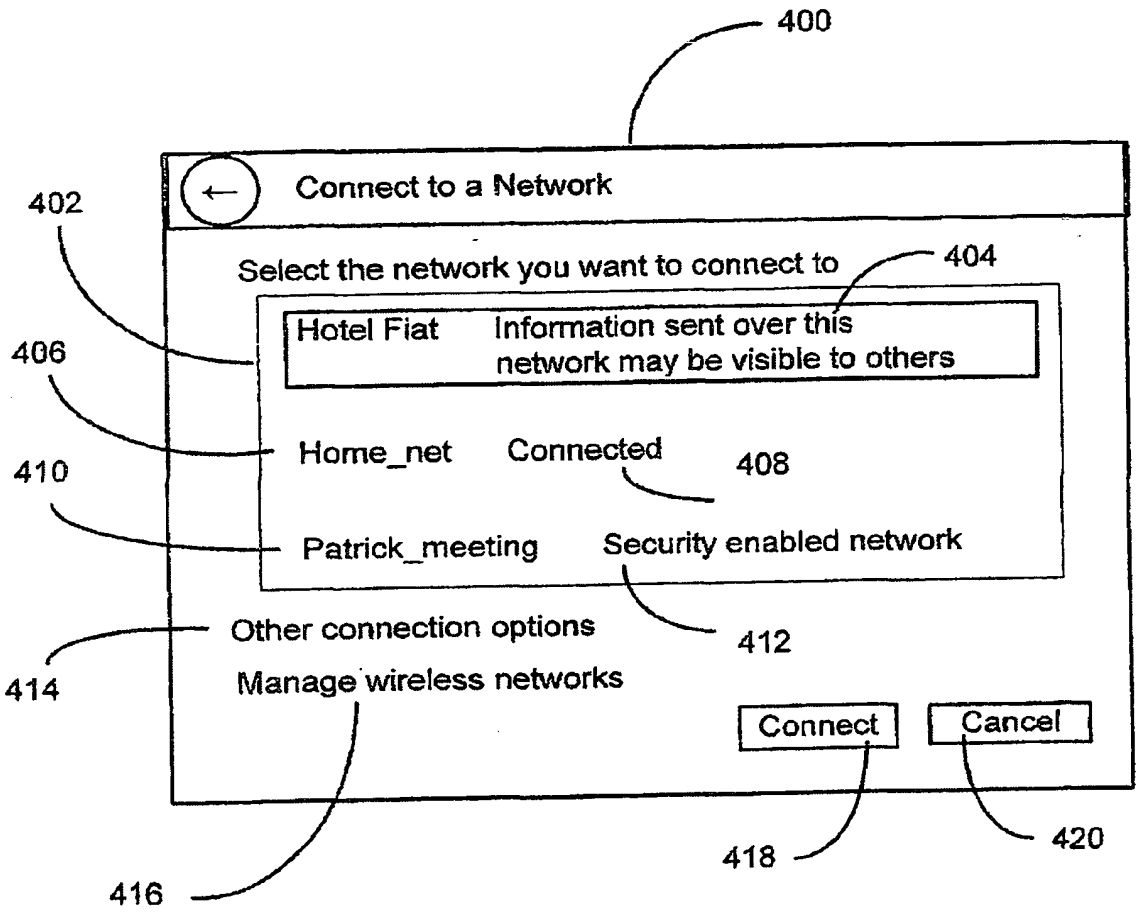

400
Connect to a Network
402
Select the network you want to connect to
404
Hotel Fiat
Information sent over this network may be visible to others
406
Home_net
Connected
408
410
Patrick_meeting
Security enabled network
412
Other connection options
414
Manage wireless networks
Connect
Cancel
416
418
420

Fig. 4

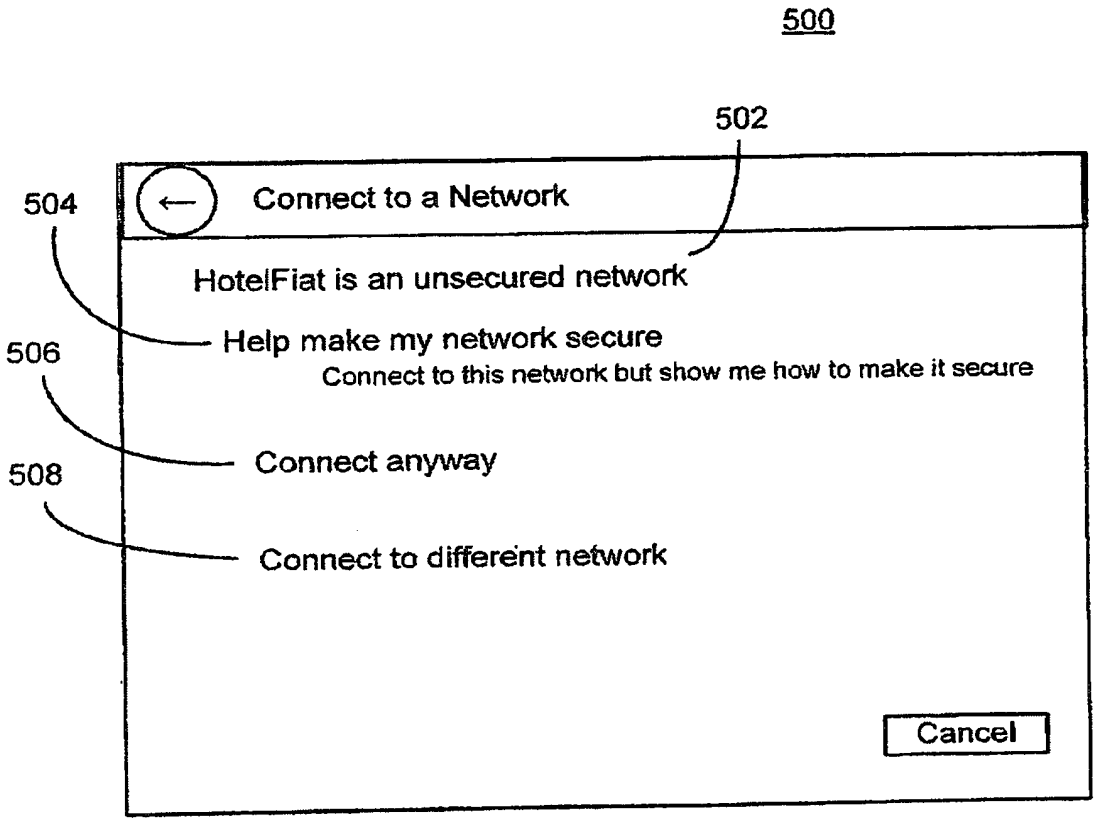

500
502
504
Connect to a Network
HotelFiat is an unsecured network
Help make my network secure
Connect to this network but show me how to make it secure
506
Connect anyway
508
Connect to different network
Cancel

Fig. 5

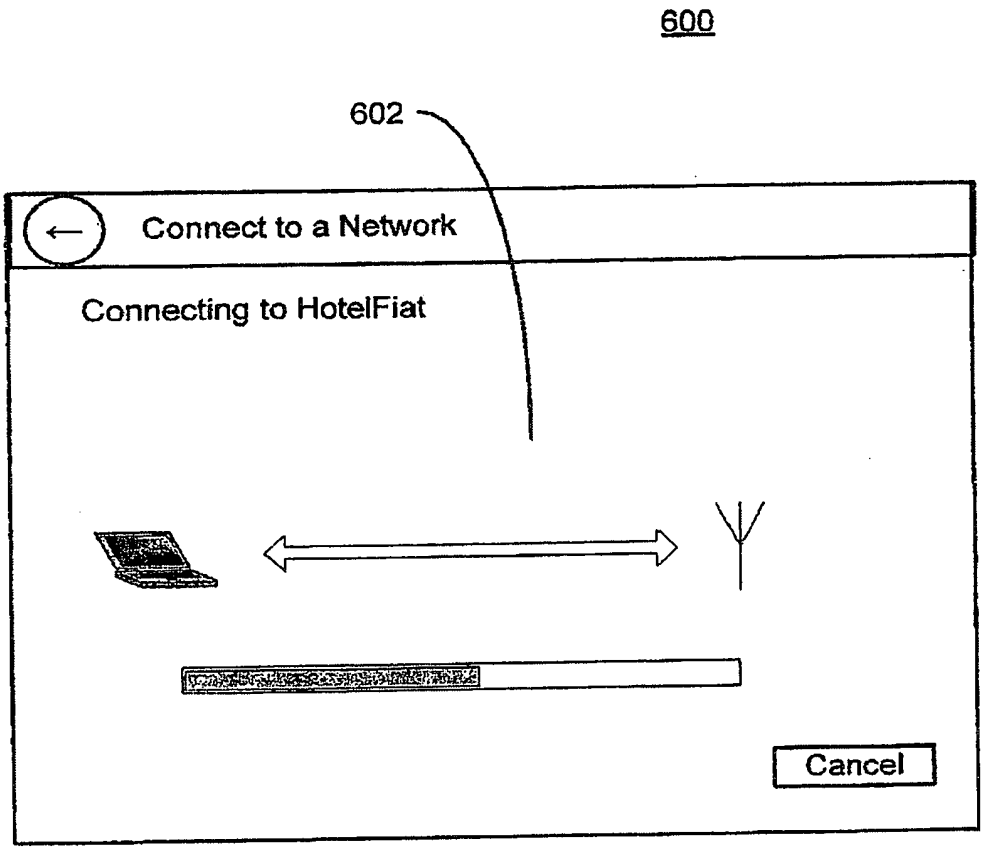

600
602
Connect to a Network
Connecting to HotelFiat
Cancel

Fig. 6

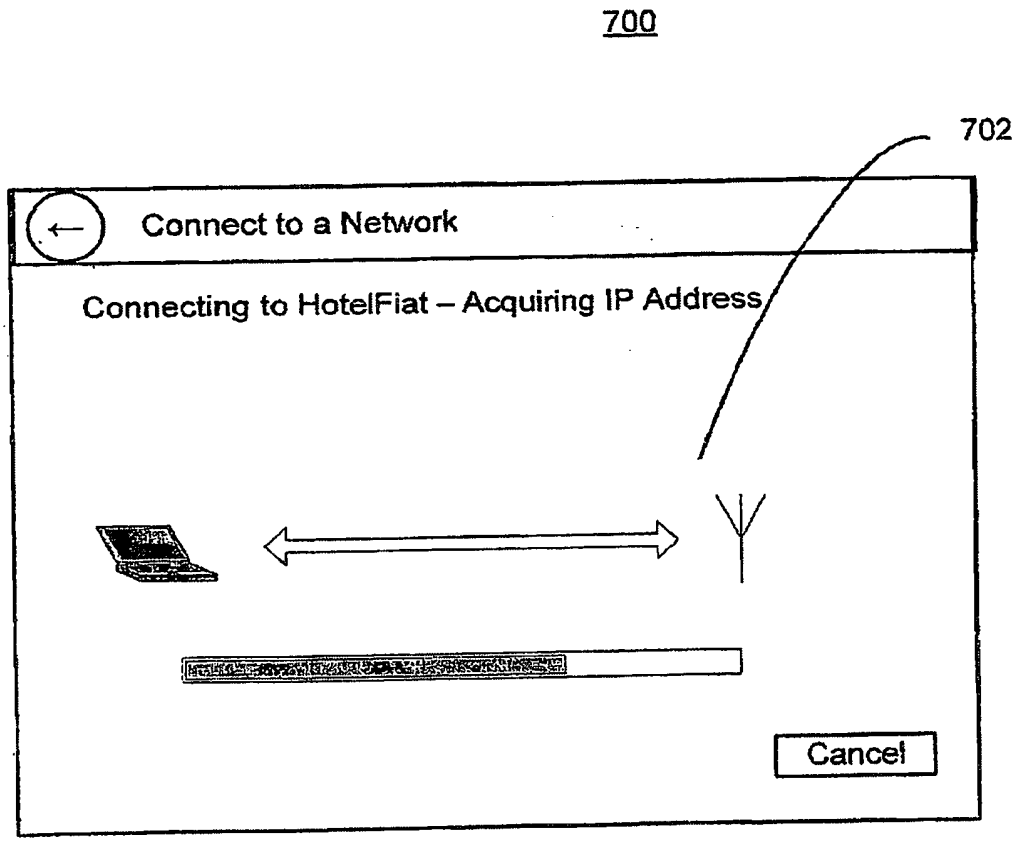

700
702
Connect to a Network
Connecting to HotelFiat – Acquiring IP Address
Cancel

Fig. 7

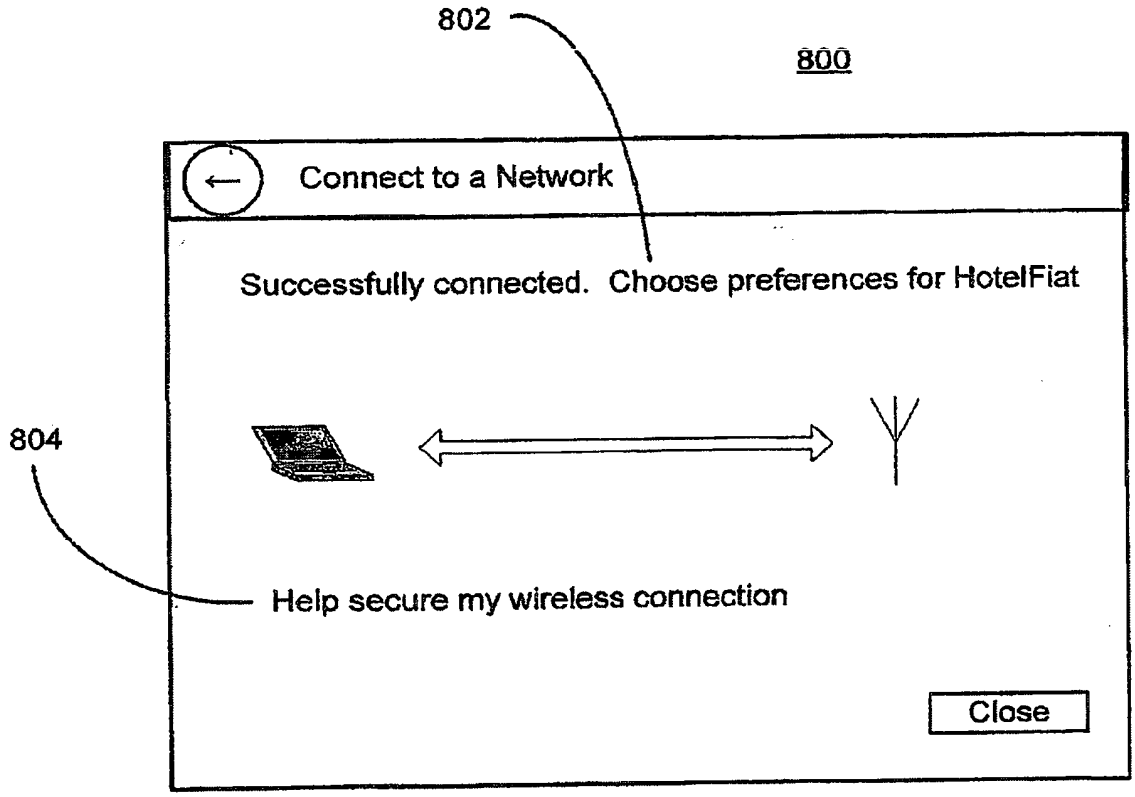

802
800
Connect to a Network
Successfully connected. Choose preferences for HotelFiat
804
Help secure my wireless connection
Close

Fig. 8

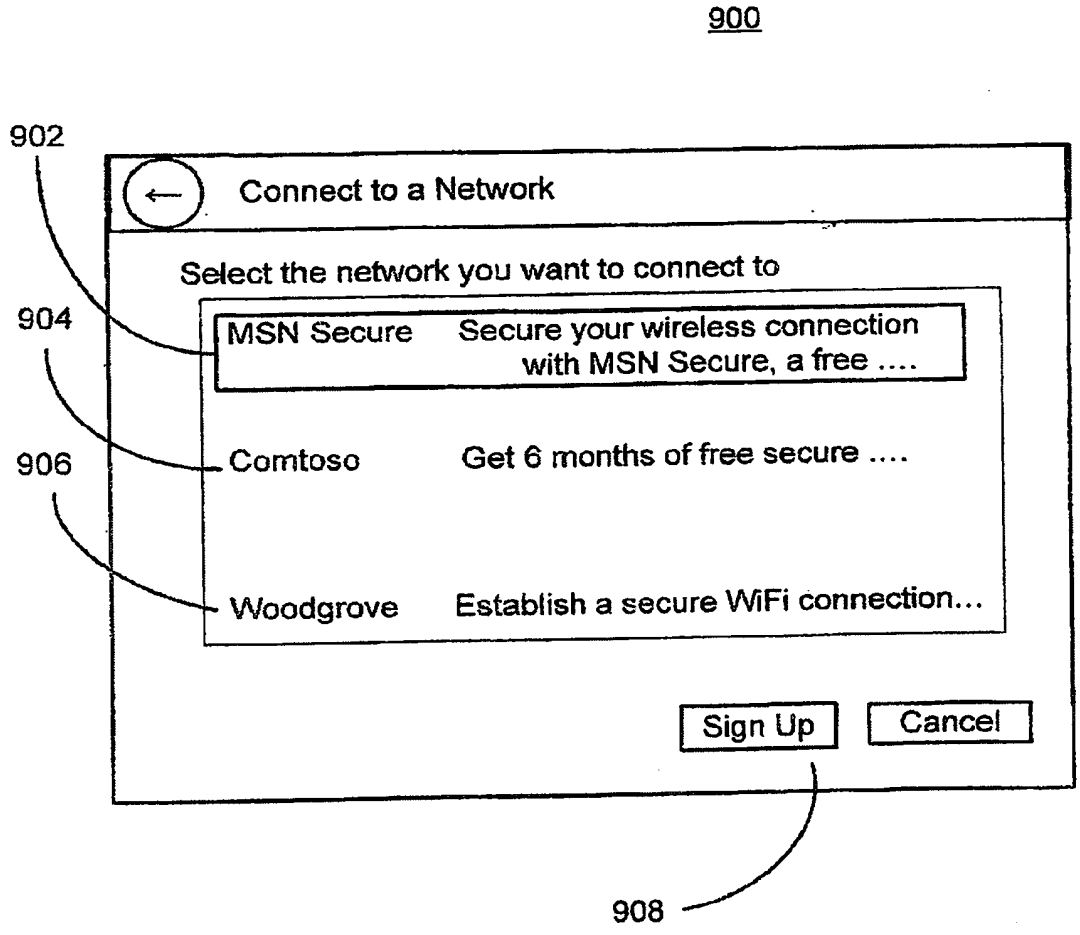

900
902
Connect to a Network
Select the network you want to connect to
904
MSN Secure
Secure your wireless connection with MSN Secure, a free ....
906
Comtoso
Get 6 months of free secure ....
Woodgrove
Establish a secure WiFi connection...
Sign Up
Cancel
908

Fig. 9

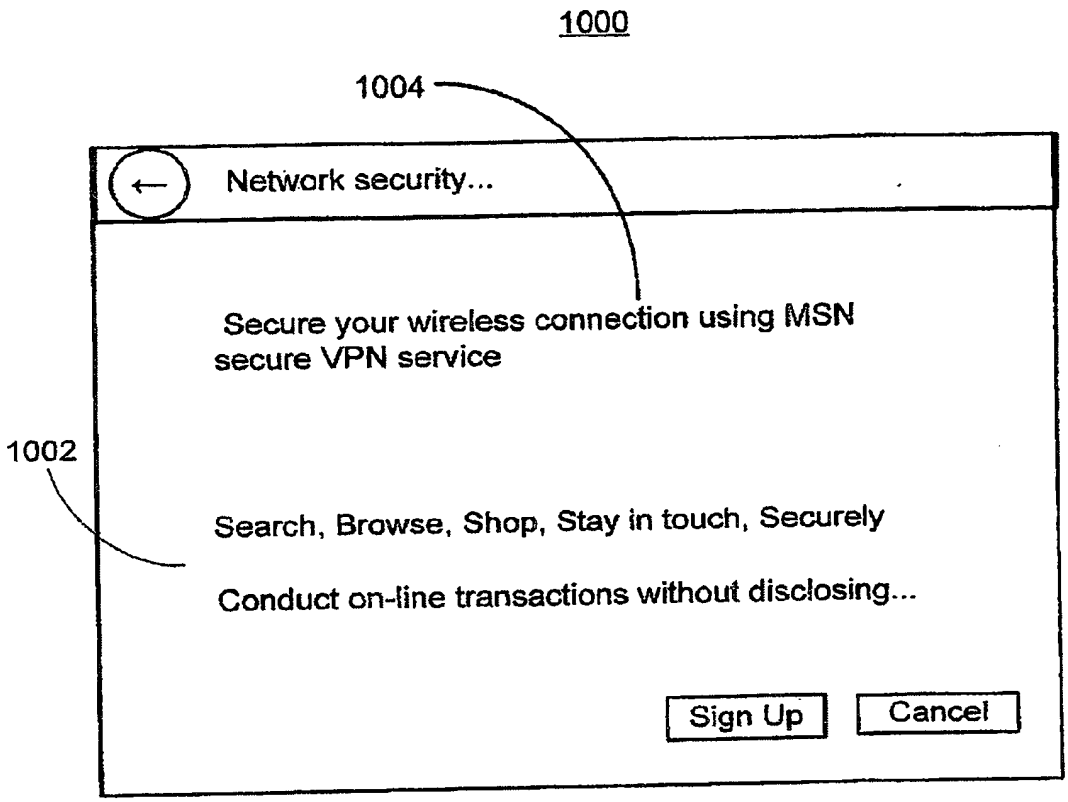

1000
1004
Network security...
Secure your wireless connection using MSN secure VPN service
1002
Search, Browse, Shop, Stay in touch, Securely
Conduct on-line transactions without disclosing...
Sign Up
Cancel

Fig. 10

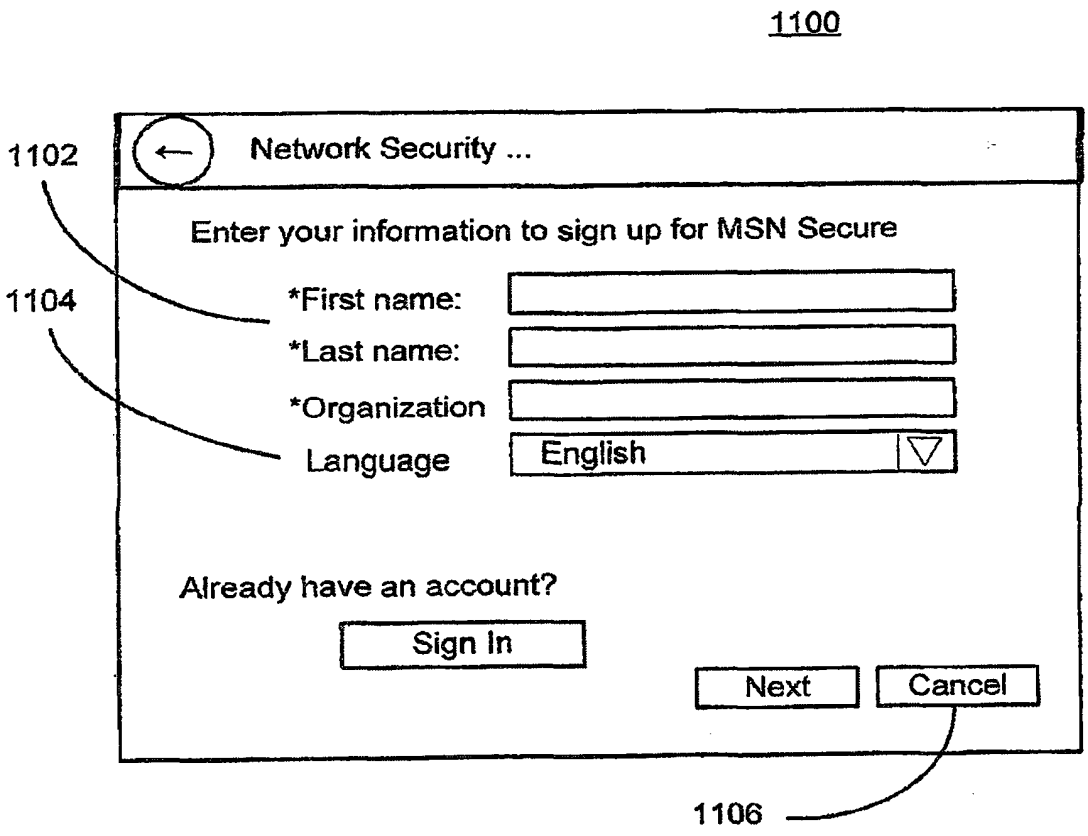

1100
1102
1104
Network Security ...
Enter your information to sign up for MSN Secure
*First name:
*Last name:
*Organization
Language
English
Already have an account?
Sign In
Next
Cancel
1106

Fig. 11

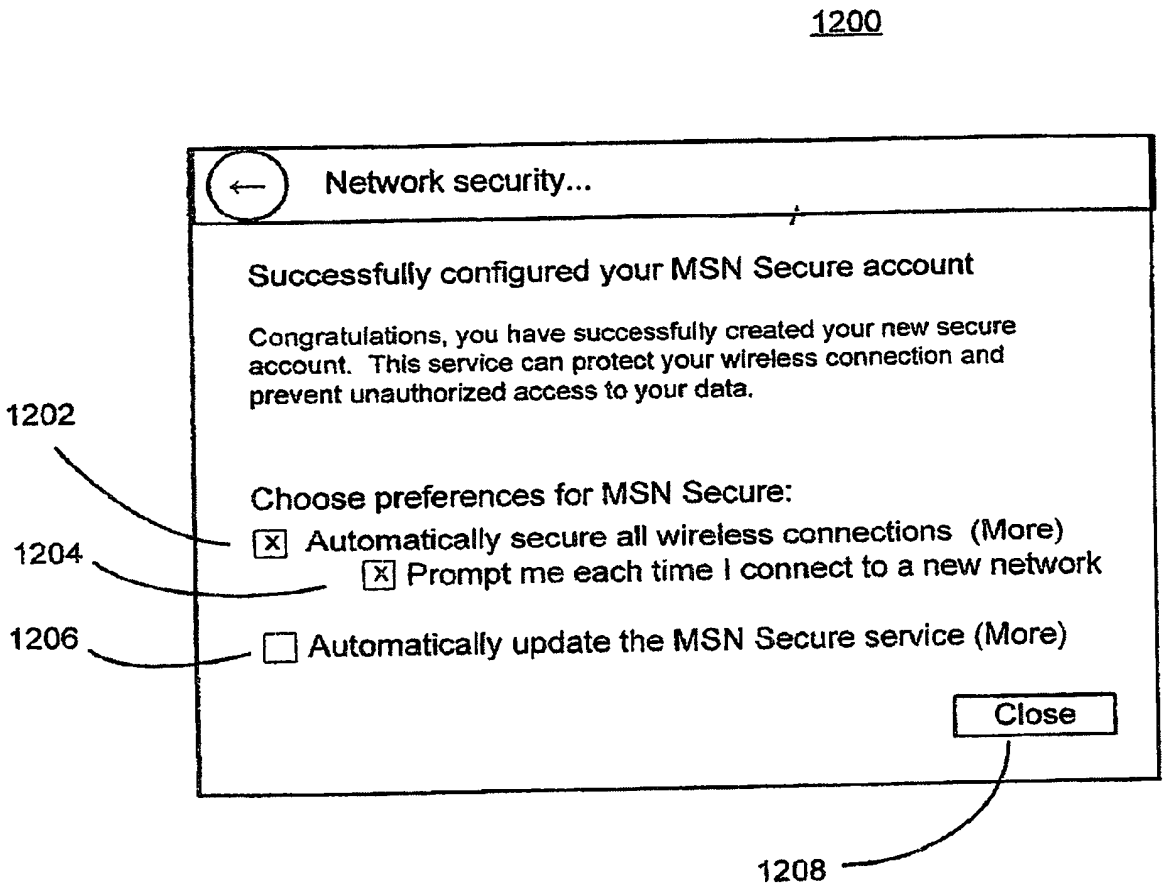

1200
Network security...
Successfully configured your MSN Secure account
Congratulations, you have successfully created your new secure account. This service can protect your wireless connection and prevent unauthorized access to your data.
1202
Choose preferences for MSN Secure:
Automatically secure all wireless connections (More)
1204
Prompt me each time I connect to a new network
1206
Automatically update the MSN Secure service (More)
Close
1208

Fig. 12

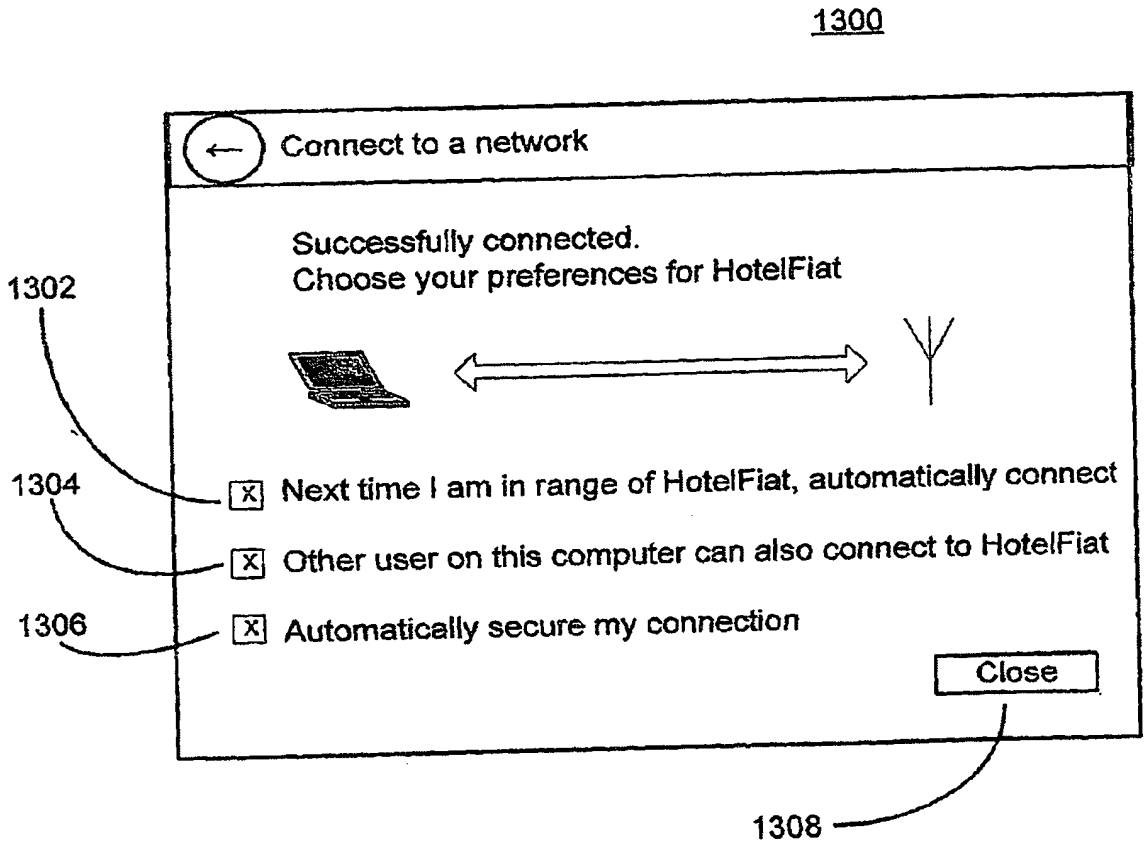

1300
Connect to a network
Successfully connected.
Choose your preferences for HotelFiat
1302
1304
1306
Next time I am in range of HotelFiat, automatically connect
Other user on this computer can also connect to HotelFiat
Automatically secure my connection
Close
1308

Fig. 13

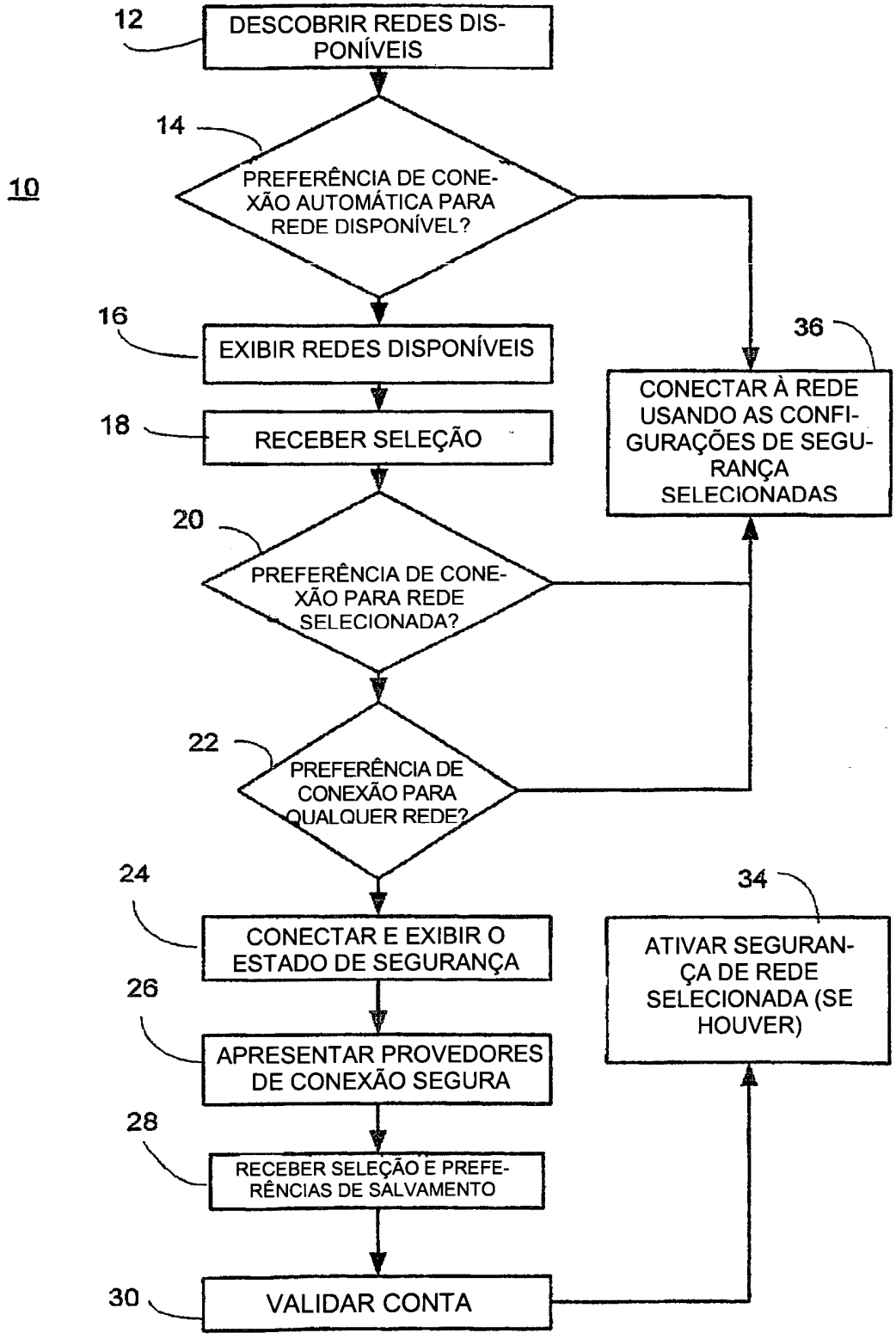

10
12
DESCOBRIR REDES DISPONÍVEIS
14
PREFERÊNCIA DE CONEXÃO AUTOMÁTICA PARA REDE DISPONÍVEL?
16
EXIBIR REDES DISPONÍVEIS
18
RECEBER SELEÇÃO
20
PREFERÊNCIA DE CONEXÃO PARA REDE SELECIONADA?
22
PREFERÊNCIA DE CONEXÃO PARA QUALQUER REDE?
24
CONECTAR E EXIBIR O ESTADO DE SEGURANÇA
26
APRESENTAR PROVEDORES DE CONEXÃO SEGURA
28
RECEBER SELEÇÃO E PREFERÊNCIAS DE SALVAMENTO
30
VALIDAR CONTA
34
ATIVAR SEGURANÇA DE REDE SELECIONADA (SE HOUVER)
36
CONECTAR À REDE USANDO AS CONFIGURAÇÕES DE SEGURANÇA SELECIONADAS

Fig. 14

PI0710927-0


RESUMO

"OFERTA E FORNECIMENTO DE SERVIÇOS DE REDE PRIVADA VIRTUAL SEM FIO PROTEGIDOS"

Um dispositivo eletrônico pode apresentar uma interface de usuário para fazer seleções relacionadas a conexão a uma rede ou seleção de uma rede a partir de uma pluralidade de redes disponíveis. Adicionalmente, uma interface de usuário pode dar ao usuário uma oportunidade de proteger a uma conexão aberta e não segura, por exemplo, uma conexão ad-hoc sem fio, tal como pode ser encontrado em uma cafeteria. Uma seleção de ofertas de segurança pode ser feita a partir de uma tela de interface de usuário que inclui provedores de serviço pré-povoados. Pode ser permitido ao usuário salvar as preferências para se conectar a novas redes, bem como as preferências relacionadas às redes previamente usadas. Ademais, o usuário pode salvar as preferências para convocar serviços de segurança em uma base por rede ou de panorama de rede. O serviço de segurança pode ser um protocolo de tunelamento conhecido (isto é VPN), tal como o L2TP ou PPTP.