



Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0903066-2

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0903066-2

(22) Data do Depósito: 11/02/2009

(43) Data da Publicação Nacional: 13/07/2010

(51) Classificação Internacional: H04L 29/08; H04L 29/06; H04L 29/14.

(52) Classificação CPC: H04L 67/16; H04L 67/1002; H04L 67/1008; H04L 65/1046; H04L 65/105; H04L 69/40.

(30) Prioridade Unionista: US 12/056.246 de 26/03/2008.

(54) Título: DISPOSITIVO DE COMUNICAÇÃO ATIVADO PELO PROTOCOLO DE INICIAÇÃO DE SESSÃO (SIP), MÉTODO PARA SUA OPERAÇÃO E MEIO LIDO POR COMPUTADOR PARA EXECUTAR AS ETAPAS DO MÉTODO

(73) Titular: AVAYA, INC., Sociedade Norte-Americana. Endereço: 211 Mount Airy Road Basking Ridge NJ 07920, ESTADOS UNIDOS DA AMÉRICA(US)

(72) Inventor: AL BAKER; MEHMET C. BALASAYGUN; FRANK J. BOYLE; GORDON BRUNSON; BENJAMIN JENKINS; PAMELA J. LAUBER; THOMAS A. PETSCHÉ.

Prazo de Validade: 10 (dez) anos contados a partir de 06/10/2020, observadas as condições legais

Expedida em: 06/10/2020

Assinado digitalmente por:

Adriana Briggs de Aguiar

Diretora Substituta de Patentes, Programas de Computador e Topografias de Circuitos Integrados

DISPOSITIVO DE COMUNICAÇÃO ATIVADO PELO PROTOCOLO DE
INICIAÇÃO DE SESSÃO (SIP), MÉTODO PARA SUA OPERAÇÃO E MEIO
LIDO POR COMPUTADOR PARA EXECUTAR AS ETAPAS DO MÉTODO
CAMPO DA INVENÇÃO

5 A invenção relaciona-se genericamente a redes de
comunicação e, mais especificamente, a redes de
sobrevivência do Protocolo de Iniciação de Sessão (SIP).

HISTÓRICO DA INVENÇÃO

O Protocolo de Iniciação de Sessão (SIP) é um
10 protocolo de sinalização aberta para estabelecer muitos
tipos de sessões de comunicação em tempo real. Exemplos dos
tipos de sessões de comunicação que poderão ser
estabelecidas utilizando o Protocolo de Iniciação de Sessão
(SIP) incluem voz, vídeo, jogos, aplicações, e/ou mensagens
15 instantâneas. Essas sessões de comunicação poderão ser
realizadas em qualquer tipo de dispositivo de comunicação
como o computador pessoal, o computador laptop, o
assistente digital pessoal (PDA), o telefone celular, o
cliente IM, o telefone IP, o telefone tradicional,
20 aplicações de servidor, agregados de aplicações, aplicações
de mesa, e assim por diante.

Um recurso chave do Protocolo de Iniciação de Sessão
(SIP) é sua capacidade de utilizar um Endereço de Registro
(AOR) como um único endereço público unificador para todas
25 as comunicações para usuários finais, aplicações, e redes
de provedor de serviço. Assim, em um mundo de comunicação
aprimorada pelo Protocolo de Iniciação de Sessão (SIP), o
Endereço de Registro (AOR) do usuário torna-se seu único
endereço que liga o usuário a todos os dispositivos de
30 comunicação associados ao usuário. Utilizando este Endereço

de Registro (AOR), aquele que chama pode atingir qualquer um dos dispositivos de comunicação do usuário, também referido como Agentes de Usuário (UAs) sem precisar saber cada um dos endereços de dispositivo singulares ou números
5 de telefone.

Muitos servidores de aplicação do Protocolo de Iniciação de Sessão (SIP) existem para as finalidades de permitir aplicações de comunicação em um ambiente de Protocolo de Iniciação de Sessão (SIP) e para servir como
10 substitutos exportados para um Agente de Usuário (UA), assim permitindo que redes complexas sejam construídas enquanto oculta aquela complexidade através de substitutos que os dispositivos utilizam para conectar dentro da rede. Uma das principais áreas para essas aplicações de
15 comunicação é o controle de chamada de um Agente de Usuário (UA) pelo Protocolo de Iniciação de Sessão (SIP). Há atualmente muito poucas soluções para o problema de fornecer uma configuração de rede de sobrevivência do Protocolo de Iniciação de Sessão (SIP). Uma maneira pela
20 qual a sobrevivência foi fornecida no passado foi através da utilização de substitutos do Protocolo de Iniciação de Sessão (SIP) que são empregados quando não há resposta à sinalização do Protocolo de Iniciação de Sessão (SIP). O substituto pode ser utilizado para rotear a sinalização
25 através de uma ou mais rotas alternativas na rede. A utilização de um substituto separado pode ficar cara, pois um elemento de rede adicional que não a controladora de chamada ou um portal é necessário para fornecer a sobrevivência.

30 Outros produtos de servidor de rede fornecem

configurações geo-redundantes, tal que o portal provavelmente não se defrontará com uma falha no servidor da rede devido a alta disponibilidade do servidor de rede. Como a utilização de substitutos, esta solução particular é

5 relativamente cara, pois servidores de alta disponibilidade precisam ser comprados e distribuídos por toda a rede. Deficiências adicionais das soluções atuais conhecidas incluem o fato de que o elemento de rede (por exemplo, portal) não tem permissão para utilizar uma via alternativa

10 se a via de sinalização do Protocolo de Iniciação de Sessão (SIP) principal estiver indisponível; essas soluções exigem configurações de reserva quente com replicação dos dados através de servidores; e eles exigem controladoras de chamada principal e secundária para utilizar exatamente a

15 mesma versão do Protocolo de Iniciação de Sessão (SIP) e fornecer exatamente o mesmo conjunto de recursos do Protocolo de Iniciação de Sessão (SIP) aos pontos terminais do Protocolo de Iniciação de Sessão (SIP).

SINOPSE

20 Além dessas deficiências, a lógica para determinar quando uma falha de rede ocorreu tem sido tradicionalmente colocada nos roteadores, que têm a capacidade de verificar a camada IP da rede para determinar se vários elementos de rede estão operando adequadamente. Esta lógica de detecção

25 de falhas/restrições foi colocada no roteador para aliviar o ônus de processamento no resto dos componentes da rede. Uma restrição importante a esta configuração particular é que os roteadores são incapazes de detectar ao nível da aplicação do Protocolo de Iniciação de Sessão (SIP) se um

30 servidor ou outro elemento de rede está operacional. Poderá

haver muitos casos em que o servidor está operacional ao nível da camada IP, mas a controladora do Protocolo de Iniciação de Sessão (SIP) não está operacional. Roteadores e outros elementos de rede da tecnologia anterior têm sido incapazes até agora de identificar essas condições de falha e registrariam esse servidor como operacional.

Essas e outras necessidades são defrontadas por várias versões e configurações da presente invenção. A presente invenção é dirigida genericamente a um sistema, dispositivo, e método para analisar a disponibilidade de parte ou da totalidade de uma rede ou sistema de comunicação. Em uma versão, o método compreende:

receber, em um ponto terminal de comunicação ativado pelo Protocolo de Iniciação de Sessão (SIP), informação da controladora relacionada a uma primeira controladora;

receber, na ponta terminal de comunicação, informação de controladora relacionada a uma segunda controladora;

analisar a informação de controladora relacionada tanto à primeira como à segunda controladoras; e

com base na etapa de análise, a ponta terminal de comunicação selecionar pelo menos uma da primeira e da segunda controladoras como a sua controladora.

As controladoras poderão fornecer ao ponto terminal funções relacionadas ao Protocolo de Iniciação de Sessão (SIP) bem como facilitar as chamadas do Protocolo de Iniciação de Sessão (SIP) de entrada/saída para o ponto terminal. De acordo com pelo menos algumas versões da presente invenção, as controladoras poderão compreender diferentes atributos e recursos e, portanto, poderão ser capazes de fornecer ao ponto terminal recursos do Protocolo

de Iniciação de Sessão (SIP) diferentes. Para dotar o ponto terminal da capacidade de sobreviver a uma falha no sistema de comunicação (por exemplo, uma falha em sua controladora primária ou algum componente que conecta a controladora primária com o ponto terminal) o ponto terminal poderá ser adaptado para manter simultaneamente seu registro tanto com a primeira como com a segunda controladoras. Em pelo menos algumas versões, o ponto terminal poderá ser adaptado para registrar simultaneamente com mais de duas controladoras ao mesmo tempo.

De acordo com pelo menos algumas versões da presente invenção, o ponto terminal poderá selecionar tanto a primeira como a segunda controladora como sua controladora primária. Nesta configuração de sobrevivência ativa-ativa, o ponto terminal poderá permitir a comunicação com ambas as controladoras. De acordo com outras versões da presente invenção, o ponto terminal poderá selecionar a primeira controladora como sua controladora primária e a segunda controladora como sua controladora secundária. Nesta configuração ativa-reserva o ponto terminal poderá discriminar contra mensagens recebidas de uma ou da outra controladora dependendo de se o ponto terminal está operando em modo primário ou de falha da operação/configuração.

O ponto terminal poderá selecionar suas controladoras com base nos atributos relativos das controladoras. De acordo com pelo menos algumas versões da presente invenção, o ponto terminal poderá ser adaptado para solicitar e descobrir informação de atributo de controladora, depois gerar uma lista ordenada das controladoras com base em sua

informação de atributo relativo. Com a lista ordenada de controladoras os pontos terminais poderão ser adaptados para arbitrar entre qual das controladoras ele deve se registrar. Ao dotar o ponto terminal da lógica para
5 selecionar as controladoras com as quais ela irá se registrar e fornecer um servidor que tem capacidade de escolher as controladoras também para o ponto terminal (por exemplo, através da sobreposição das prioridades e assemelhados), a combinação ponto terminal e servidor será
10 mais bem equipada para lidar com condições de falha, pois nenhum deles está confiando em qualquer um componente individual da rede para informá-lo quais controladoras devem ser utilizadas. Ademais, o ponto terminal terá permissão para atualizar dinamicamente a lista ordenada de
15 controladoras ao solicitar periodicamente informação de controladora e obter a informação de estado atualizada para os componentes que compreendem as controladoras. Como será aqui descrito a mais, o ponto terminal e suas controladoras poderão operar em uma configuração primária que corresponde
20 à configuração arquitetural principal antes da falha. O modo de falha de operação ou configuração poderá corresponder à configuração arquitetural de backup dos componentes que é utilizada no caso de uma condição de falha. Esta configuração de falha fornece ao ponto terminal
25 a capacidade de sobreviver a condições de falha. A configuração de falha pode ser simétrica ou assimétrica entre a configuração primária e a configuração de backup tal que o ponto terminal pode ser conhecedor da simetria, se aplicável. O termo "aplicação do Protocolo de Iniciação
30 de Sessão (SIP)" deve ser compreendido como incluindo

qualquer aplicação ou operação que seja compatível para utilização de acordo com o Protocolo de Iniciação de Sessão (SIP) e pode ser facilitada através da transmissão de mensagens do Protocolo de Iniciação de Sessão (SIP).

5 "Recursos do Protocolo de Iniciação de Sessão (SIP) básicos" conforme aqui utilizado, inclui qualquer Solicitação de Comentários (RFC -Request For Comments) da norma Força Tarefa de Engenharia da Internet (IETF - Internet Engineering Task Force) para a sinalização do
10 Protocolo de Iniciação de Sessão (SIP) que não inclui extensões prolongadas ao sinalização ou dados contidos dentro daquela sinalização. Isto inclui normas relacionadas adicionais que poderão ser utilizadas em conjunto com o Protocolo de Iniciação de Sessão (SIP), como a norma de
15 presença para descrever o conteúdo XML utilizado em mensagens de notificação "SIP NOTIFY" que indicam presença.

"Monitorar", conforme aqui utilizado, inclui qualquer tipo de função relacionada a observar, registrar, ou detectar com instrumentos que não têm qualquer efeito sobre
20 a operação ou a condição do elemento ou grupo de elementos que estão sendo monitorados.

Como é aqui utilizado, "pelo menos um", "um ou mais", e "e/ou" são expressões de extremidade aberta que são tanto conjuntivas como disjuntivas em operação. Por exemplo, cada
25 uma das expressões "pelo menos um de A, B, e C", "pelo menos um de A, B, ou C", "um ou mais de A, B, e C", "um ou mais de A, B, ou C" e "A, B, e/ou C" significa A sozinho, B sozinho, C sozinho, A e B juntos, A e C juntos, B e C juntos, ou A, B e C juntos.

30 Os termos "a" ou "o" entidade referem-se a um ou mais

daquela entidade. Como tal, os termos "a" (ou "o"), "um ou mais" e "pelo menos um" podem ser aqui utilizados de modo intercambiável. Deve-se observar que os termos "compreender", "incluir" e "ter" podem ser utilizados de modo intercambiável.

O termo "automático" e variações do mesmo, conforme aqui utilizado, refere-se a qualquer processo ou operação feita sem entrada humana material quando o processo ou a operação for efetuada. No entanto, o processo ou operação pode ser automático mesmo se o desempenho do processo ou da operação utiliza entrada humana, quer material ou imaterial, recebida antes do desempenho do processo ou da operação. A entrada humana é considerada como sendo material se essa entrada influenciar como o processo o a operação será realizada. A entrada humana que consente com o desempenho do processo ou da operação não é considerado como sendo "material".

O termo "meio lido por computador" conforme aqui utilizado refere-se a qualquer meio de armazenamento e/ou de transmissão tangível que participa no fornecimento de instruções para o processador para execução. O meio lido por computador pode ser um conjunto serializado de instruções codificadas em uma transmissão de rede por uma rede IP (por exemplo, SOAP). Esse meio poderá assumir muitas formas, incluindo, sem a elas se limitar, mídia não volátil, mídia volátil, e mídia de transmissão. Mídia não volátil inclui, por exemplo, VNRAM, ou discos magnéticos ou ópticos. Mídia volátil inclui memória dinâmica (por exemplo, RAM), como a memória principal. Formas comuns de mídia lida por computador incluem, por exemplo, um disco

flexível, um disco rígido, fita magnética, o qualquer outro meio magnético, meio magneto-óptico, um CD-ROM, qualquer outro meio óptico, cartões perfurados, fita de papel, qualquer outro meio físico com padrões de orifícios, RAM, 5 PROM, EPROM, FLASH-EPROM, meio de estado sólido como um cartão de memória, qualquer outro chip ou cartucho de memória, uma onda portadora conforma descrita doravante, ou qualquer outro meio do qual o computador possa ler. Um arquivo digital anexado a uma correspondência eletrônica ou 10 outro arquivo de informação auto-contido ou conjunto de arquivos é considerado um meio de distribuição equivalente a um meio de armazenamento tangível. Quando o meio lido por computador for configurado como uma base de dados, deve ser compreendido que a base de dados poderá ser qualquer tipo 15 de base de dados, como relacional, hierárquica, orientada a objeto, e/ou assemelhados. Assim, a invenção é considerada como incluindo um meio de armazenamento tangível ou meio de distribuição e equivalentes reconhecidos pela tecnologia anterior e meios sucessores, em que as implementações de 20 software da presente invenção são armazenadas.

Os termos "determinar", "calcular" e "computar", e variações destes, conforme aqui utilizados, são utilizados de modo intercambiável e incluem qualquer tipo de metodologia, processo, operação matemática ou técnica. Mais 25 especificamente, esses termos poderão incluir regras interpretadas como BPEL ou linguagem de regras em que a lógica não é codificada dura, mas representada em um arquivo de regras que pode ser lido, interpretado, computado, e executado.

30 O termo "módulo" ou "ferramenta" conforme aqui

utilizado refere-se a qualquer hardware, software, firmware, inteligência artificial, lógica difusão, ou combinação de hardware e software conhecidos ou desenvolvidos posteriormente que seja capaz de efetuar a funcionalidade associada àquele elemento. Outrossim, embora a invenção seja descrita em termos de versões exemplares, deve ser apreciado que aspectos individuais da invenção podem ser reivindicados em separado.

O que precede é um resumo simplificado da invenção para fornecer uma compreensão de alguns aspectos da invenção. Este resumo não é nem extenso nem abrangente como uma visão geral da invenção e suas várias versões. Pretende-se nem identificar elementos chaves ou críticos da invenção nem delinear o escopo da invenção, mas sim apresentar conceitos seletos da invenção de forma simplificada como uma introdução à descrição mais detalhada apresentada abaixo. Como será apreciado, outras versões da invenção são possíveis utilizando, sozinho ou em combinação, um ou mais dos recursos explicitados acima ou descritos em detalhe abaixo.

DESCRIÇÃO SUCINTA DOS DESENHOS

A Figura 1 é um diagrama de blocos que representa um sistema de comunicação de acordo com pelo menos algumas versões da presente invenção.

A Figura 2 é um diagrama de blocos que representa um método de descoberta e registro de uma controladora do Protocolo de Iniciação de Sessão (SIP) de acordo com pelo menos algumas versões da presente invenção.

A Figura 3 é um diagrama de fluxo que representa um método de determinação de estado de acordo com pelo menos

algumas versões da presente invenção.

A Figura 4 é um diagrama de fluxo que representa um método de determinação de estado reativo de acordo com pelo menos algumas versões da presente invenção.

5 A Figura 5 é um diagrama de fluxo que representa um método de operação de portal de acordo com pelo menos algumas versões da presente invenção.

A Figura 6 é um diagrama de fluxo que representa um método de determinação de estado para um ponto terminal de
10 acordo com pelo menos algumas versões da presente invenção.

A Figura 7 é um diagrama de fluxo que representa um método de notificação de estado de acordo com pelo menos algumas versões da presente invenção.

DESCRIÇÃO DETALHADA

15 A invenção será ilustrada abaixo em conjunto com um sistema de comunicação exemplar. Embora seja bem adequada para utilização, por exemplo, com um sistema que utilize servidores e/ou bases de dados, a invenção não é limitada ao uso com qualquer tipo particular de sistema de
20 comunicação ou configuração dos elementos do sistema. Ademais, o termo "base de dados" conforme aqui utilizado poderá incluir não apenas sistemas de base de dados relacionais, mas qualquer mecanismo de armazenamento por computador, disponível tanto em hardware como em software,
25 em RAM ou em um disco rígido. Aqueles habilitados na tecnologia reconhecerão que as técnicas reveladas poderão ser utilizadas em qualquer aplicação de comunicação em que seja desejável manter uma rede de sobrevivência do Protocolo de Iniciação de Sessão (SIP).

30 Os sistemas e métodos exemplares desta invenção também

serão descritos em relação a software de análise, módulos e hardware de análise associado. No entanto, para evitar obscurecer desnecessariamente a presente invenção, a descrição seguinte omite estruturas, componentes e dispositivos bem conhecidos que poderão ser mostrados na forma de diagrama de blocos e são bem conhecidos ou de outra forma reduzidos. Exemplos de estruturas assim bem conhecidas incluem, sem limitação, infra-estrutura IP, comutadores de Camada 2, roteadores de OP de camada, paredes de fogo ao nível IP, dispositivos de Tradução de Endereço de Rede (NAT - Network Address Translation), Controladoras de Borda de Sessão (SBCs - Session Border Controllers) do SIP, etc.

Para fins de explicação, numerosos detalhes são explicitados para fornecer uma compreensão completa da presente invenção. No entanto, deve ser apreciado que a presente invenção poderá ser praticada de uma variedade de formas além dos detalhes específicos aqui apresentados.

Com referência inicialmente à Figura 1, uma arquitetura de sistema de comunicação exemplar 100 será descrita de acordo com pelo menos algumas versões da presente invenção. O sistema de comunicação 100 compreende uma primeira rede 104 que conecta um ponto terminal como o Agente do Usuário (UA) do Protocolo de Iniciação de Sessão (SIP) para um número de outros dispositivos de comunicação. O Agente do Usuário (UA) 108 poderá ser adaptado para comunicar com pontos terminais também conectados à primeira rede 104 bem como outros pontos terminais externos à primeira rede 104. Por exemplo, o Agente do Usuário (UA) 108 poderá ser adaptado para comunicar com um ponto

terminal externo 156 conectado a uma segunda rede 152.

A primeira 104 e a segunda 152 redes poderão corresponder a qualquer tipo de rede de comunicação conhecida ou coleção de equipamento de comunicação. A
5 primeira rede 104 poderá compreender uma Rede de Área Local (LAN), uma Rede de Área Ampla (WAN), ou qualquer outro tipo de rede de camada 3 e de camada 4 conforme definido pelo modelo OSI.

A segunda rede 152 poderá compreender qualquer tipo de
10 meio de transporte de informação e poderá utilizar qualquer tipo de protocolo para transportar mensagens entre pontos terminais. A Internet é um exemplo da rede de comunicação
104 que constitui uma rede IP que consiste de muitos computadores e outros dispositivos de comunicação
15 localizados por todo o mundo, que são conectados através de muitos sistemas de telefonia e de outros meios. Outros exemplos da segunda rede 152 incluem, sem limitação, um Sistema de Telefonia Antiga Simples (POTS), uma Rede Digital de Serviços Integrados (ISDN), a Rede de Telefonia
20 Comutada Pública (PSTN), uma LAN, uma WAN, rede de comunicação celular, e qualquer outro tipo de rede comutada por pacote ou comutada por circuito conhecida na tecnologia. Ambas as redes de comunicação 104, 152 poderão incluir tecnologias de comunicação fiada e/ou sem fio.

25 As funções do Protocolo de Iniciação de Sessão (SIP) do Agente do Usuário (UA) 108 poderão ser fornecidas por um ou mais servidores 136, que também estão conectados à primeira rede 104. O Agente do Usuário (UA) 108 também poderá ser controlado por outros servidores ou dispositivos
30 de comunicação externos à primeira rede 104. Por exemplo,

um portal 148 que conecta a primeira rede 104 com a segunda rede 152 também poderá ser adaptado para fornecer capacidades de controle do Protocolo de Iniciação de Sessão (SIP) para o Agente do Usuário (UA) 108.

5 Além de fornecer funções do Protocolo de Iniciação de Sessão (SIP), o servidor 136 também poderá incluir software de chamada de voz (por exemplo, software VoIP), software de chamada de vídeo, software IM, software de mensagens de voz (por exemplo, mensagens multimídia como mensagens de áudio
10 e de vídeo, mensagens IM, etc.), software de gravação, um servidor de voz IP, um servidor de fax, um servidor da Web, um servidor de correspondência eletrônica, aplicações de centro de chamada, e assemelhados.

De acordo com versões da presente invenção, o servidor
15 136 pode incluir interfaces para vários outros protocolos como o Protocolo de Acesso de Diretório Leve (LDAP - Lightweight Directory Access Protocol), H.248, Protocolo de Transferência de Correspondência Simples (SMTP - Simple Mail Transfer Protocol), Protocolo de Acesso à Mensagem da
20 Internet 4 (IMAP4 - Internet Message Access Protocol 4), Rede Digital de Serviços Integrados (ISDN - Integrated Services Digital Network), E1/T1, HTTP, SOAP, XCAP, STUN, e linha ou tronco analógico.

O servidor 136 também poderá incluir um PBX, um
25 Distribuição de Chamada Automático (ACD -Automatic Call Distribution), um comutador de empreendimento, ou outro tipo de comutador de sistema de comunicação (por exemplo, qualquer dispositivo capaz de rotear chamadas de um telefone para outro, como uma máquina complexa (ou uma
30 série delas) em uma estação central que funciona ao

conectar juntos dois ou mais circuitos, cada circuito sendo conectado a um telefone de assinante, de acordo com um número de telefone discado) ou servidor, bem como outros tipos de dispositivos de controle da comunicação com base no processador como servidores de mídia, computadores, adjuntos, etc.

O portal 148 é fornecido para agir como uma unidade de tradução entre redes de telecomunicação díspares como a PSTN; Redes da Próxima Geração (Next Generation Networks); redes de acesso de rádio 2G, 2,5G e 3G; ou PBX. Uma das funções do portal 148 é converter entre as diferentes técnicas de codificação e de transmissão para as várias redes. Funções de streaming da mídia, como cancelamento de eco, DTMF, e remetente de tom também poderão ser suportados pelo portal 148. O portal 148 ainda poderá converter sinais/mensagens de um paradigma operacional de rede (por exemplo, protocolo de transmissão) para outro.

Para fornecer funcionalidades do Protocolo de Iniciação de Sessão (SIP) para o Agente do Usuário (UA) 108, os servidores 136 e/ou o portal 148 poderão compreender uma ou mais controladoras 140a-N de cada vez. Conforme é aqui utilizado, o termo "registro" e "registrar" referem-se ao registro do Protocolo de Iniciação de Sessão (SIP) e método e processo de fixação da rede, que inclui, sem a eles se limitar, o envio e a confirmação da mensagem "SIP REGISTER", e poderá incluir outros mecanismos como a mensagem "SUBSCRIBE" para assinaturas, consultas utilizando a mensagem "OPTIONS", bem como outros mecanismos não-SIP, como a parede de fogo e detecções NAT utilizando o protocolo STUN, consultas HTTP, etc.

As controladoras 140a-N poderão corresponder a aplicações ou firmware residente no servidor 136 e as controladoras 140a-N poderão ser utilizadas para lidar com mensagens do Protocolo de Iniciação de Sessão (SIP) 5 dirigidas e recebidas do Agente do Usuário (UA) 108 controlado. As mensagens do Protocolo de Iniciação de Sessão (SIP) lidas pelas controladoras 140a-N poderão corresponder a mensagens do Protocolo de Iniciação de Sessão (SIP) de saída originadas pelo Agente do Usuário 10 (UA) 108 e dirigida no sentido de outro ponto terminal 156 ou mensagens do Protocolo de Iniciação de Sessão (SIP) de entrada originadas por outro ponto terminal 156 e dirigida no sentido do Agente do Usuário (UA) 108. As controladoras 140a-N poderão operar na camada de aplicação do sistema de 15 comunicação 100.

De acordo com pelo menos uma versão da presente invenção, o Agente do Usuário (UA) 108 poderá ser capaz de registrar simultaneamente com duas ou mais controladoras 140. Cada uma das controladoras 140 com as quais o Agente 20 do Usuário (UA) 108 está registrado simultaneamente poderá compreender atributos diferentes e, portanto, poderá ser capaz de dotar o Agente do Usuário (UA) 108 com funções do Protocolo de Iniciação de Sessão (SIP) diferentes. Por exemplo, o Agente do Usuário (UA) 108 poderá ser registrado 25 simultaneamente com uma primeira controladora 140a que utiliza extensões estendidas (isto é, conjuntos de recursos avançados) e uma segunda controladora 140b que utiliza extensões do Protocolo de Iniciação de Sessão (SIP) enquadrada na norma IETF para o processamento de chamadas 30 de acordo com um ou mais RFCs IETF no Protocolo de

Iniciação de Sessão (SIP), incluindo, mas sem limitação, ao RFC 3261.

Em uma configuração de registro simultânea, o Agente do Usuário (UA) 108 poderá ser capaz quer de um registro ativo-ativo ou um registro ativo-reserva. Em um registro ativo-ativo, o Agente do Usuário (UA) 108 poderá aceitar mensagens do Protocolo de Iniciação de Sessão (SIP) quer da controladora 140 e enviar mensagens do Protocolo de Iniciação de Sessão (SIP) para uma das controladoras 140 sem determinar se a mensagem está sendo enviada ou vindo de uma controladora primária 140. Em uma configuração de registro ativo-reserva, entretanto, o Agente do Usuário (UA) 108 apenas poderá utilizar a controladora ativa 130 para fins de sinalização do Protocolo de Iniciação de Sessão (SIP) a menos que a controladora ativa 140 fique inoperante. Em tal configuração, se mensagens são recebidas da controladora reserva 140 e o Agente do Usuário (UA) 108 acredita que a controladora primária 140 está operacional, então o Agente do Usuário (UA) 108 poderá enviar a mensagem do Protocolo de Iniciação de Sessão (SIP) de volta para a controladora reserva 140 para um rerroteamento através da controladora primária 140.

De acordo com outras versões da presente invenção, o Agente do Usuário (UA) 108 poderá executar um registro de prioridade com as controladoras 140a-N, pelo qual o Agente do Usuário (UA) 108 é registrado com a primeira controladora 140a a menos que o Agente do Usuário (UA) 108 determine que a primeira controladora 140a está fora de serviço ou de outra forma indisponível para fornecer funções do Protocolo de Iniciação de Sessão (SIP), em cujo

caso o Agente do Usuário (UA) 108 poderá registrar com a segunda controladora 140b.

De acordo com ainda outras versões da presente invenção, uma configuração de rede pico-a-pico do Protocolo de Iniciação de Sessão (SIP) poderá ser empregada, em cujo
5 caso o Agente do Usuário (UA) 108 poderá registrar com uma controladora 140 em outro ponto terminal ou pluralidade de pontos terminais.

O Agente do Usuário (UA) 108 poderá compreender uma
10 memória 112 e um processador 124 para executar rotinas armazenadas na memória 112 bem como processar mensagens do Protocolo de Iniciação de Sessão (SIP) de entrada/saída e mídia. A memória 112 poderá incluir um módulo de descoberta 116 e uma lista de controladoras 120. O módulo de
15 descoberta 116 poderá ser empregado para descobrir os dispositivos no sistema 100 que compreendem controladoras 140 capazes de controlar o Agente do Usuário (UA) 108. De acordo com pelo menos algumas versões da presente invenção, o módulo de descoberta 116 poderá ser adaptado para enviar
20 uma solicitação de descoberta a que qualquer das controladoras 140 disponíveis pode responder. Com base nas respostas (ou falta delas) recebidas das controladoras 140, o módulo de descoberta 116 pode popular a lista 120 com um número de controladoras 140. O módulo de descoberta 116
25 poderá então ser capaz de criar uma lista ordenada 128 que compreende uma listagem de prioridade das controladoras 140 com base em seus respectivos atributos 132. O Agente do Usuário (UA) 108 poderá então determinar qual controladora 140 registrar-se com base na ordem das controladoras 140 na
30 lista ordenada 128.

Além de fornecer a capacidade de descobrir e arbitrar entre controladoras 140, o módulo de descoberta 116 poderá ser ainda adaptado para monitorar o estado do sistema de comunicação 100 para determinar se há qualquer falha na rede corrente 104, falhas no servidor 136, falhas no portal 148, ou qualquer outro tipo de falha que poderá afetar a relação entre o Agente do Usuário (UA) 108 e suas controladoras 140. Como será discutido em maior detalhe aqui, o módulo de descoberta 116 poderá ser adaptado para monitorar proativamente e reativamente o estado do sistema 100 e de seus componentes. Enquanto monitora proativamente o estado do sistema 100, o módulo de descoberta 116 poderá empregar mensagens do Protocolo de Iniciação de Sessão (SIP) não-diálogo juntamente com uma lógica predeterminada para determinar o estado do sistema 100. O Agente do Usuário (UA) 108 poderá adicionalmente ser orientado por outro componente do sistema 100 (por exemplo, o portal 148) para iniciar reativamente o monitoramento do estado do sistema 100. Dotar o Agente do Usuário (UA) 108 com a capacidade de monitorar o estado do sistema 100 é um desvio das técnicas de monitoramento de rede da tecnologia anterior, pois a lógica do Agente do Usuário (UA) 108 é utilizada em vez de descarregar o ônus do processamento para outro componente, como o roteador. Isto fornece a vantagem surpreendente de permitir que cada Agente do Usuário (UA) 108 monitore o estado do sistema 100 independentemente, o que fornece mais visões do sistema 100 e permite que cada Agente do Usuário (UA) 108 mantenha seus registros pessoais para suas controladoras 140. Em outras palavras, ao utilizar uma combinação da inteligência do

Agente do Usuário (UA) 108 e de outros componentes no sistema 100 (por exemplo, o portal 148 e/ou os servidores 136), um quadro mais preciso e atualizado do estado do sistema 100 pode ser obtido. Permitir que o Agente do

5 Usuário (UA) 108 inspecione a operabilidade da camada de rede (por exemplo, ao enviar pacotes IP através do sistema 100), a camada de aplicação do Protocolo de Iniciação de Sessão (SIP) (por exemplo, ao enviar mensagens do Protocolo de Iniciação de Sessão (SIP) através do sistema 100), e o

10 agregado dos dois pode ainda aumentar a precisão do quadro da saúde do sistema.

Os servidores 136 e o portal 148 também poderão compreender um módulo de descoberta 144 para avaliar o estado do sistema 100. Mais especificamente, cada módulo de

15 descoberta 144 poderá ser utilizado para monitorar independentemente o estado de vários componentes pares (por exemplo, componentes do sistema 100 que estão adjacentes ao dispositivo que compreende o módulo de descoberta 144) bem como componentes da extremidade distante (por exemplo,

20 componentes do sistema 100 que não estão adjacentes ao dispositivo que compreende o módulo de descoberta 144). Cada módulo de descoberta 144 poderá ser utilizado para avaliar independentemente o estado do sistema 100 e os componentes do mesmo.

25 De acordo com pelo menos algumas versões da presente invenção, os módulos de descoberta 144 poderão compreender um módulo de software que é capaz de ser acessado por agentes do usuário 108 ou outros pontos terminais 156 de maneira agrupada (isto é, múltiplos servidores 136 poderão

30 ser capazes de responder a uma pergunta de um ponto

terminal que perguntar: "qual controladora devo usar") ou como um unitário. Os módulos de descoberta 144 podem ser implementados utilizando uma pletora de protocolos e ainda podem suportar múltiplos protocolos de uma vez. Mais especificamente, cada módulo de descoberta 144 poderá ser adaptado para suportar um ou mais de SOAP/HTTP, SXAP (outra norma XML sobre HTTP como SOAP) e até o Protocolo de Iniciação de Sessão (SIP) (por exemplo, ao fornecer a lista de controladoras 140 no corpo da mensagem do Protocolo de Iniciação de Sessão (SIP)).

O módulo de descoberta 144 poderá ser adaptado para determinar sua própria lista de controladoras para um agente de usuário 108 dado (que ele pode em última instância fornecer ao agente usuário 108 quando solicitado) através do processamento de regras. O processamento de regras poderá ser codificado duro (por exemplo, código Java) ou poderá compreender um motor de regras que toma um script, como XML, analisa-o, e o executa quando quiser determinar qual é a controladora 140 mais apropriada para o agente usuário 108 solicitando uma lista de controladoras. O tipo de regras que poderão ser incluídas no algoritmo incluem, sem a elas se limitar:

(1) Inspeção da localidade da rede que analisa a topologia de rede crua (por exemplo, ao analisar pacotes IP transmitidos pela rede) para determinar a controladora 140 mais apropriada para o agente usuário 108. Essa regra poderá incluir uma função de gerenciamento de largura de banda, em que o módulo de descoberta 144 inspeciona o IP do agente usuário 108 solicitante, então faz uma pesquisa para uma loja de largura de banda que lista a largura de banda

mais bem disponível e então seleciona a controladora 140 de
melhor casamento para o agente usuário 108. Neste caso, o
melhor casamento mais provavelmente corresponderia ao
servidor 136 que compreende uma controladora 140 que está
5 mais próxima do agente usuário 108 e tem uma largura de
banda disponível.

(2) Algoritmo de inspeção de segurança, pois poderá
haver certos casos em que o agente de usuário 108 deve
conectar a um servidor 136 específico/controladora 140 para
10 fins de segurança. Por exemplo, o telefone do Principal
Executivo da Empresa (CEO) poderá querer conectar apenas
com os servidores de mais alta segurança que são
constantemente monitorados e consertados dentro de
segundos. Por outro lado, o telefone do suporte técnico
15 poderá ter permissão de conectar a qualquer um de um
conjunto de servidores 136 que formam uma fazenda de
servidores, em que consertos de segurança são tratados
dentro de 24 horas.

(3) Algoritmo de designação do usuário em que o módulo
20 de descoberta 144 poderá inspecionar um mapeamento de quais
servidores 136 podem fornecer serviço para determinado
usuário. Se há múltiplos servidores, como em uma
configuração geo-redundante, múltiplas controladoras 140
podem ser retornadas na resposta.

25 (4) Algoritmo de regras negociais em que o módulo de
descoberta 144 poderá ter alças fornecidas pelo cliente no
script que diz que todos os vendedores utilizam um servidor
136 e todo o pessoal de suporte técnico utilizam outro
servidor.

30 (5) Algoritmo de modalidade de dispositivo que pode

ser iniciado quando o agente usuário solicitante 108 expressa seu modo (por exemplo, voz, mensagem instantânea (IM), vídeo, etc.) quando procura por uma controladora 140. Quando empregar este algoritmo, o módulo de descoberta 144
5 poderá pesquisar uma designação de capacidades internas para escolher a melhor controladora 140 que fornece mais tipos de modos para o usuário. Por exemplo, o agente usuário 108 que pode fazer voz e IM preferiria um servidor 136 que seja capaz de suportar ambas essas funções em vez
10 de apenas um servidor de voz. E

(6) Algoritmo de compatibilidade de protocolo que pode ser iniciado quando o agente usuário solicitante 108 identifica que ele suporta um conjunto de protocolo específico. Isto é particularmente útil em Protocolo de
15 Iniciação de Sessão (SIP), pois o Protocolo de Iniciação de Sessão (SIP) é uma multidão de extensões de protocolos. Quando o agente usuário solicitante 108 pede por uma controladora 140, ela pode expressar os recursos de protocolo que ela suporta (por exemplo, assinaturas de
20 presença ou assinaturas em geral) e o servidor pode encontrar o melhor casamento para aquele tipo de agente usuário 108.

Com referência agora à Figura 2, será descrito um método de descoberta e registro de controladora, de acordo
25 com pelo menos algumas versões da presente invenção. O método poderá ser executado por um ponto terminal, como o Agente do Usuário (UA) 108 no sistema de comunicação 100. Cada Agente do Usuário (UA) 108 no sistema de comunicação poderá ser adaptado para descobrir e registrar com
30 diferentes controladoras 140. O método é iniciado quando o

ponto terminal envia uma mensagem de descoberta (etapa 204). A mensagem de descoberta, de acordo com pelo menos uma versão da presente invenção, compreende qualquer tipo conhecido de mensagem de descoberta incluindo mensagens do
5 Protocolo de Iniciação de Sessão (SIP) (por exemplo, mensagem "OPTIONS", mensagem "NOTIFY", ou mensagem "SUBSCRIBE") que pode ser transmitida para um ou mais outros componentes no sistema 100 para testar/consultar a funcionalidade do Protocolo de Iniciação de Sessão (SIP) do
10 componente.

Quando a mensagem de descoberta é recebida pelos outros componentes do sistema 100 (por exemplo, os servidores 136 e/ou o portal 148) que compreende uma controladora 140, o componente responde à mensagem de
15 descoberta com uma mensagem de resposta. Alternativamente, se nenhum componente estiver disponível atualmente para responder à mensagem de descoberta, então nenhuma mensagem de resposta é mandada de volta para o ponto terminal iniciador. As mensagens de resposta da controladora 140 é
20 então recebida na ponta terminal iniciadora (etapa 208). Ao o ponto terminal receber essas respostas, ou a falta de respostas para as mensagens de descobertas dirigidas, o ponto terminal empregará seu módulo de descoberta 116 para popular a lista de controladoras 120.

25 As mensagens de resposta também poderão incluir os atributos 132 de cada controladora respondente 140. Exemplos da informação de atributo contida na mensagem de resposta incluem, sem limitação, as capacidades de processamento do servidor 136 ou do portal 148
30 correspondente, as extensões do Protocolo de Iniciação de

Sessão (SIP) (isto é, funções do Protocolo de Iniciação de Sessão (SIP)) fornecidas pela controladora 140, o número de Agentes do Usuário (UA) registradas atualmente na controladora 140, a proximidade da controladora 140 ao ponto terminal (isto é, número de saltos entre o ponto terminal e o dispositivo correspondente), e assim por diante. O módulo de descoberta 116 do ponto terminal poderá utilizar a informação de atributo para arbitrar a ordem das controladoras na lista ordenada 128 (etapa 212). O módulo de descoberta 116 poderá empregar qualquer tipo de algoritmo de arbitragem conhecido para determinar a ordem das controladoras 140. Por exemplo, o módulo de descoberta 116 poderá tentar otimizar todos os atributos listados para todas as controladoras 140. Alternativamente, o módulo de descoberta 116 poderá colocar a controladora 140 com um atributo selecionado sendo mais bem adequado para as necessidades do ponto terminal mais alto na lista ordenada 128.

Após o módulo de descoberta 116 do ponto terminal haver gerado a lista ordenada de controladoras 128, o módulo de descoberta 116 seleciona uma ou mais controladoras 140 com as quais o ponto terminal registrará (etapa 216). As controladoras 140 poderão ser selecionadas com base em sua ordem respectiva na lista ordenada de controladoras 128. De acordo com pelo menos uma versão da presente invenção, o módulo de descoberta 116 poderá selecionar uma controladora 140 de um servidor 136 e uma controladora do portal 148 com as quais registrar simultaneamente. Em uma configuração ativa-reserva, o ponto terminal poderá selecionar a controladora 140 do servidor

136 como a controladora primária e a controladora 140 do portal 148 como a controladora secundária ou de reserva.

Após a seleção da controladora 140, o ponto terminal tem permissão para registrar com as controladoras 5 selecionadas 140 (etapa 220). De acordo com pelo menos algumas versões da presente invenção, o ponto terminal poderá ser adaptado para registrar com controladoras 140 tendo capacidades diferentes e recursos do Protocolo de Iniciação de Sessão (SIP). Por exemplo, o ponto terminal 10 poderá ter permissão para registrar simultaneamente com uma primeira controladora 140 utilizando extensões do Protocolo de Iniciação de Sessão (SIP) estendidas e uma segunda controladora 140 utilizando extensões do Protocolo de Iniciação de Sessão (SIP) padrão. As extensões do Protocolo 15 de Iniciação de Sessão (SIP) estendidas poderão ser utilizadas pela primeira controladora 140 para fornecer recursos adicionais não alcançados através da segunda controladora 140.

Uma mensagem "SIP REGISTER, SUBSCRIBE, ou OPTIONS", ou 20 outra sinalização do Protocolo de Iniciação de Sessão (SIP) poderá ser transmitida para detectar se a controladora primária 140 ainda está online e disponível para facilitar as mensagens do Protocolo de Iniciação de Sessão (SIP). Por exemplo, uma mensagem "SIP REGISTER" poderá ser enviada 25 pelo ponto terminal para a controladora selecionada 140 para iniciar o processo de registro. Além de dotar o ponto terminal com a capacidade de registrar com suas controladoras 140, a mensagem "SIP REGISTER" também poderá ser utilizada como uma batida de coração para as 30 controladoras 140. A frequência da transmissão da mensagem

"SIP REGISTER" poderá ser configurada com base nas exigências do sistema. Em outras palavras, o ponto terminal poderá enviar registros renovados para qualquer controladora 140 com a qual estiver registrado.

5 Tanto na configuração ativa-reserva como na configuração ativa-ativa, o ponto terminal poderá registrar concorrentemente com todas suas controladoras 140 selecionadas. Durante sua operação, o ponto terminal poderá tentar manter registros ativos concorrentes com as
10 controladoras 140 (por exemplo, através da transmissão periódica de mensagens "SIP REGISTER" subseqüentes). Em uma configuração ativa-ativa, o ponto terminal poderá ter permissão para enviar/receber mensagens do Protocolo de Iniciação de Sessão (SIP) de/para qualquer uma das
15 controladoras 140 com as quais estiver registrado. Nessa configuração, o ponto terminal estará registrado simultaneamente com duas ou mais controladoras 140. Este registro dual permitira que solicitações do Protocolo de Iniciação de Sessão (SIP) de entrada (por exemplo,
20 mensagens SIP INVITE) de qualquer uma das controladoras 140 com as quais o ponto terminal está registrado (por exemplo, quer a primeira controladora 140a, a segunda controladora 140b, a terceira controladora 140c, etc.). Se o ponto terminal for configurado com uma política de utilizar um
25 modelo de controladora ativa-ativa, então o ponto terminal poderá considerar que a chamada de entrada de uma controladora anteriormente falhada 140 como se ele tivesse vindo de uma controladora 140 em serviço. Quando isso ocorre, o ponto terminal poderá tentar novamente o
30 algoritmo para detectar se o servidor falhado voltou ao

serviço. O ponto terminal será configurado para permitir o recebimento dessas mensagens do Protocolo de Iniciação de Sessão (SIP) de qualquer controladora 140. De acordo com pelo menos algumas versões da presente invenção, o ponto terminal tratará os registros como registros independentes, mantendo cada um com a lógica de registro aqui discutida. Mais especificamente, o ponto terminal terá permissão de registrar o mesmo Endereço de Registro (AOR) com cada controladora, embora a implementação do ponto terminal pode ser flexível para acomodar os Endereços de Registro (AOR) diferentes. Isto também é verdadeiro para a configuração ativa-reserva.

Em uma configuração ativa-reserva, por outro lado, o ponto terminal poderá apenas ter permissão de rotear chamadas de saída e receber chamadas de entrada de sua controladora primária 140. Enquanto operacional, esta controladora primária 140 também poderá ser referida como a controladora de chamada ativa 140. As outras controladoras 140 com as quais o ponto terminal estiver registrado poderão ser referidas como as controladoras inativas ou de reserva.

Na configuração ativa-reserva, se o ponto terminal receber uma chamada de entrada da controladora secundária o de reserva 140 enquanto o ponto terminal estiver no modo primário (isto é, o ponto terminal acredita que a controladora primária 140 está ativa), então o ponto terminal:

- (1) Responderá à controladora secundária 140 com uma mensagem de tentativa 100;
- (2) Enviará uma renovação de registro para a

controladora primária 140 para ver se a controladora primária ainda está online e disponível para facilitar as mensagens do Protocolo de Iniciação de Sessão (SIP);

(3) Se a controladora primária 140 ainda estiver online, então o ponto terminal enviará uma resposta de redirecionamento 305 (isto é, Use Proxy) para a controladora secundária 140. A resposta de redirecionamento 305 rejeitará a chamada através da controladora de chamada secundária e solicitará que a controladora secundária 140 re-roteie a sinalização através da controladora primária 140. E

(4) Se a controladora primária não estiver mais online, então o ponto terminal fornecerá processamento de chamada padrão para a chamada recebida. Como parte deste processo, o ponto terminal falhará para a controladora secundária 140 da controladora primária 140 e renovará seu registro com a controladora secundária 140 e renova seu registro com a controladora secundária 140.

Na configuração ativa-reserva, se o ponto terminal receber uma chamada de entrada de sua controladora primária 140 enquanto ele estiver operando no modo falhado (isto é, sob a suposição de que o estado de sua controladora primária 140 está fora de serviço e está utilizando a controladora secundária 140 como a controladora ativa), então a chamada poderá ser rejeitada.

Durante uma condição de falha ou qualquer outro tempo quando o ponto terminal acreditar que o componente do sistema 100 está fora de serviço, o ponto terminal não tentará estabelecer uma sessão de comunicação em tempo real com a controladora primária 140. Adicionalmente, o ponto

terminal falhará para a segunda ou a próxima controladora
140 na lista ordenada de controladoras 128. A sinalização
de chamada roteada através da controladora sobrevivente 140
(isto é, secundária, terciária, ou de reserva) permitirá ao
5 usuário do ponto terminal enviar e receber novas chamadas
durante o período de falha.

Como parte do processo de falha, que será descrito em
maior detalhe abaixo, o ponto terminal identificará o
endereço para a controladora ativa 140 e ainda derivará os
10 atributos e recursos associados suportados pela
controladora 140. Em outras palavras, o ponto terminal
poderá ser adaptado para derivar se a controladora 140 com
a qual ele está registrado é designada como
"estendida/proprietária" ou "SIP básico", por exemplo. O
15 módulo de descoberta 116 do ponto terminal poderá ser
adaptado para descobrir se uma controladora utiliza o
Protocolo de Iniciação de Sessão (SIP)básico ou estendido
utilizando a lógica seguinte:

(1) Quando da falha o ponto terminal renovará seu
20 registro com cada controladora 140.

(2) Como parte desse processo, o ponto terminal
tentará re-assinar com todos os pacotes de recursos da
controladora primária 140 com a controladora secundária
140.

25 (3) Quando o ponto terminal enviar uma solicitação
"SUBSCRIBE" para a controladora secundária 140, a
controladora secundária não reconhecerá a solicitação de
assinatura de recurso se ele apenas suportar operações do
Protocolo de Iniciação de Sessão (SIP) básicas. E então

30 (4) A controladora secundária simples 140 responderá

com Erro de Cliente 405 método não permitido.

O ponto terminal poderá utilizar esta informação para identificar a controladora secundária 140 como uma controladora enquadrada na norma IEFT do Protocolo de Iniciação de Sessão (SIP). O ponto terminal então exibirá apenas recursos do Protocolo de Iniciação de Sessão (SIP) básicos em sua Interface de Usuário (UI) enquanto operar no modo falhado. Se a controladora ativa 140 for designada como "estendida" (por exemplo, porque ela respondeu apropriadamente à solicitação "SUBSCRIBE"), então o ponto terminal utilizará o Protocolo de Iniciação de Sessão (SIP) com as extensões estendidas para chamada e processamento de recursos e exibirá uma UI compatível.

Recursos adicionais que poderão ser fornecidos em uma configuração ativa-reserva incluem, sem limitação:

(1) O ponto terminal nunca roteará chamadas de saída para a controladora inativa 140.

(2) Quando o ponto terminal falhar da controladora ativa 140 para a controladora reserva 140, a controladora anteriormente ativa 140 será designada como inativa e a controladora anteriormente inativa será designada como ativa.

(3) O ponto terminal aguardará até todas as chamadas ativas tiverem sido completadas antes de falhar para a controladora designada 140. Em outras palavras, nenhuma chamada nova de entrada será aceita pelo ponto terminal da controladora recém designada como controladora ativa 140 até as chamadas ativas haverem terminado (isto é, até o ponto terminal receber uma mensagem "BYE" da rede 104 para as chamadas ativas ou quem chamou já desligou). De modo

similar, nenhuma chamada de saída será permitida até a falha estar completa. E

(4) Se o ponto terminal receber qualquer mensagem de sinalização da controladora primária 140, mas fora de serviço, enquanto ela estiver utilizando a controladora secundária 140 então as mensagens de sinalização da controladora primária 140 marcadas como fora de serviço serão ignoradas. Entretanto, poderá haver uma exceção a esta regra. A saber, se o ponto terminal receber uma mensagem "NOTIFY" de sua controladora primária pedindo que registre novamente, então o ponto terminal iniciará quer uma renovação ou a tentativa de renovar seu registro. Neste caso o ponto terminal responderá ao "NOTIFY" utilizando o processamento do Protocolo de Iniciação de Sessão (SIP) padrão descrito acima.

Após o ponto terminal registrou com sua respectiva controladora 140, o método termina (etapa 224).

Com referência agora à Figura 3, um método de determinação do estado do sistema de comunicação 100 será descrito de acordo com pelo menos algumas versões da presente invenção. Em uma configuração de sobrevivência, poderá ser importante para os portais 148 serem equipados para detectar quando rotear a sinalização de chamada através de uma via de sinalização primária ou secundária. O método é iniciado quando o portal 148 envia uma mensagem "SIP OPTIONS" para outro componente no sistema de comunicação 100 (etapa 304). Esses componentes poderão corresponder aos componentes do Protocolo de Iniciação de Sessão (SIP) ativados. O componente poderá ainda corresponder a componentes pares (isto é, componentes que

possuem pelo menos um componente intermediário entre eles e o portal 148). De acordo com pelo menos algumas versões da presente invenção, o monitoramento proativo dos componentes de extremidade distante do Protocolo de Iniciação de Sessão (SIP) deve ser feito parcimoniosamente, normalmente apenas se o administrador do sistema 100 souber que os componentes intermediários não são capazes de monitorar seus pares. De acordo com versões da presente invenção, o portal 148 poderá enviar a mensagem "SIP OPTIONS" com uma fixação de MaxForwards=0, com isso assegurando que a mensagem "OPTIONS" não atravessa mais do que um único salto (isto é, ela é direcionada no sentido de um componente par).

Como pode ser apreciado por alguém habilitado na tecnologia, embora técnicas de monitoramento empregando a mensagem "SIP OPTIONS" são aqui descritas, qualquer outro tipo de transação do Protocolo de Iniciação de Sessão (SIP) não-diálogo poderá ser utilizada para monitorar o estado do sistema de comunicação 100 e seus componentes. Mais especificamente, uma mensagem genérica do Protocolo de Iniciação de Sessão (SIP) (por exemplo, uma mensagem "INFO METHOD", "MESSAGE METHOD", ou até uma mensagem do Protocolo de Iniciação de Sessão (SIP) vazia) poderá ser transmitida para invocar qualquer tipo de resposta com base em Protocolo de Iniciação de Sessão (SIP). A mensagem do Protocolo de Iniciação de Sessão (SIP) transmitida pelo portal 1487 também poderá incluir instruções a serem executadas pelo receptor da mensagem. Por exemplo, uma mensagem SIP poderá ser gerada compreendendo uma mensagem XML (xExtensible Markup Language) reportando a saúde do portal 148 e quaisquer outros componentes monitorados pelo

portal 148, como componentes pares, bem como ações a serem tomadas pelo receptor com base na saúde reportada do portal 148.

Após o portal 148 enviar a mensagem SIP OPTIONS ele
5 aguarda o recebimento de uma resposta (etapas 308 e 312). A quantidade de tempo que o portal 148 aguarda pelo recebimento da resposta poderá variar dependendo das características do sistema 100. De acordo com pelo menos uma versão da presente invenção, o comprimento de tempo que
10 o portal 148 aguarda poderá ser determinado ao implementar uma função SIP Timer como o SIP Timer B ou o SIP Timer F (SIP Timer B e F são cronômetros do Protocolo de Iniciação de Sessão (SIP) padrão definidos na RFC 3261, o conteúdo inteiro da qual são aqui incorporados por esta referência)
15 que cancela as transações de sinalização do Protocolo de Iniciação de Sessão (SIP) (como a mensagem "SIP INVITE") se nenhuma resposta do Protocolo de Iniciação de Sessão (SIP) for recebida dentro de um número predeterminado de segundos após a solicitação ter sido enviada. O Timer B ou o Timer F
20 é cancelado ou curto circuitado se qualquer resposta do Protocolo de Iniciação de Sessão (SIP) (mesmo a Tentativa 100) for recebida. No entanto, se o Time B dispara, o portal 148 poderá ser obrigado a cancelar a transação do Protocolo de Iniciação de Sessão (SIP) ofensiva e tentar
25 rotear a solicitação utilizando uma rota alternativa. De acordo com pelo menos algumas versões da presente invenção, se todos os endereços de roteamento conhecidos do portal 148 tiverem sido exauridos, então o portal do Protocolo de Iniciação de Sessão (SIP) 148 poderá responder à transação
30 de sinalização do Protocolo de Iniciação de Sessão (SIP)

original com uma Solicitação de Intervalo 408.

Uma vez recebida uma resposta (por exemplo, quer como uma resposta efetiva ou como a determinação de que nenhuma resposta foi recebida dentro de uma quantidade
5 predeterminada de tempo), o método continua com o portal 148 empregando o módulo de descoberta 144 para determinar se a resposta corresponde a uma condição de falha (etapa 316). A resposta poderá indicar que uma rede 104 ou o componente do sistema 100 falhou se qualquer uma das
10 condições seguintes são satisfeitas:

(1) A solicitação de monitoramento "OPTIONS" falhar devido a expiração do cronômetro.

(2) Um número predeterminado (por exemplo, cinco) de falhas de transação de solicitação do Protocolo de
15 Iniciação de Sessão (SIP) consecutivas ocorrerem devido a expirações da transação e/ou expirações do Timer B (para transações "INVITE"). Ou

(3) Qualquer uma das respostas de classe 400 ou 500 forem recebidas com um cabeçalho Retry-After para uma
20 solicitação de monitoramento "OPTIONS" se e apenas se a monitoração estiver sendo feita salto-a-salto (isto é, Max-Forwards=1) e não ponta-a-ponta (isto é, Max-Forwards >1), mais o endereço ser marcado como "sobrecarregado" por pelo menos a duração especificada no cabeçalho Retry-After.

25 Com relação a condição (3), diálogos existentes que incluem o endereço IP do endereço devem continuar a utilizar esse endereço a menos que ocorra uma falha, mas o ponto terminal não deve utilizar esse endereço para novos diálogos até ele haver recuperado. Nos casos em que um
30 diálogo existente está utilizando um nome de hospedeiro em

vez de um endereço IP, a resolução desse nome de hospedeiro para cada transação ocorrerá e o endereço retornado seria o endereço de prioridade mais alta que estiver disponível. Se o nome de hospedeiro só resolver para um único endereço IP, e esse endereço estiver marcado como "sobrecarregado", então a solicitação deve ser enviada. O efeito líquido da condição (3) é que o módulo de descoberta 144 do portal 148 deve estar ciente de três estados: disponível; fora de serviço; e sobrecarregado. Endereços que estão marcados como sobrecarregados continuam a receber solicitações subseqüentes dentro de um diálogo, mas nenhuma solicitação de diálogo novo.

Se, com base na resposta à mensagem OPTIONS, o módulo de descoberta 144 do portal 148 determina que não há condição de falha e que o sistema 100 está em estado normal de operação, então o módulo de descoberta 144 continuará ao determinar se instruções estão incluídas na resposta (etapa 320). O módulo de descoberta 144 poderá analisar a resposta para instruções executáveis que estão incluídas na resposta ou apensadas à resposta (isto é, em um cabeçalho ou rodapé da mensagem). Se instruções estão incluídas na resposta, então as instruções são executadas (etapa 324). Daí em diante, ou no evento de que a resposta não incluiu instruções, o módulo de descoberta 144 continua ao atualizar seus registros para o estado do sistema 100 para refletir a operação do componente respondedor, como o servidor 136 (etapa 328). Uma vez que o estado da rede foi atualizado, o método continua com o módulo de descoberta 144 determinando se já é hora de enviar uma nova mensagem (etapa 332). Mais particularmente, o portal 148 poderá

utilizar a transmissão periódica das mensagens "SIP OPTIONS" para outros servidores do Protocolo de Iniciação de Sessão (SIP) 136 como um mecanismo de batidas de coração para determinar se os demais servidores do Protocolo de Iniciação de Sessão (SIP) 136 estão ou não ativos. A mensagem "OPTIONS" poderá ser enviada para os demais componentes do sistema 100 a um intervalo predeterminado. O comprimento do intervalo predeterminado poderá ser determinado ao implementar um SIP Timer B ou um variante do mesmo. Mais especificamente, o monitoramento "OPTIONS" pode ser feito a intervalos diferentes dependendo sobre se o portal 148 detecta ou não uma condição de falha.

De acordo com pelo menos algumas versões da presente invenção, o intervalo de monitoramento proativo para a mensagem "SIP OPTIONS" poderá ser configurado dentro de uma faixa de cerca de 60 a cerca de 100.000 segundos e deve utilizar um tempo aleatório uniforme entre 75% e 125% do valor configurado entre tentativas de monitoramento subseqüentes. Por exemplo, se o intervalo de monitoramento proativo for fixado para 60 segundos, então o intervalo efetivo entre transmissão de mensagens "OPTIONS" pode ser distribuído uniformemente entre 45 e 74 segundos. Esta introdução deliberada de jitter no processo de monitoramento proativo permite que as solicitações permaneçam não-sincronizadas assim espalhando igualmente a carga nos componentes monitorados (isto é, servidores 136) no tempo. Em uma versão, o intervalo de monitoramento proativo poderá ser configurado para ser cerca de 900 segundos ou 15 minutos.

De acordo com pelo menos algumas versões da presente

invenção, o intervalo de monitoramento reativo para a mensagem "SIP OPTIONS" poderá ser configurado dentro de uma faixa de cerca de 10 a cerca de 3.600 segundos e também poderá ter um tempo aleatório uniforme entre 75% e 125% do valor configurado entre tentativas de monitoramento subseqüentes. A provisão de um cronômetro separado para o monitoramento reativo (em oposição ao monitoramento proativo) permite ao portal 148 detectar mais rapidamente quando o componente atualmente fora de serviço sendo monitorado torna-se disponível novamente. Em uma versão, o intervalo de monitoramento reativo poderá ser configurado para ser cerca de 120 segundos.

Embora versões exemplares da presente invenção estejam sendo descritas em conexão com a utilização do SIP Timer B, qualquer faixa de valores, com ou sem uma modificação no tempo aleatório uniforme daquele valor, poderá ser implementada sem desviar dos princípios da presente invenção. Adicionalmente, os intervalos de monitoramento poderão ser modificados com base em ganchos lógicos empresariais externos. Por exemplo, se o mecanismo de monitoramento estiver enganchado dentro de um sistema de gerenciamento de largura de banda, o sistema de monitoramento poderá ainda ajustar o intervalo de monitoramento por algum coeficiente que represente a largura de banda disponível na rede.

Com referência de volta à etapa 316, se o módulo de descoberta 144 determina que a resposta corresponde a uma condição de falha, então o módulo de descoberta 144 atualizará seus registros do estado do sistema 100 para refletir a falha (etapa 336). Como resultado de detectar

esta falha no componente, o portal 148 falhará e iniciará a operar em estado de falha, especialmente se o componente falhado residir em uma via de comunicação primária.

Durante a falha o módulo de descoberta 144 do portal 5 148 iniciará a monitorar reativamente os componentes no sistema 100 ao continuar a enviar a mensagem "OPTIONS" ao componente identificado como fora de serviço (etapa 340). Este monitoramento reativo permite que o módulo de descoberta 144 do portal 148 detecte quando o componente 10 voltar online. Quando o monitoramento reativo começa, o portal 148 deixará de monitorar proativamente o componente e começará a aplicar regras do monitoramento reativo. Mais especificamente, durante o monitoramento reativo, o módulo de descoberta 144 do portal 148 poderá iniciar um teste de 15 manutenção para determinar se o componente monitorado está ou não disponível ou fora de serviço (etapa 344). O teste de manutenção poderá empregar um algoritmo de monitoramento similar ao algoritmo de monitoramento proativo. O módulo de descoberta 144 do portal 148 continuará a aplicar este 20 teste de manutenção até falhar (isto é, até o estado do componente mude de fora de serviço para disponível) (etapa 348). Durante o teste de manutenção, o portal 148 poderá transmitir qualquer tipo de solicitação do Protocolo de Iniciação de Sessão (SIP) (por exemplo, "INVITE", 25 "SUBSCRIBE", "NOTIFY", etc.) ao componente atualmente marcado como fora de serviço. Se uma ou mais das condições seguintes aplicarem, então o módulo de descoberta 144 do portal 148 continuará a marcar o componente como fora de serviço:

30 (1) SIP Timer B dispara após uma mensagem "INVITE" ter

sido transmitida.

(b) O portal 148 recebe uma resposta da Solicitação de Intervalo 408.

(3) A transação de solicitação do Protocolo de Iniciação de Sessão (SIP) expira; ou

(4) Ocorre um erro de rede 104 ou de camada de transporte enquanto tenta enviar a solicitação.

Se nenhuma das condições listadas acima aplicar durante o teste de manutenção, então o módulo de descoberta 144 do portal 148 determinará que a falha já ocorreu e o método continuará com a etapa 328. De acordo com pelo menos algumas versões da presente invenção, o monitoramento reativo e os testes de manutenção continuarão a ser aplicados até o componente objeto do monitoramento responde com qualquer resposta do Protocolo de Iniciação de Sessão (SIP) exceto Serviço Não Disponível 503 para duas tentativas de solicitação "OPTIONS" consecutivas. Uma vez essas condições tenham sido satisfeitas, o portal 148 poderá considerar o componente de volta ao serviço, poderá reverter para o algoritmo de monitoramento proativo, pode gerar um evento do Protocolo de Gerenciamento de Rede (SNMP =Simple Simple Network Management Protocol) e, se aplicável, iniciará a utilizar o componente agora ativo.

Como pode ser apreciado por alguém habilitado na tecnologia, o portal 148 não é o único componente do sistema 100 que poderá manter informação de realocação de via. Ao contrário, qualquer elemento de rede do Protocolo de Iniciação de Sessão (SIP) poderá ser adaptado para incluir informação de realocação de via e assemelhados. Por exemplo, um ponto terminal como o Agente do Usuário (UA)

108 também poderá manter uma tabela de realocação de via que lista as vias de comunicação que poderão ser utilizadas se certos componentes forem identificados como fora de serviço.

5 Com referência agora à Figura 4, será descrito um método de monitoramento reativo de acordo com pelo menos algumas versões da presente invenção. O método inicia quando o portal 148 recebe uma solicitação de um servidor 136 ou componente do sistema 100 similar (etapa 404). O
10 portal 148 trata a solicitação recebida da maneira normal (etapa 408). Mais especificamente, o portal 148 poderá processar a solicitação como se o componente de enviar estivesse em serviço, sem primeiro determinar se o componente está efetivamente em serviço.

15 Daí em diante, o portal 148 determina se o componente de envio está efetivamente marcado como fora de serviço com base em suas tabelas de estado mantidas internamente (etapa 412). Se o componente não estiver marcado como estando fora de serviço, então o método encerra (etapa 424). Caso
20 contrário, o portal 148 iniciará seu teste de manutenção ao enviar mensagens "SIP OPTIONS" para o componente (etapa 416). O portal 148 poderá então atualizar seus registros do estado do componente (etapa 420). Este teste de manutenção e processo de atualização do estado é repetido até o
25 componente ser determinado como estando de volta em serviço, em cujo ponto o método termina (etapa 424).

Com referência à Figura 5, a operação do portal 148 durante os estados de falha serão descritas de acordo com pelo menos algumas versões da presente invenção. Neste
30 método particular, a controladora 140 associada ao portal

148 poderão corresponder a uma controladora secundária ou de reserva 140 para um ponto terminal de sobrevivência. O método é iniciado quando o portal 148 recebe uma chamada de entrada para um ponto terminal de sobrevivência (etapa 504). O portal 148 então determina se a via de sinalização primária está disponível para uso (etapa 508). De acordo com pelo menos algumas versões da presente invenção, o portal 148 poderá referenciar suas tabelas de estado do componente interno durante esta etapa.

10 Se a via de sinalização primária for determinada como estando operacional, então o portal 148 roteia o sinal recebido para o ponto terminal alvo através da via primária (etapa 512) após o que o método termina (etapa 536). No entanto, se o portal 148 determina que a via de sinalização primária está indisponível por qualquer razão (por exemplo, uma rede 104, um servidor 136, ou outro componente na via de sinalização primária está fora de serviço), então o método continua com o portal 148 enviando o sinal ao ponto terminal alvo através da via de sinalização secundária (etapa 516). Esta etapa particular é efetuada com base na suposição de que a via de sinalização secundária não está também indisponível. Se o portal determina que a via de sinalização secundária também está indisponível, então outra via de sinalização de reserva que circunda os componentes falhados é selecionada e utilizada para enviar o sinal para o ponto terminal.

Após o sinal de chamada ter sido transmitido para o ponto terminal alvo através da via de sinalização secundária, o portal 148 aguarda para determinar se uma mensagem de resposta de redirecionamento 305 (use Proxy) é

30

recebida do ponto terminal (etapa 520). Em uma configuração ativa-reserva, o ponto terminal que recebe o sinal de chamada através da segunda via poderá transmitir uma resposta de redirecionamento 305 se o ponto terminal
5 acreditar que a via de sinalização primária está operacional. Esta crença teria por base em operações de monitoramento de estado efetuadas no ponto terminal e não no portal 148. Assim, com base na perspectiva diferente do sistema 100, o ponto terminal poderá ter um estado
10 diferente marcado para um ou mais componentes do sistema 100. Assim, se uma resposta de redirecionamento 305 é recebida pelo portal 148 com base em seu redirecionamento do sinal de chamada através da via secundária, então o portal 148 tentará redirecionar o sinal de chamada através
15 da via de sinalização primária (etapa 524). Se a via de sinalização primária é determinada como estando disponível (etapa 528) devido à transmissão bem sucedida do sinal de chamada, então o método termina na etapa 536. Se a chamada for rejeitada devido à indisponibilidade da via de
20 sinalização primária, então a chamada poderá ser rejeitada ou enviada de volta através da via de sinalização secundária (etapa 532). Adicionalmente, o portal 148 poderá enviar uma mensagem "NOTIFY" para o ponto terminal alvo instruindo-o a reverificar sua visão do estado da via de
25 sinalização primária. Daí em diante, ou se nenhuma mensagem de resposta de redirecionamento for recebida do ponto terminal, o método termina (etapa 536).

Com referência agora à Figura 6, um método de ponto terminal da determinação do estado do sistema 100 será
30 descrito de acordo com pelo menos algumas versões da

presente invenção. Inicialmente, o ponto terminal (por exemplo, o Agente do Usuário (UA) 108 de sobrevivência) opera em estado normal (etapa 604). O ponto terminal então emprega a lógica de seu módulo de descoberta 116 para
5 determinar se uma falha de rede foi detectada (etapa 608). Em uma configuração de sobrevivência é útil para as pontas terminais serem capazes de detectar quando falhar. De acordo com pelo menos algumas versões da presente invenção, a lógica do módulo de descoberta 116 utilizada pelo ponto
10 terminal determinará que uma falha de rede ocorreu se um ou mais dos eventos seguintes ocorrer:

(1) O ponto terminal não recebe uma resposta a uma mensagem "SIP REGISTER" como uma batida de coração de todas as controladoras 140 com as quais ele está tentando
15 registrar (por exemplo, suas controladoras primária e secundária 140).

(2) O ponto terminal não recebe uma resposta a uma mensagem "SIP INVITE", em que a mensagem "SIP INVITE" poderá ter sido transmitida no processo normal de tentar
20 estabelecer uma chamada de saída.

(3) O ponto terminal não recebe uma resposta a qualquer mensagem de sinalização do Protocolo de Iniciação de Sessão (SIP) enviada para a criação normal de um novo diálogo do Protocolo de Iniciação de Sessão (SIP) ou
25 mudanças em meio-diálogo; ou

(4) O ponto terminal não recebe uma resposta bem sucedida a uma solicitação crítica (que pode ser realizada por tipos diferentes de protocolos como TCP/IP, HTTP, XML, OU SOAP) de seus servidores de configuração, ou qualquer
30 outro serviço de não-comunicação fora da banda como

serviços de dados utilizados para recuperar dados relacionados à falha.

Se o ponto terminal não detecta a própria falha, então o método continua com o ponto terminal determinando se ele
5 foi notificado de uma falha (etapa 612). A notificação poderá ser recebida no ponto terminal na forma de uma mensagem "SIP NOTIFY" transmitida do portal 148, do servidor 136, ou de algum outro componente no sistema 100 que é capaz de monitorar o estado do sistema 100. A
10 mensagem "SIP NOTIFY" poderá indicar que o ponto terminal deve falhar, reinicializar, ou renovar/refrescar seu registro com todas as suas controladoras 140 (assim desviando da lógica do ponto terminal). Se nenhuma notificação for recebida, então o método retorna de volta à
15 etapa 604.

No entanto, se o ponto terminal for notificado de uma falha no sistema 100 (por exemplo, através do recebimento de uma mensagem "SIP NOTIFY"), então o ponto terminal determina se a notificação de falha está correta
20 (etapa 616). Mais especificamente, o ponto terminal poderá verificar sua lista mantida internamente de controladoras 120, 128 para determinar se qualquer uma das controladoras 140 está marcada como inativa ou de outra forma fora de serviço. Na maioria das vezes o ponto terminal simplesmente
25 cumprirá com as diretivas da mensagem "NOTIFY". No entanto, sob certas circunstâncias, o ponto terminal poderá determinar que sua visão do sistema 100 é a visão correta e poderá responder à mensagem "NOTIFY" com uma mensagem de resposta de redirecionamento (etapa 620). Esta resposta de
30 redirecionamento poderá fazer com que o componente

iniciador da mensagem "NOTIFY" verifique sua visão do sistema 100. O método então retorna para a etapa 604.

Se o ponto terminal decidir que a notificação de falha está correta ou decidir cumprir com as diretivas da mensagem "NOTIFY", então o ponto terminal determina se a mensagem NOTIFY continha instruções (etapa 624). As instruções poderão ser instruções relativamente genéricas como a tentativa de re-registrar com todas as controladoras 140. Alternativamente, as instruções poderão compreender um conjunto de instruções que exige que o ponto terminal tente e re-registre com uma controladora específica 140. O ponto terminal poderá tentar renovar ou registrar com a controladora 140 quer a intervalos longos ou curtos. O comprimento do intervalo de renovação/registo poderá variar dependendo das instruções no conjunto de instruções ou de outros fatores. As instruções também poderão conter informação da saúde para o sistema 100 inteiro conforme percebido pelo componente que transmitiu a mensagem NOTIFY. Se a mensagem de fato contém instruções, então o ponto terminal executará as instruções (etapa 628).

Após as instruções terem sido executadas pelo ponto terminal ou no evento de que a mensagem não contém instruções, o método continua com o ponto terminal executando uma falha tal que ele começa a operar em estado de reserva (etapa 632). Esta etapa também é efetuada no evento de que o ponto terminal detectou uma falha no sistema 100 ele próprio. Durante a operação no modo de falha, o ponto terminal utilizará sua controladora de reserva 140 e/ou utilizará uma via de sinalização secundária. Além de operar no modo de falha, o ponto

terminal poderá monitorar por falha no sistema 100 (etapa 636). O ponto terminal determinará que uma falha ocorreu se o módulo de descoberta 116 detectar que sua controladora primária 140 está disponível para continuar seu papel como
5 a controladora ativa. Esta lógica de ponto terminal interno poderá ser governada pela mensagem batida de coração/"SIP REGISTER" que é enviada periodicamente a todas as controladoras 140 com as quais o ponto terminal está registrado, independentemente de se a controladora 140 está
10 ou não ativa a qualquer tempo dado.

Se o ponto terminal não detecta a falha por sua própria conta, o método continua com o ponto terminal determinando se ele foi notificado da falha por outro componente (por exemplo, ao receber uma mensagem "NOTIFY"
15 do portal 148, do servidor 136, etc.) (etapa 640). Se o ponto terminal não é notificado de falha, então o método retorna à etapa 632. No entanto, se o ponto terminal de fato recebe uma mensagem "NOTIFY" indicando falha, então o método continua ao determinar se a mensagem "NOTIFY"
20 continha instruções para execução pelo ponto terminal (etapa 644). Se instruções foram incluídas na mensagem "NOTIFY", então as instruções são executadas pelo ponto terminal (etapa 648). Após a execução das instruções, se não houve instruções, ou se a falha foi detectada pelo
25 próprio ponto terminal, o método retorna à etapa 604.

De acordo com pelo menos algumas versões da presente invenção, o módulo de descoberta 116 poderá compreender um parâmetro configurável que governa se a falha das controladoras primária ou secundária 140 deve ser disparado
30 pela detecção do ponto terminal automatizado ou se ele é

apenas para ser disparado manualmente (isto é, pelo recebimento de uma mensagem "SIP NOTIFY"). O mecanismo de monitoramento da batida de coração empregado pelo módulo de descoberta 116 poderá ser feito a intervalos diferentes 5 dependendo de se o ponto terminal detecta ou não uma condição de falha.

Com referência agora à Figura 7, um método de notificação de estado será descrito de acordo com pelo menos algumas versões da presente invenção. O método inicia 10 com um componente do sistema 100 (por exemplo, o servidor 136, o portal 148, ou qualquer outro dispositivo que compreende um módulo de descoberta 144) determinar se ele deve notificar um ponto terminal, como o Agente do Usuário (UA) 108, com relação ao sistema 100 (etapa 704). 15 Tipicamente, o componente enviará uma mensagem "NOTIFY" para um ponto terminal, notificando o ponto terminal de que algum aspecto do estado do sistema 100 mudou. Por exemplo, a mensagem "NOTIFY" poderá informar o ponto terminal que um componente no sistema foi registrado como fora de serviço. 20 Alternativamente, a mensagem "NOTIFY" poderá informar o ponto terminal do envio da saúde do componente.

O método permanece na etapa 704 até ser determinado que uma mensagem de notificação deve ser transmitida para o ponto terminal. Após fazer tal determinação, o método 25 continua com o componente gerando a mensagem (por exemplo, uma mensagem "NOTIFY") (etapa 708). No entanto, como pode ser apreciado, qualquer outro tipo de mensagem do Protocolo de Iniciação de Sessão (SIP) ou não poderá ser empregada pelo componente para notificar o ponto terminal. A 30 notificação poderá permitir ao componente disparar o ponto

terminal para falhar em uma falha do sistema 100 ou
condição de recuperação. Como o ponto terminal poderá
manter uma lista ordenada de controladoras 128 e o ponto
terminal tem a capacidade de manter registros ativos com
5 todas essas controladoras, o componente do sistema 100 pode
disparar o ponto terminal para tomar medidas quando ele
detectar uma condição de falha no sistema 100. As ações
poderão ser disparadas quer ao transmitir uma mensagem de
notificação padrão (por exemplo, uma mensagem "NOTIFY" que
10 cumpre com o Protocolo de Iniciação de Sessão (SIP) IETF
padrão) ou uma mensagem estendida que contém um conjunto de
instruções específicas, por exemplo. Assim, o método
continua com o componente determinando se a mensagem de
notificação deve nela incluir instruções (etapa 712).

15 Se nenhuma instrução específica é determinada como
sendo necessária, então o componente pode dizer ao ponto
terminal para re-registrar com todas as controladoras 140
na lista ordenada de controladoras 128 e enviar uma
mensagem de notificação genérica para o ponto terminal
20 (etapa 720). Assim, qualquer ponto terminal que recebe tal
notificação tentará re-registrar com cada controladora 140
em sua lista. Com base no sucesso deste re-registro
tentado, o ponto terminal será capaz de derivar quais
controladoras 140 estão disponíveis para processar
25 transações do Protocolo de Iniciação de Sessão (SIP) (por
exemplo, suportar chamadas do Protocolo de Iniciação de
Sessão (SIP) de entrada e de saída). O ponto terminal
poderá então comportar-se de acordo com esta informação
auto-determinada utilizando a controladora de prioridade
30 mais alta 140 na lista ordenada de controladoras 128 como

sua controladora primária. Este mecanismo particular poderá utilizar mensagens "NOTIFY" cumpridoras da norma do Protocolo de Iniciação de Sessão (SIP) IETF com o parâmetro "NOTIFY" "event"="probation". Um exemplo de tal mensagem

5 "NOTIFY" é fornecida abaixo:

```
<registrationaor=sip:joe@example.comid="a7"state="active">  
  <contactid="76" state="active" event-"probation"  
    expires="0"  
    q="0.8"retry-after="0">
```

10 No entanto, se o componente determinar que instruções específicas devem ser incluídas na mensagem de notificação, então o componente poderá acrescentar um ou mais conjuntos de instrução à mensagem (etapa 716) antes de enviar a mensagem para o ponto terminal (etapa 720). Ao incorporar

15 instruções na mensagem de notificação, o componente pode dizer ao ponto terminal para começar a utilizar uma controladora específica 140 na lista de controladoras 120 do ponto terminal. Em tal cenário, o ponto terminal depende do componente para dizê-lo qual controladora 140 deve ser

20 utilizada, em vez de depender em sua própria inteligência. Este mecanismo particular poderá utilizar a mensagem "SIP NOTIFY" padrão com uma extensão estendida. A mensagem NOTIFY geralmente seguirá a norma do Protocolo de Iniciação de Sessão (SIP) para mensagens "NOTIFY". Adicionalmente,

25 ele poderá utilizar um formato de pacote de evento de perfil exemplar com o nome de evento como <eventName>changeServer</eventName> se o ponto terminal deve falhar. A mensagem também poderá incluir um carimbo de tempo e o endereço do servidor 136 contendo a controladora

30 particular 140 a qual o ponto terminal deve falhar. Um

exemplo de tal mensagem "SIP NOTIFY" estendida é fornecido abaixo com um conjunto de instrução XML:

```

NOTIFY sip:1111@10.1.75.2 SIP/2.0
Call-ID:Cid-1@10.1.75.2
5   CSeq:2 NOTIFY
    From:sip:1111@atler.com;tag=random2
    To:sip:1111@atler.com;tag=random1
    Via:SIP/2.0/UDP 10.0.0.100;branch-id=z9hG4bK-random-
the primary call controller
10  SIP/2.0/TLS 10.0.0.200; branch-id= z9hG4bK-random-cm1
    Content-Length:22
    Content-Type:application/profile+xml
    Contact:<sip:1111@10.0.0.200;transport=tls/
    Max-Forwards:69
15  User-Agent:Communication Manager v1.0
    Event:ccs-profile
    Subscription-State:active;expires=3600
    Record-Route:sip:10.0.0.100:1r;transport=UDP
    <?xml version="1.0">
20  <event>
    <eventName>changeServer</eventName>
    <eventTime>{time stamp}</eventTime>
    <eventData>{ip address}</eventData>
    </event>
25  Como pode ser apreciada por alguém habilitado na
tecnologia, as instruções poderão tomar muitas formas
diferentes que não um conjunto de instruções XML. Por
exemplo, as instruções poderão compreender um disparo
predeterminado que corresponde e causa a execução de um
30 algoritmo ou aplicação já armazenada na memória 112 do

```

ponto terminal. Adicionalmente, embora a mensagem "NOTIFY" exemplar acima inclui seu conjunto de instruções no corpo da mensagem, o conjunto de instruções também poderá ser colocado no cabeçalho ou no trailer de uma mensagem de notificação. Isto poderá variar dependendo do tipo de mensagem de notificação empregado. As instruções poderão ser utilizadas para efetuar um número de ações diferentes como transportar informação de saúde do componente remetente bem como sua informação de estado para o resto do sistema 100 bem como disparar o ponto terminal para efetuar uma tarefa particular.

Embora os fluxogramas descritos acima tenham sido discutidos em relação a uma seqüência particular de eventos, deve ser apreciado que mudanças nesta seqüência podem ocorrer sem afetar materialmente a operação da invenção. Adicionalmente, a seqüência exata dos eventos não precisa ocorrer conforme explicitadas nas versões exemplares. As técnicas exemplares aqui ilustradas não são limitadas às versões especificamente ilustradas, mas também podem ser utilizadas com as outras versões exemplares e cada recurso descrito é reivindicado individual e separadamente.

Os eventos, métodos e protocolos desta invenção podem ser implementados em um computador de finalidades gerais além de ou em lugar de o equipamento de comunicação descrito, um microprocessador programado ou microcontroladora e elementos de circuito integrado periférico, um ASIC ou outro circuito integrado, um processador de sinal digital, um circuito lógico ou eletrônico fiado como um circuito de elemento discreto, um dispositivo de lógica

programável como PLD, PLA, FPGA, PAL, um dispositivo de comunicação, como um servidor, computador pessoal, qualquer meio comparável, ou assemelhados. Em geral, qualquer dispositivo capaz de implementar uma máquina de estado que, por sua vez, é capaz de implementar a metodologia aqui ilustrada pode ser utilizado para implementar os vários métodos, protocolos e técnicas de comunicação de acordo com esta invenção.

Ademais, os métodos revelados poderão ser prontamente implementados em software utilizando ambientes de desenvolvimento de software orientado ao objeto ou procedimental que fornecem código fonte portátil que pode ser utilizado em uma variedade de plataformas de computador ou de estação de trabalho. Alternativamente, o sistema revelado poderá ser implementado parcial ou integralmente em hardware utilizando circuitos lógicos padrão ou projeto VLSI. Quer seja utilizado software ou hardware para implementar os sistemas de acordo com esta invenção é dependente da velocidade e/ou da eficiência dos requisitos do sistema, a função particular, e os sistemas de software ou hardware ou sistemas de microprocessador ou de microcomputador que estiverem sendo utilizados. O sistema, métodos e protocolos de análise aqui ilustrados podem ser prontamente implementados em hardware e/ou software utilizando qualquer sistema ou estruturas, dispositivos e/ou software já conhecidos ou posteriormente desenvolvidos por aqueles de habilidade ordinária na tecnologia aplicável a partir da descrição funcional aqui fornecida e com um conhecimento básico geral da tecnologia de comunicação.

Ademais, os métodos revelados poderão ser prontamente

implementados em software que pode ser armazenado em um meio de armazenamento, executado em um computador de finalidade geral programado com a cooperação de uma controladora e de memória, um computador de finalidade especial, um microprocessador, ou assemelhados. Nesses casos, os sistemas e métodos desta invenção podem ser implementados como programa embutido em um computador pessoal como um applet, script de JAVA® ou CGI, como um recurso residente em um servidor ou estação de trabalho de computador, como uma rotina embutida em um sistema de comunicação dedicado ou componente de sistema, ou assemelhado. O sistema também pode ser implementado ao fisicamente incorporar o sistema e/ou método dentro de um sistema de software e/ou de hardware, como os sistemas de hardware e de software de um dispositivo ou sistema de comunicação.

Portanto, é aparente que foi fornecido, de acordo com a presente invenção, sistemas, aparelhos e métodos para manter uma rede de Protocolo de Iniciação de Sessão (SIP) de sobrevivência e componentes de rede. Embora esta invenção tenha sido descrita em conjunto com um número de versões, é evidente que muitas alternativas, modificações e variações seriam ou são aparentes para aqueles de habilidade ordinária nas tecnologias aplicáveis. Assim, pretende-se abarcar todas essas alternativas, modificações, equivalentes e variações que estiverem dentro do espírito e escopo desta invenção.

REIVINDICAÇÕES

1. Método, **caracterizado** pelo fato de compreender:

receber, em um ponto terminal de comunicação ativado em um Protocolo de Iniciação de Sessão (SIP), informação de
5 controladora relacionada a uma primeira controladora;

receber, no ponto terminal de comunicação, informação de controladora relacionada a uma segunda controladora;

analisar a informação de controladora relacionada tanto à primeira como à segunda controladoras;

10 com base na etapa de análise, o ponto terminal de comunicação utiliza um módulo de descoberta para selecionar pelo menos uma da primeira e da segunda controladoras como sua controladora; e

o ponto terminal de comunicação registra com a
15 primeira controladora enquanto que o ponto terminal de comunicação estiver em um de (i) registrando e (ii) registrado com a segunda controladora, em que o ponto terminal de comunicação registra com a primeira e segunda controladoras ao enviar mensagem de registro SIP à ambas
20 primeira e segunda controladoras e recebe confirmação de recebimento das mensagens de registro SIP a partir da primeira e segunda controladoras.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de a informação de controladora
25 relacionada à primeira e à segunda controladoras compreender atributos da primeira e da segunda controladoras, respectivamente, e em que o módulo de descoberta é ainda operado para comparar os atributos da primeira controladora com os atributos da segunda
30 controladora, determinar que os atributos da primeira

controladora são mais bem adequados para controlar o dispositivo de comunicação do que os atributos da segunda controladora, selecionar a primeira controladora como a controladora primária do dispositivo, e selecionar a
5 segunda controladora como a controladora secundária do dispositivo.

3. Método, de acordo com qualquer uma das reivindicações 1 ou 2, caracterizado pelo fato de o módulo de descoberta ser ainda operado para registrar o
10 dispositivo com a primeira controladora enquanto o dispositivo estiver em um de (i) registrando e (ii) registrado com a segunda controladora, e em que o dispositivo registra com a primeira e segunda controladoras ao executar registro SIP e processo de conexão de redes.

15 4. Método, de acordo com a reivindicação 3, caracterizado pelo fato de o módulo de descoberta ser ainda operado para registrar simultaneamente com a primeira e a segunda controladoras.

20 5. Método, de acordo com a reivindicação 4, caracterizado pelo fato de os atributos da primeira controladora serem diferentes dos atributos da segunda controladora.

25 6. Método, de acordo com a reivindicação 5, caracterizado pelo fato de a primeira controladora fornecer extensões do Protocolo de Iniciação de Sessão (SIP) estendidas para o dispositivo de comunicação e em que a segunda controladora fornece extensões do Protocolo de Iniciação de Sessão (SIP) padrão para o dispositivo de comunicação.

30 7. Método, de acordo com a reivindicação 4,

caracterizado pelo fato de o dispositivo de comunicação ser registrado com a primeira e a segunda controladoras em uma de uma configuração ativa-ativa e uma configuração ativa-reserva, em que na configuração ativa-ativa o dispositivo
5 utiliza tanto a primeira como a segunda controladora para processar as chamadas de entrada e de saída, e em que na configuração ativa-reserva o dispositivo utiliza uma controladora selecionada como a controladora primária para processar as chamadas de entrada e de saída e solicitações
10 de que as chamadas de entrada recebidas de uma controladora secundária sejam redirecionadas através da controladora primária.

8. Método, de acordo com qualquer uma das reivindicações anteriores 1, 2, 3, 4, 5, 6 ou 7,
15 **caracterizado** pelo fato de o módulo de descoberta ser ainda operado para gerar uma lista de controladoras que compreende pelo menos a primeira e a segunda controladoras, comparar informação de controladora para a primeira controladora com informação de controladora para a segunda
20 controladora, e ordenar a lista de controladoras com base na comparação da informação de controladora.

9. Dispositivo de comunicação ativado pelo Protocolo de Iniciação de Sessão (SIP), **caracterizado** pelo fato de compreender:

25 uma memória e um processador para executar rotinas armazenadas na memória, a memória incluindo um módulo de descoberta operado para solicitar e receber informação de controladora relacionado a uma primeira e uma segunda controladora e selecionar pelo menos uma da primeira e da
30 segunda controladora como uma controladora com base na

controladora recebida da informação do dispositivo, em que o módulo de descoberta é ainda operável para registrar o dispositivo com a primeira controladora enquanto o dispositivo estiver em um de (i) registrando e (ii) registrado com a segunda controladora, e em que o dispositivo registra com a primeira e segunda controladoras ao executar um registro SIP e processo de conexão de rede.

10. Dispositivo, de acordo com a reivindicação 9, **caracterizado** pelo fato de a informação de controladora relacionada à primeira e à segunda controladoras compreender atributos da primeira e da segunda controladoras, respectivamente, e em que o módulo de descoberta ser ainda operado para comparar os atributos da primeira controladora com os atributos da segunda controladora, determinar que os atributos da primeira controladora são mais bem adequados para controlar o dispositivo de comunicação do que os atributos da segunda controladora, selecionar a primeira controladora como a controladora primária do dispositivo, e selecionar a segunda controladora como a controladora secundária do dispositivo.

11. Dispositivo, de acordo com qualquer uma das reivindicações 9 ou 10, **caracterizado** pelo fato de o módulo de descoberta ser ainda operado para registrar o dispositivo com a primeira controladora enquanto o dispositivo estiver um de (i) registrando e (ii) registrado com a segunda controladora e em que o dispositivo registra com a primeira e segunda controladoras ao executar registro SIP e processo de conexão de redes.

12. Dispositivo, de acordo com a reivindicação 11,

caracterizado pelo fato de o módulo de descoberta ser ainda operado para registrar simultaneamente com a primeira e a segunda controladoras.

13. Dispositivo, de acordo com a reivindicação 12,
5 **caracterizado** pelo fato de os atributos da primeira controladora serem diferentes dos atributos da segunda controladora.

14. Dispositivo, de acordo com a reivindicação 13,
10 **caracterizado** pelo fato de a primeira controladora fornecer extensões do Protocolo de Iniciação de Sessão (SIP) estendidas para o dispositivo de comunicação e em que a segunda controladora fornece extensões do Protocolo de Iniciação de Sessão (SIP) padrão para o dispositivo de comunicação.

15 15. Dispositivo, de acordo com a reivindicação 13,
caracterizado pelo fato de o dispositivo de comunicação ser registrado com a primeira e a segunda controladoras em uma de uma configuração ativa-ativa e uma configuração ativa-reserva, em que na configuração ativa-ativa o dispositivo
20 utiliza tanto a primeira como a segunda controladora para processar as chamadas de entrada e de saída, e em que na configuração ativa-reserva o dispositivo utiliza uma controladora selecionada como a controladora primária para processar as chamadas de entrada e de saída e solicitações
25 de que as chamadas de entrada recebidas de uma controladora secundária sejam redirecionadas através da controladora primária.

16. Dispositivo, de acordo com qualquer uma das reivindicações 9, 10, 11, 12, 13, 14 ou 15, **caracterizado**
30 pelo fato de o módulo de descoberta ser ainda operado para

gerar uma lista de controladoras que compreende pelo menos a primeira e a segunda controladoras, comparar informação de controladora para a primeira controladora com informação de controladora para a segunda controladora, e ordenar a
5 lista de controladoras com base na comparação da informação de controladora.

17. Meio lido por computador caracterizado pelo fato de compreender instruções executáveis por processador que são operadas, quando executadas, para efetuar as etapas do
10 método definido na reivindicação 1.

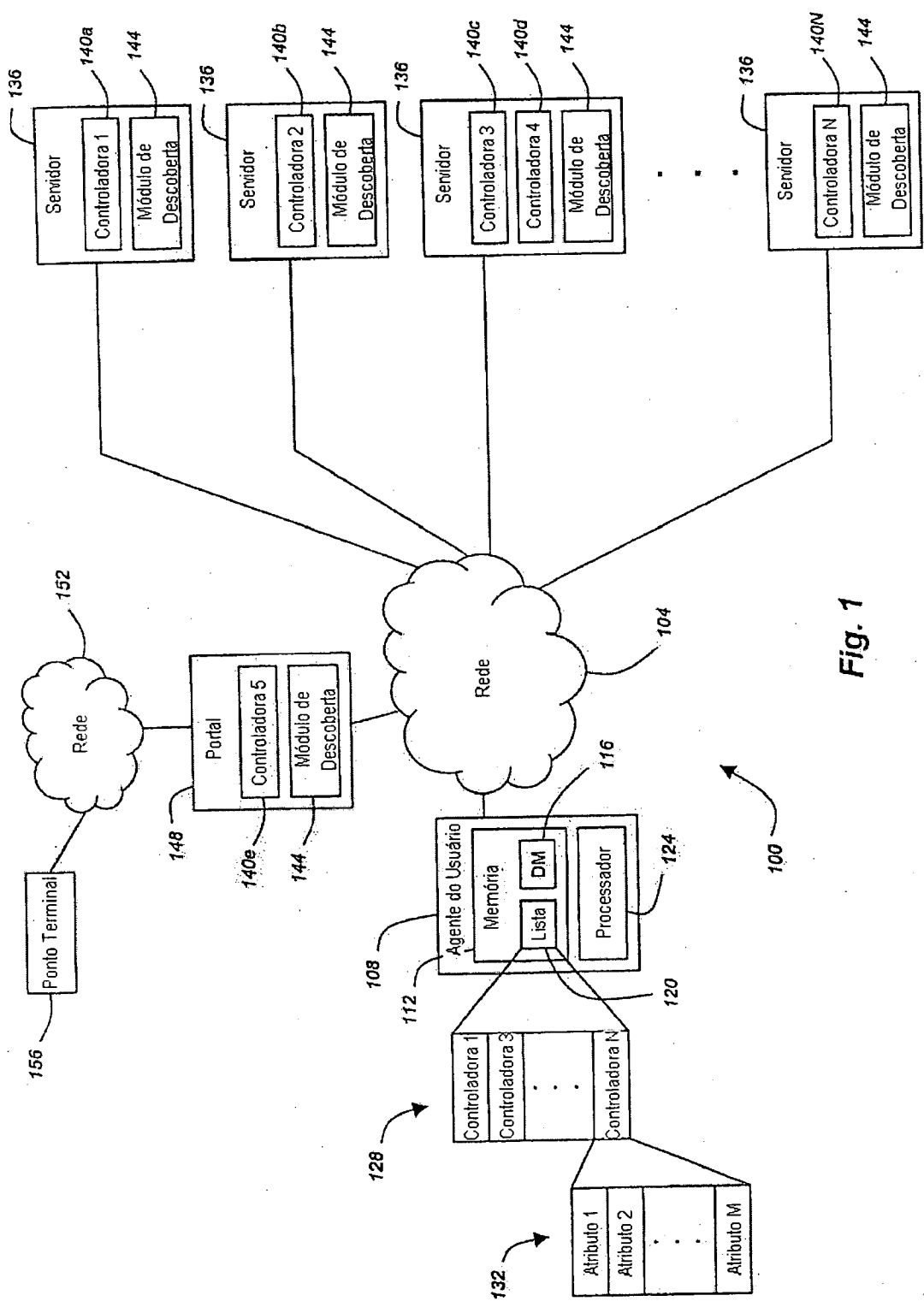


Fig. 1

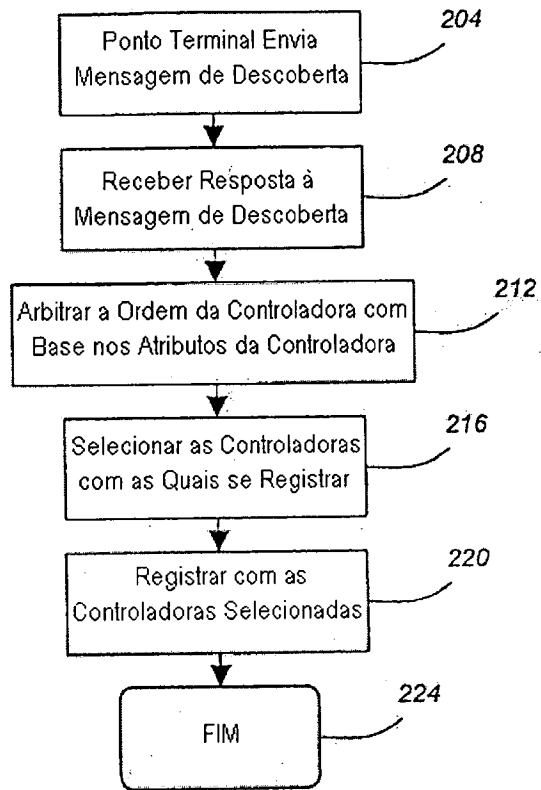


Fig. 2

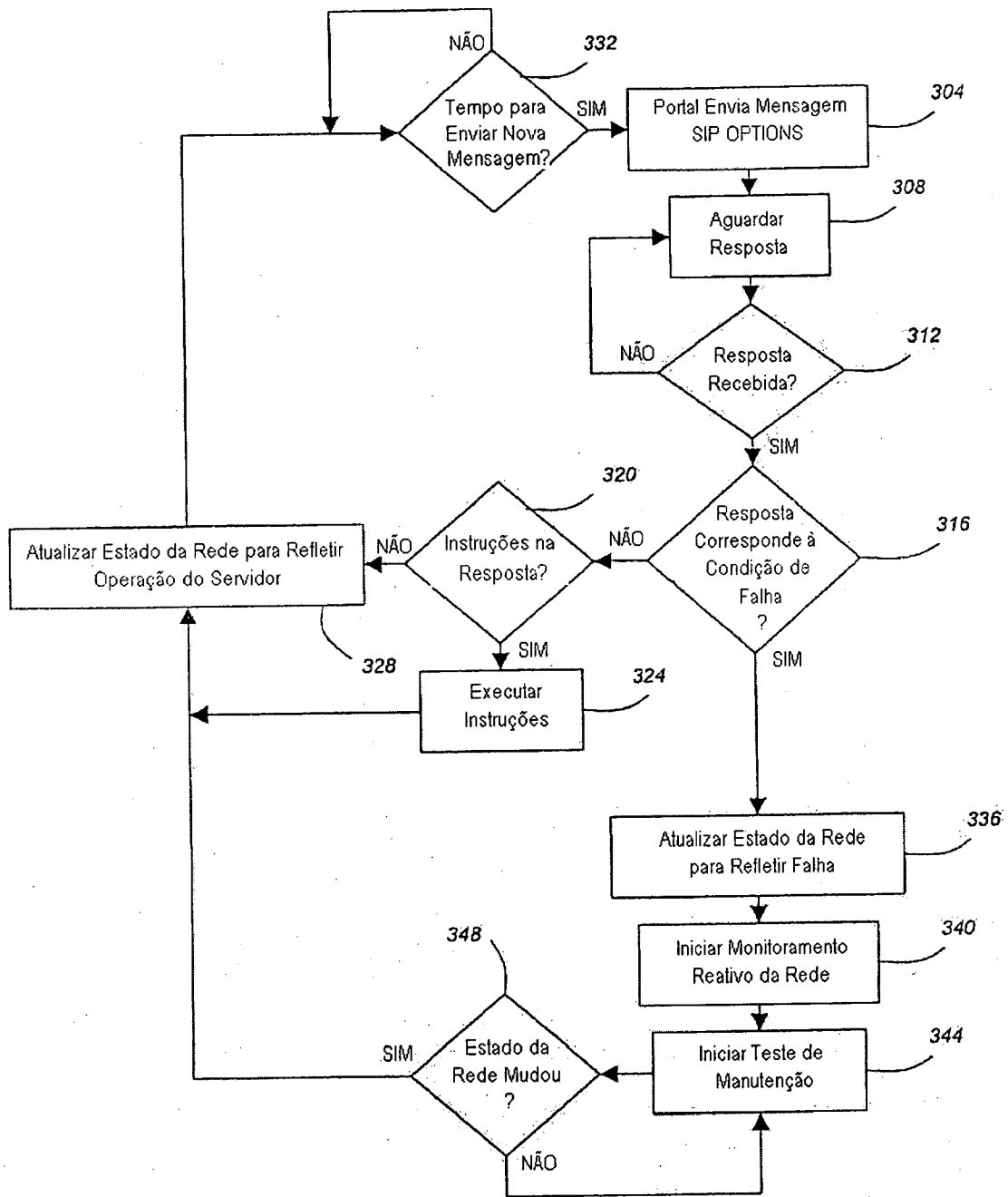
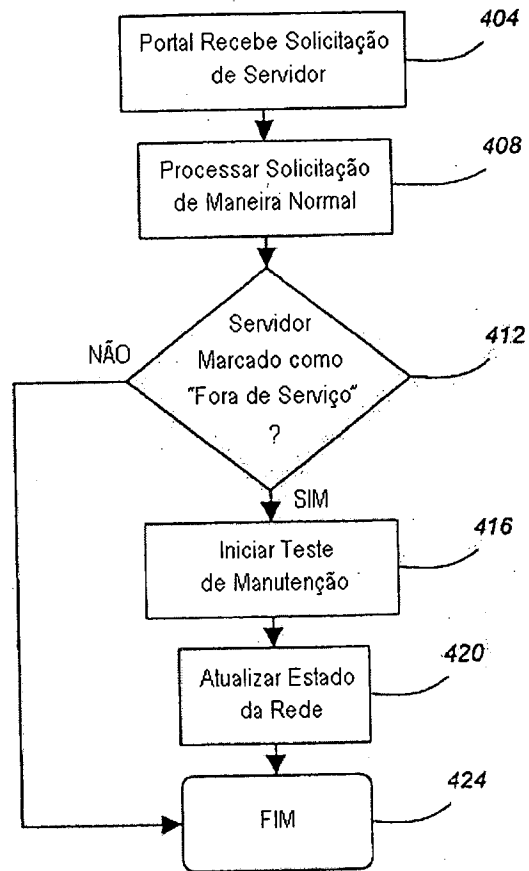


Fig. 3

**Fig. 4**

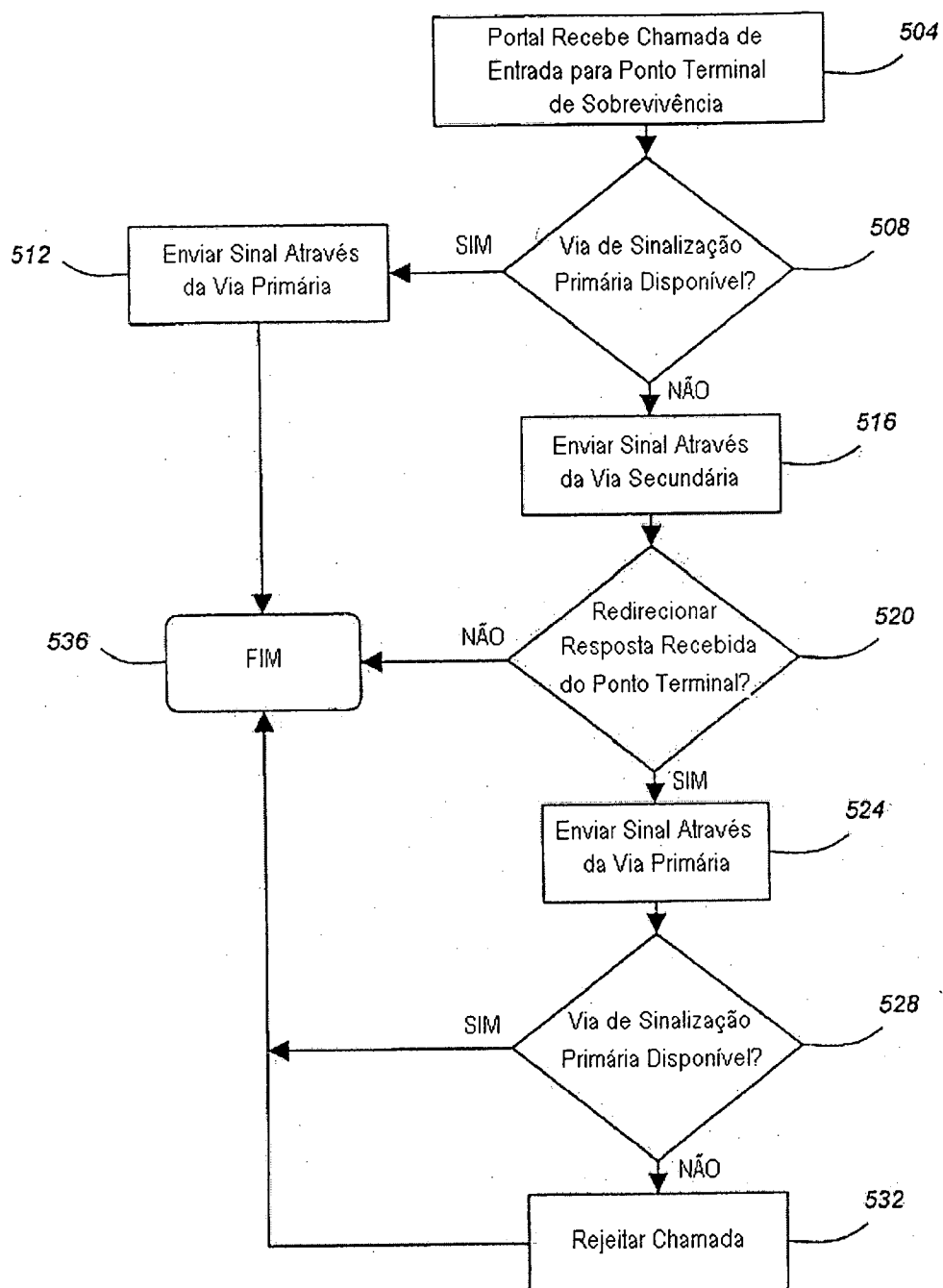


Fig. 5

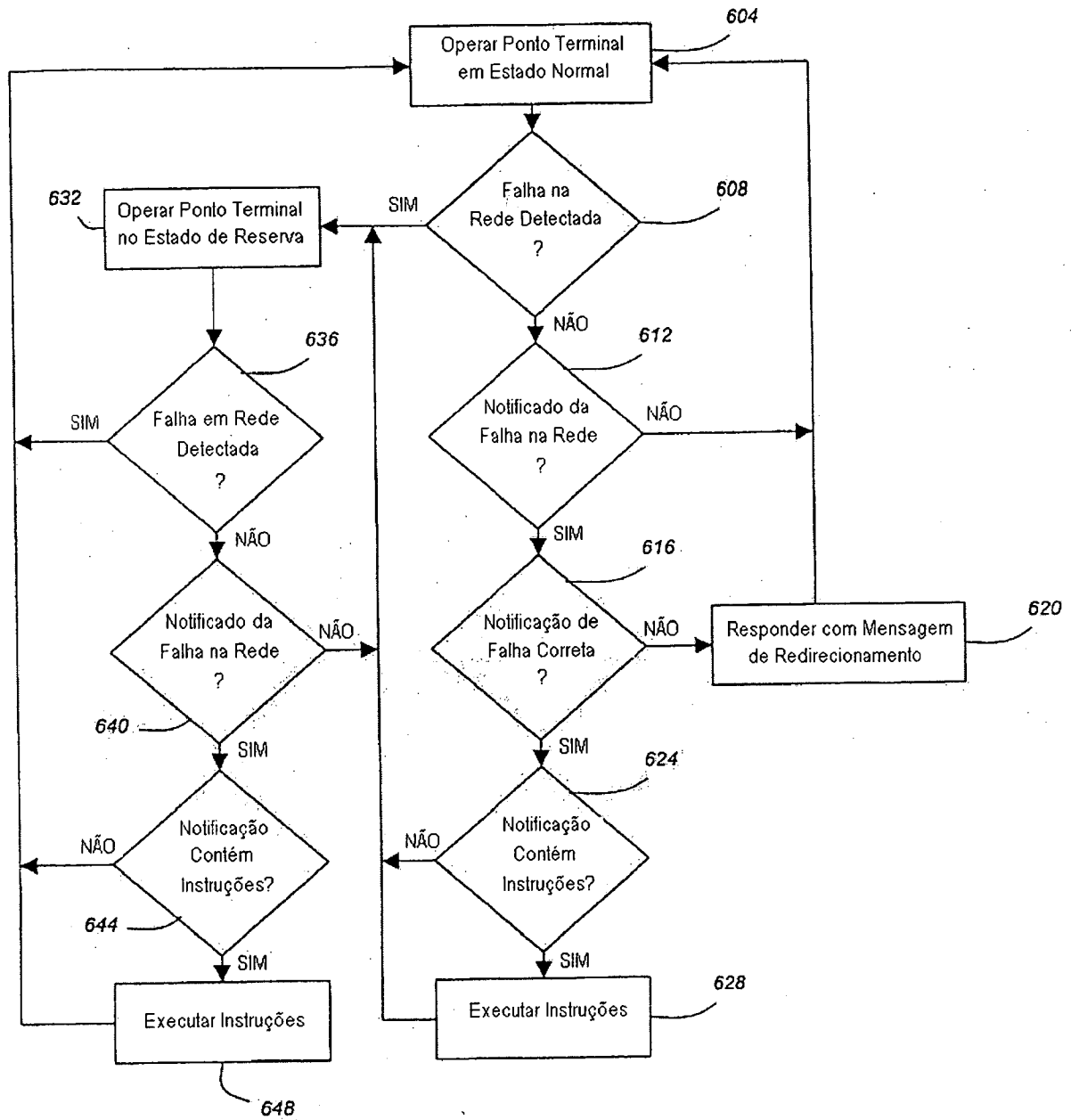
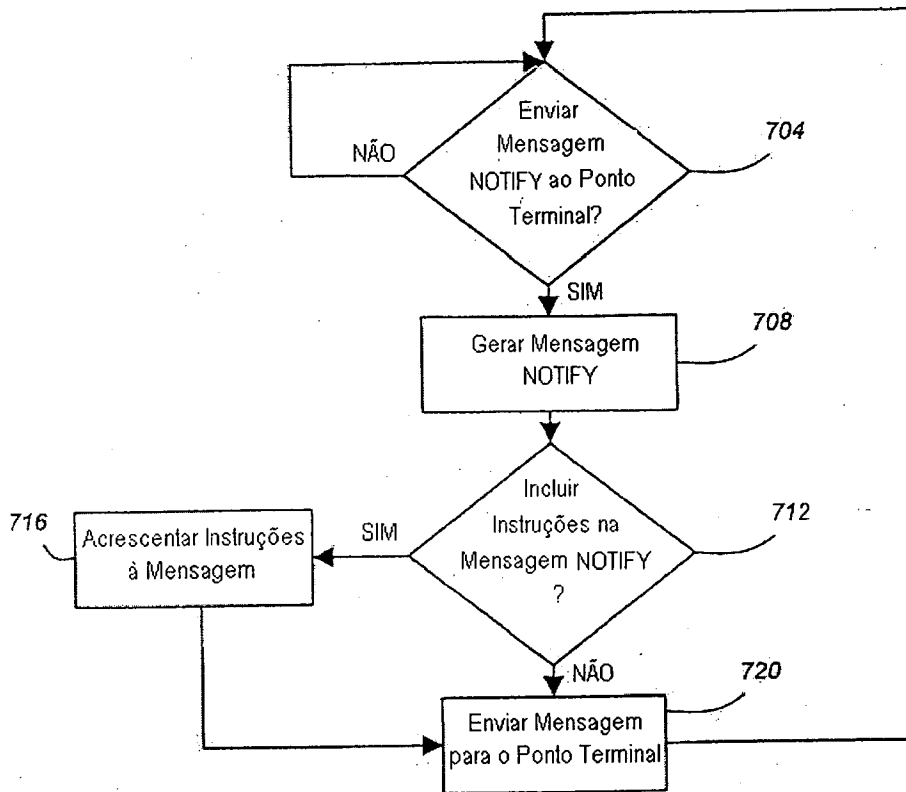


Fig. 6

**Fig. 7**