(11) Número de Publicação: **PT 1876754 E**

(51) Classificação Internacional:
H04L 12/24 (2011.01) ***H04L 29/12*** (2011.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2006.04.28**

(30) Prioridade(s): **2005.04.29 CN 200510069417**

(43) Data de publicação do pedido: **2008.01.09**

(45) Data e BPI da concessão: **2012.02.22 090/2012**

(73) Titular(es):
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI ADMINISTRATION BUILDING BANTIAN LONGGANG DISTRICT, SHENZHEN GUANGDONG 518129 **CN**

(72) Inventor(es):
JIAHONG WEI **CN**
JUN LI **CN**
WUMAO CHEN **CN**

(74) Mandatário:
MARIA SILVINA VIEIRA PEREIRA FERREIRA
RUA CASTILHO, N.º 50, 5º - ANDAR 1269-163 LISBOA **PT**

(54) Epígrafe: **MÉTODO, SISTEMA E SERVIDOR PARA REALIZAR ATRIBUIÇÃO SEGURA DE ENDEREÇO DHCP**

(57) Resumo:
SÃO DIVULGADOS UM MÉTODO, UM SISTEMA E UM SERVIDOR DE AUTENTICAÇÃO PARA REALIZAR UMA ATRIBUIÇÃO SEGURA DE UM ENDEREÇO DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) PROTOCOLO DE CONFIGURAÇÃO DINÂMICA DE ENDEREÇOS DE REDE. O MÉTODO INCLUI: ENVIAR UMA MENSAGEM DE DESCOBERTA DE DHCP ATRAVÉS DE UMA REDE DE ACESSO; OBTER A INFORMAÇÃO DE IDENTIFICAÇÃO DO DHCP CLIENTE E REALIZAR UMA AUTENTICAÇÃO AO DHCP CLIENTE COM BASE NA INFORMAÇÃO DE IDENTIFICAÇÃO; E APENAS ATRIBUIR O ENDEREÇO AO DHCP CLIENTE SE TIVER PASSADO A AUTENTICAÇÃO. POR CONSEGUINTE, NA PRESENTE INVENÇÃO, A AUTENTICAÇÃO DE ACESSO PODE SER REALIZADA NUM ASSINANTE DE ACORDO COM A INFORMAÇÃO DE LOCALIZAÇÃO, E O ENDEREÇO IP (PROTOCOLO DE INTERNET) APENAS É ATRIBUÍDO AO ASSINANTE E TERMINAL VÁLIDOS. POR CONSEGUINTE, A SEGURANÇA DA ATRIBUIÇÃO DE ENDEREÇO EM MODO DHCP PODE SER GRANDEMENTE MELHORADA. PARA ALÉM DISSO, NA PRESENTE INVENÇÃO, OS ENDEREÇOS PODEM SER GERIDOS DE FORMA CONJUNTA POR UM SERVIDOR AAA, OU OS ENDEREÇOS PODEM SER ATRIBUÍDOS APÓS TEREM SIDO AUTENTICADOS COM SUCESSO PELO SERVIDOR AAA.

RESUMO

"MÉTODO, SISTEMA E SERVIDOR PARA REALIZAR ATRIBUIÇÃO SEGURA DE ENDEREÇO DHCP"

São divulgados um método, um sistema e um servidor de autenticação para realizar uma atribuição segura de um endereço DHCP (Dynamic Host Configuration Protocol) Protocolo de Configuração Dinâmica de Endereços de Rede. O método inclui: enviar uma mensagem de descoberta de DHCP através de uma rede de acesso; obter a informação de identificação do DHCP cliente e realizar uma autenticação ao DHCP cliente com base na informação de identificação; e apenas atribuir o endereço ao DHCP cliente se tiver passado a autenticação. Por conseguinte, na presente invenção, a autenticação de acesso pode ser realizada num assinante de acordo com a informação de localização, e o endereço IP (Protocolo de Internet) apenas é atribuído ao assinante e terminal válidos. Por conseguinte, a segurança da atribuição de endereço em modo DHCP pode ser grandemente melhorada. Para além disso, na presente invenção, os endereços podem ser geridos de forma conjunta por um servidor AAA, ou os endereços podem ser atribuídos após terem sido autenticados com sucesso pelo servidor AAA.

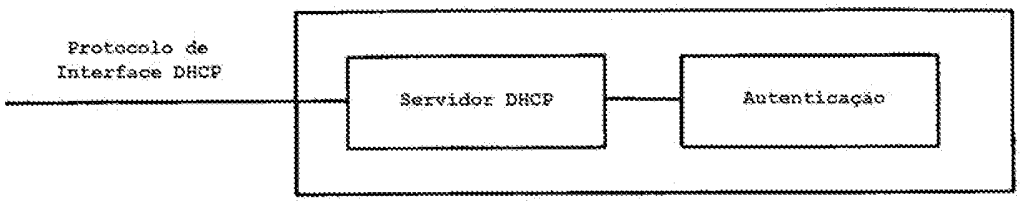


Fig. 3

DESCRIÇÃO

"MÉTODO, SISTEMA E SERVIDOR PARA REALIZAR ATRIBUIÇÃO SEGURA DE ENDEREÇO DHCP"

Campo da invenção

A presente invenção está relacionada com o campo técnico das redes de comunicações, em particular, com um método, um sistema e um servidor para realizar uma atribuição segura de um Protocolo de Configuração Dinâmica de Endereços de Rede (DHCP).

Antecedentes da Invenção

À medida que as tecnologias de acesso como sejam ADSL (Linha de Assinante Digital Assimétrica), a Ethernet torna-se mais e mais consolidada, o acesso de banda larga torna-se mais e mais popular; e os serviços desenvolvidos de IPTV (Televisão sobre Protocolo de Internet) vídeo e VoIP (Voz sobre Protocolo de Internet) baseados em acesso de rede em banda larga são cada vez mais abundantes. O desenvolvimento de cada serviço necessita de empregar um terminal dedicado; por exemplo, o serviço de vídeo necessita de utilizar STB (Set Top Box - Conversor para Televisão), o serviço de voz necessita de utilizar IAD (Dispositivo de Acesso Integrado). Cada terminal dedicado necessita de obter um endereço local antes de um serviço ser executado, e então cada serviço pode ser executado utilizando o endereço local.

Numa rede de comunicações, cada terminal obtém usualmente um endereço IP (Protocolo de Internet) baseado no protocolo DHCP. No entanto, num serviço tradicional online, é usualmente empregue PPPoE (Protocolo sobre Ethernet Ponto a Ponto), e é necessário um servidor AAA (Autenticação,

Autorização e Auditoria) para autenticar um acesso de assinante e atribuir o endereço IP. Usualmente, o servidor AAA pode ser um servidor RADIUS (Autenticação Remota da Ligação do Utilizador ao Servidor) ou outro servidor de autenticação.

A Figura 1 mostra uma estrutura de um sistema de rede de comunicação no qual é realizada uma autenticação por um servidor RADIUS e o endereço IP é obtido através de um servidor DHCP.

Um servidor DHCP é um servidor para gerir endereços IP e está adaptado para responder a um pedido de atribuição de endereço a partir de um computador e atribuir um endereço IP apropriado ao computador.

O cliente DHCP é um terminal adaptado para obter parâmetros de rede como seja o endereço IP utilizando o protocolo DHCP, incluindo o computador, STB e IAD.

O servidor RADIUS está adaptado para gerir a conta e a palavra passe de um assinante e realizar uma autenticação de um acesso de um assinante.

O BRAS (Servidor de Acesso Remoto de Banda Larga) está adaptado para gerir o acesso de um assinante de banda larga; para um assinante de PPPoE, o BRAS atua como um cliente RADIUS e inicia um pedido de autenticação ao servidor RADIUS; e para um assinante DHCP, o BRAS implementa a função de transmissão do DHCP.

A rede de acesso é uma rede intermédia entre a casa do assinante e o BRAS.

O nó de acesso é um dispositivo que liga diretamente à linha do assinante numa rede de acesso, como seja o dispositivo ADSL de acesso DSLAM (Multiplexador de Acesso DSL).

O OSS (Sistema de Suporte de Operações) é um sistema para o operador libertar e gerir um serviço.

Na Figura 1, a um cliente DHCP como seja STB e IAD pode ser atribuído um endereço IP correspondente utilizando o protocolo DHCP através de um servidor DHCP disposto na rede.

O processo específico no qual cada cliente DHCP da Figura 1 obtém o endereço é mostrado na Figura 2, incluindo os passos seguintes.

Passo 21: Um cliente DHCP liga-se, envia uma mensagem de descoberta de DHCP para procurar um servidor capaz de fornecer o serviço DHCP.

Passo 22: Como uma transmissão DHCP, um BRAS transmite a mensagem de descoberta de DHCP ao servidor DHCP designado.

Passo 23: O servidor DHCP devolve uma mensagem de oferta para indicar que o servidor DHCP é capaz de atribuir um endereço IP ao cliente.

Passo 24: O cliente DHCP envia uma mensagem de Pedido DHCP e o BRAS transmite a mensagem de pedido DHCP para o servidor DHCP.

Passo 25: O servidor DHCP atribui um endereço IP apropriado e devolve uma mensagem de Resposta DHCP.

Por conseguinte, o cliente DHCP pode obter o endereço IP, e assim ter acesso à rede e obter o obter o serviço de rede.

Pode ver-se a partir do processo de atribuição de endereço DHCP acima que: durante o processo no qual o cliente DHCP obtém o endereço IP num modo DHCP, um assinante inválido pode facilmente obter o endereço IP correspondente e assim obter o serviço de rede. Por conseguinte, o problema de um pirata informático utilizar os recursos de endereço IP e atacar uma rede é fácil de ocorrer. Além disso, após o pirata informático atacar a rede, ele não pode ser rastreado.

Adicionalmente, o operador necessita de usar um servidor DHCP para gerir o endereço IP do utilizador do cliente DHCP e usar um servidor RADIUS para gerir o endereço IP do utilizador do cliente PPPoE. Em resultado disso, existem dois conjuntos de mecanismos de gestão de recursos de endereços IP, os dados estão descentralizados, e o custo de gestão é elevado.

Para além disso, o documento WO 99/16266 A divulga os seguintes conteúdos. Aplicações a correr numa estação móvel ou uma entidade de rede externa como seja um fornecedor de serviços internet pode especificar numa base de fluxo de aplicação individual uma qualidade de serviço pedida. A partir dessa qualidade de serviço pedida, é determinado um tipo ótimo de portadora para transferir o fluxo de aplicação através da rede de comunicações móveis. Por exemplo, pode ser alocada uma portadora por comutação de pacotes se o pedido for para um serviço que não seja do tipo em tempo real. Podem ser empregues vários outros critérios de tomada de decisão. Uma estação móvel e um nó

de porta de ligação de uma rede móvel incluem cada uma um mapeador para mapear um fluxo de aplicação individual para uma portadora de uma rede por comutação de circuitos e uma portadora de rede por comutação de pacotes dependendo da qualidade de serviço pedida para o fluxo de aplicação individual. Os parâmetros da qualidade de serviço da camada de rede correspondentes a um fluxo de aplicação individual são mapeados para parâmetros de portadora por comutação de circuitos se o fluxo de aplicação estiver mapeado para a rede por comutação de circuitos e para parâmetros de portadora por comutação de pacotes se o fluxo de aplicação estiver mapeado para a rede por comutação de circuitos. O nó da porta de ligação inclui um servidor de acesso comum o qual permite que uma estação móvel estabeleça inicialmente uma sessão de comunicações com uma entidade exterior à rede para realizar apenas um único procedimento de acesso comum para comunicações subsequentes utilizando uma das redes por comutação de circuitos e por comutação de pacotes. Após esse procedimento de acesso comum ter sido completado, fluxos de aplicação subsequentes entre a estação móvel e a entidade exterior à rede são estabelecidos utilizando procedimentos abreviados sem ter que aceder à entidade exterior à rede.

Além disso, a NORMA IETF “DHCP Relay Agent Information Option; rfc 3046.txt” divulga conteúdos técnicos relacionados com o agente de transmissão.

Além disso, um pedido de patente (WO/2004/006503) fornece um arranjo e um método com configuração dinâmica de porta de equipamento de rede para comunicação numa rede de banda larga. Uma gestão de base de dados centralizada em ligação com um servidor com um Protocolo de Configuração Dinâmica de Endereços de Rede está a guardar matrizes com gravações

de parâmetros de equipamento de rede para as configurações dos seus portos físicos e serviços desdobrados. Por conseguinte, permitir a atualização dinâmica das configurações dos portos através da transmissão das matrizes com gravações de parâmetros a partir do servidor de Protocolo de Configuração Dinâmica de Endereços de Rede. As configurações dos parâmetros são atualizadas no dispositivo intermédio. No entanto, na solução técnica de D3, visto a base de dados estar localizada fora do servidor DHCP, o custo da gestão dos dados é elevado e a segurança da transmissão dos dados é baixa.

Sumário da Invenção

Tendo em vista os problemas acima no estado da técnica, um objetivo da presente invenção é fornecer um método, um sistema e um servidor para realizar uma atribuição segura de um endereço DHCP. E por conseguinte a segurança do processo de atribuição de endereço do servidor DHCP pode ser efetivamente garantida e o custo da gestão de dados é baixo.

O objetivo da presente invenção é realizado pelas seguintes soluções técnicas.

Um método para realizar uma atribuição segura de um endereço DHCP, compreendendo:

receber, através de um servidor de acesso, uma mensagem de Descoberta de DHCP;

inserir, através do servidor de acesso, informação de localização do cliente DHCP na mensagem de Descoberta de DHCP;

enviar, através do servidor de acesso, a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP para um servidor de autenticação DHCP;

receber, através do servidor de autenticação DHCP, a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP, em que o servidor de autenticação DHCP é um servidor DHCP tendo uma função de autenticação localmente configurada, o servidor de autenticação DHCP compreende uma base de dados local compreendendo informação de identificação guardada localmente para um assinante válido;
realizar uma autenticação do cliente DHCP com base na informação de localização e na informação de identificação guardada localmente para o assinante válido através do servidor de autenticação DHCP; e
enviar, através do servidor de autenticação DHCP, uma mensagem DHCP com informação de endereço que está atribuído ao cliente DHCP cuja autenticação foi validada através do servidor de acesso, após a autenticação do cliente DHCP ter sido validada.

Um servidor de autenticação DHCP para realizar uma atribuição segura de um endereço DHCP, tendo o servidor de autenticação uma função de autenticação configurada localmente, e compreendendo um módulo de processamento de autenticação, um servidor DHCP para atribuir um endereço IP a um cliente DHCP que solicita um endereço IP, e uma base de dados local compreendendo informação de identificação guardada para um assinante válido localmente, em que:
o módulo de processamento de autenticação está adaptado para obter informação de localização de um cliente iniciando um processo DHCP, realizar uma validação de autenticação do cliente de acordo com a informação de localização e a informação de identificação guardada para o assinante válido, e enviar uma mensagem de Descoberta de DHCP de um cliente DHCP cuja autenticação foi validada pelo servidor DHCP; e

o servidor DHCP está adaptado para receber a mensagem de Descoberta de DHCP enviada através do módulo de processamento de autenticação e enviar uma mensagem de Oferta de DHCP ao cliente DHCP, e atribuir um endereço IP a um cliente DHCP correspondente numa lista de endereços do servidor DHCP quando o cliente DHCP envia uma mensagem de pedido DHCP.

Um sistema para realizar uma atribuição segura de um endereço DHCP, compreendendo um servidor de acesso e um servidor de autenticação DHCP; em que
o servidor de acesso está adaptado para receber a mensagem de Descoberta de DHCP enviada a partir do cliente DHCP, inserir a informação de localização do cliente DHCP na mensagem de Descoberta de DHCP e enviar a mensagem de Descoberta de DHCP com a informação de localização para o servidor de autenticação DHCP; e
o servidor de autenticação DHCP tem uma função de autenticação configurada localmente, e está adaptado para receber a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP e realizar uma autenticação do cliente DHCP baseada na informação de localização e na informação de identificação guardada para um assinante válido localmente; e enviar uma mensagem DHCP com informação de endereço que seja atribuída ao cliente DHCP que validou a autenticação através do servidor de acesso.

Além disso, na presente invenção, os endereços podem ser geridos unicamente por um servidor RADIUS, por outras palavras, o servidor DHCP e o servidor RADIUS em conjunto gerem os endereços IP, embora o custo da gestão da rede possa ser reduzido. Para além disso, as medidas de segurança originais do servidor RADIUS podem ser usadas para controlar o número de endereços IP a serem obtidos por

um subscritor, para que a utilização de endereços maliciosos para ataque possa ser efetivamente evitada. Mesmo se o ataque à rede ou outros problemas de segurança na rede ocorrerem, a localização física do assinante pode ser rastreada de acordo com o endereço IP, para que deste modo um pirara possa ser efetivamente desencorajado de realizar uma atividade de ataque.

A presente invenção tem boa compatibilidade, por outras palavras, durante a implementação da presente invenção não é adicionado nenhum interface e comando extra ao sistema OSS, e o processo de gestão de serviço no utilizador do cliente DHCP é consistente com o lançamento do serviço original do processo de gestão no cliente PPPoE. Em resultado disso, o investimento do operador pode estar protegido.

Breve Descrição dos Desenhos

A Figura 1 é uma representação estrutural de um sistema de acesso de banda larga;

A Figura 2 é um diagrama esquemático mostrando um processo no qual um servidor DHCP obtém um endereço;

A Figura 3 é uma representação estrutural do servidor de autenticação DHCP de acordo com a presente invenção;

A Figura 4 é um outro sistema de representação estrutural de acordo com a presente invenção; e

A Figura 5 é um diagrama esquemático de um processo de atribuição de endereços DHCP baseado no sistema mostrado na Figura 4.

Descrição Detalhada das Formas de Realização

O conceito principal da presente invenção assenta em: durante o processo no qual um cliente DHCP obtém um endereço a partir de um servidor, é adicionado um processo de autenticação de validação no cliente DHCP, para que um assinante inválido possa ser impedido de atacar o servidor DHCP. Para além disso, com base no conceito acima, a gestão de endereços do servidor DHCP e o servidor de autenticação podem ser juntos, sendo deste modo fácil de executar a gestão de endereços. O servidor de autenticação inclui um servidor AAA como seja um servidor RADIUS. Opcionalmente, o servidor de autenticação podem ser outros servidores de autenticação com a função idêntica.

Uma forma de realização da presente invenção fornece um método para realizar uma atribuição segura de um endereço DHCP, incluindo principalmente o seguinte.

(1) Um cliente DHCP envia uma mensagem de Descoberta de DHCP através de uma rede de acesso.

(2) O servidor de acesso do lado da rede (como seja BRAS e nó de acesso) determina a informação de identificação do cliente DHCP, como seja o número da porta, VPI (Identificadores de caminho virtuais)/VCI (Identificadores de canal Virtuais) e VLAN ID (ID de Rede de Área Local Virtual), de acordo com a porta de ingresso de informação da mensagem de Descoberta de DHCP, e realiza uma autenticação do cliente DHCP com base na informação de identificação do cliente DHCP e da informação de identificação pré configurada para um assinante válido.

(3) A mensagem de Descoberta de DHCP do cliente DHCP tendo sido validada pela autenticação é enviada para o servidor

DHCP, e o endereço é atribuído ao cliente DHCP através do servidor DHCP. O processo específico de atribuição de endereço é o mesmo que um processo de atribuição de endereço convencional, e o processo de descrição do mesmo está omitido.

Além disso, um servidor DHCP correspondente com uma função de autenticação pode ser configurado na rede, para que o servidor DHCP possa realizar primeiro um processo de autenticação depois de receber uma mensagem de Descoberta de DHCP enviada a partir de um cliente DHCP, e o endereço correspondente apenas será atribuído após a autenticação ter sido validada.

A presente invenção fornece um servidor de autenticação DHCP com a função de autenticação. Descrições do servidor de autenticação DHCP serão agora ilustradas em conjunto com os desenhos respetivamente.

Para o servidor de autenticação DHCP com a função de autenticação, a função de autenticação está configurada e implementada localmente. A estrutura específica do servidor de autenticação DHCP é como se mostra na Figura 3, incluindo um módulo de processamento de autenticação e um módulo de servidor DHCP.

O módulo de processamento de autenticação está adaptado para obter a informação de identificação do cliente DHCP durante a inicialização do processo DHCP, realizar uma validação de autenticação do cliente de acordo com a informação de identificação guardada para assinantes válidos, e então enviar um resultado de autenticação para o módulo servidor DHCP, em que a informação de identificação

do subscritor válido é gravada num módulo de armazenamento correspondente (não mostrado).

O módulo servidor DHCP está adaptado para obter o resultado da autenticação no cliente DHCP do módulo de processamento da autenticação, enviar uma mensagem de Oferta DHCP ao cliente DHCP com o resultado de autenticação de VALIDADO para indicar que o servidor DHCP pode atribuir um endereço IP correspondente ao cliente DHCP após o cliente DHCP ter enviado uma mensagem de pedido DHCP. Deste modo, a função do servidor DHCP é implementada.

Neste ponto, o servidor de autenticação DHCP opera num modo servidor, corresponde a um servidor com uma função de autenticação segura, e pode implementar a autenticação e a atribuição de endereço para um cliente de forma independente.

O servidor de autenticação DHCP acima com a função de autenticação pode ser configurado em qualquer rede que necessite de um servidor para realizar a função correspondente de atribuição de endereço.

A presente invenção fornece um sistema correspondente com uma atribuição de endereço DHCP e uma função de autenticação para realizar uma atribuição segura de um endereço DHCP. A estrutura do sistema é mostrada na Figura 4, incluindo especificamente um cliente DHCP, uma rede de acesso e um servidor de autenticação DHCP. O servidor de autenticação DHCP está adaptado para realizar uma validação de autenticação de uma mensagem de Descoberta DHCP do cliente DHCP obtida através do acesso à rede, e realizar uma atribuição de endereço ao cliente DHCP cuja autenticação foi validada.

No sistema de acordo com a presente invenção, o servidor de autenticação DHCP pode realizar a autenticação do cliente DHCP e atribuir um endereço IP correspondente da seguinte forma.

Conforme mostrado na Figura 5, a validação da autenticação é realizada sobre a informação de identificação do cliente DHCP de acordo com a informação de identificação do assinante válido guardada localmente, e o servidor DHCP pode atribuir o endereço IP correspondente ao cliente DHCP cuja autenticação foi validada.

Especificamente, no sistema, o nó de acesso e o BRAS suportam a captura de uma mensagem DHCP e inserem uma opção Opção82 na mensagem DHCP, para que o servidor de autenticação possa obter a informação de identificação correspondente do cliente DHCP após receber a mensagem DHCP. Na opção Opção82 na mensagem DHCP, é identificada informação local do assinante, atuando como sendo a informação de identificação. Especificamente, a informação de localização do assinante inclui informação da porta, informação VPI/VCI e VLAND ID.A opção Opção82 pode ser inserida na mensagem DHCP no BRAS.

A presente invenção fornece ainda um método correspondente para realizar uma atribuição segura de um endereço DHCP baseado no sistema acima. Uma descrição detalhada será agora ilustrada abaixo.

Por exemplo, o método é descrito no caso em que o servidor de autenticação DHCP opera num modo de servidor, conforme mostrado na Figura 4 e Figura 5.

Passo 91: Quando um assinante abre uma conta, o operador adiciona uns dados a um servidor de autenticação DHCP e grava a informação de localização de assinante, o modo de codificação é consistente com a opção Opção82 inserida através do nó de acesso ou do BRAS, e do endereço MAC de um terminal (STB, IAD) pode ser gravada seletivamente.

Passo 92: Quando um cliente DHCP necessita de obter o endereço IP, o cliente DHCP necessita de enviar uma mensagem de Descoberta DHCP do cliente DHCP para o BRAS.

Passo 93: Como um transmissor DHCP, o BRAS captura a mensagem DHCP e insere a opção Opção82 na mensagem, e então envia a mensagem de Descoberta DHCP transportando a informação de localização para o servidor de autenticação DHCP. A informação de localização de assinante, como seja informação da porta, VPI/VCI e VLAN ID, é identificada na opção Opção82.

O servidor de autenticação DHCP recebe a mensagem transmitida pelo BRAS, extrai a opção Opção82 e o endereço MAC do terminal como a informação de identificação, pesquisa uma base de dados local, e realiza uma autenticação da informação de identificação do cliente DHCP de acordo com a informação de identificação gravada localmente para um assinante válido. Se a autenticação for validada, o servidor de autenticação devolve uma mensagem de Oferta DHCP ao cliente DHCP, conforme descrito no Passo 94.

Passo 94: O servidor de autenticação DHCP envia uma mensagem de Oferta DHCP para o cliente DHCP.

Passo 95: Após ter recebido a mensagem de Oferta DHCP, o cliente DHCP envia uma mensagem de pedido para o servidor de autenticação DHCP.

Passo 96: O servidor de autenticação DHCP atribui o endereço IP cliente, e envia o endereço IP para o cliente DHCP através de uma mensagem de Resposta DHCP.

De forma similar, conforme descrito no passo 93 da Figura 5, o BRAS insere a opção Opção82. Na prática, a opção Opção82 pode também ser inserido através de um nó de acesso como DSLAM, enquanto o BRAS apenas atua como o transmissor DHCP. Outros processos são os mesmos que aqueles acima descritos.

Em conclusão, a presente invenção pode melhorar grandemente a segurança da atribuição de endereços no modo DHCP, e pode realizar uma autenticação de acesso de um assinante de acordo com informação de localização, e pode apenas atribuir um endereço IP a um assinante válido ou um terminal válido. Por conseguinte, o ataque de endereços maliciosos pode ser efetivamente evitado. Além disso, quando o ataque de rede ou outros problemas de segurança de rede ocorrem, a localização física do assinante pode ser rastreada de acordo com o endereço IP, para que um pirata possa ser efetivamente desencorajado de levar a cabo um ataque.

Vantagens e modificações adicionais ocorrerão prontamente àqueles que sejam qualificados na técnica. Por conseguinte, a presente invenção nos seus aspetos mais amplos não está limitada aos detalhes específicos e formas de realização representativas aqui mostradas e descritas. Consequentemente, várias modificações e variações podem ser

feitas sem se afastar do âmbito da presente invenção conforme definido através das reivindicações juntas e dos seus equivalentes.

Lisboa, 26 de Abril de 2012

REIVINDICAÇÕES

1. Um método para realizar uma atribuição segura de um endereço DHCP, compreendendo:

receber, através de um servidor de acesso, uma mensagem de Descoberta de DHCP (91);

inserir, através de um servidor de acesso, informação de localização do cliente DHCP na mensagem de Descoberta de DHCP (93);

enviar, através do servidor de acesso, a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP para um servidor de autenticação DHCP (93);

receber, através do servidor de autenticação DHCP, a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP (93),

caracterizado por:

o servidor de autenticação DHCP ser um servidor DHCP tendo uma função de autenticação configurada localmente;

o servidor de autenticação DHCP compreende uma base de dados local compreendendo informação de identificação guardada para um assinante válido localmente;

em que o método compreende ainda:

realizar, através do servidor de autenticação DHCP, uma autenticação do cliente DHCP com base na informação de localização e na informação de identificação guardada para o assinante válido localmente; e

enviar, através do servidor de autenticação DHCP, uma mensagem DHCP com informação de endereço que está atribuída ao cliente DHCP cuja autenticação foi validada através do servidor de acesso, após a autenticação do cliente DHCP ter sido validada (96).

2. O método para realizar a atribuição segura do endereço DHCP de acordo com a reivindicação 1, em que, a informação de localização compreende:

um número de porta, um número de circuito e um número de ligação do cliente DHCP.

3. O método para realizar a atribuição segura do endereço DHCP de acordo com a reivindicação 1 ou 2, em que, receber a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP através do servidor de autenticação e realizar a autenticação do cliente DHCP com base na informação de localização e na informação de identificação guardada para o assinante válido localmente através do servidor de autenticação compreende:

receber, através do servidor de autenticação DHCP, a mensagem de descoberta de DHCP com a informação de localização do cliente DHCP e realizar uma validação de autenticação do cliente DHCP de acordo com a informação de localização e com a informação de identificação guardada para o assinante válido localmente.

4. O método para realizar a atribuição segura do endereço DHCP de acordo com a reivindicação 3, compreendendo ainda:

atribuir, através de um servidor de autenticação DHCP, a informação de endereço ao cliente DHCP cuja autenticação foi validada após receber informação de autenticação válida.

5. Um servidor de autenticação DHCP para realizar uma atribuição segura de um endereço DHCP, compreendendo um servidor DHCP para atribuir um endereço IP a um cliente DHCP que solicita um endereço IP, caracterizado por:

O servidor de autenticação DHCP ter uma função de autenticação configurada localmente, e o servidor de

autenticação compreender ainda: um módulo de processamento de autenticação, e uma base de dados local compreendendo informação de identificação guardada para um assinante válido, em que:

o módulo de processamento de autenticação está adaptado para obter informação de localização de um cliente iniciando um processo de DHCP, realizar uma validação de autenticação do cliente de acordo com a informação de localização e a informação de identificação guardada para o assinante válido, e enviar uma mensagem de Descoberta de DHCP de um cliente DHCP cuja autenticação foi validada através do servidor DHCP; e

o servidor DHCP está adaptado para receber a mensagem de Descoberta de DHCP enviada pelo módulo de processamento de autenticação e enviar uma mensagem de Oferta ao cliente DHCP, e atribuir um endereço IP a um cliente DHCP correspondente numa lista de endereços do servidor DHCP quando o cliente DHCP envia uma mensagem de pedido DHCP.

6. O servidor de autenticação DHCP de acordo com a reivindicação 5, em que, a informação de localização compreende:

um número de porta, um número de circuito e um número de ligação do cliente DHCP.

7. Um sistema para realizar uma atribuição segura de um endereço DHCP, compreendendo um servidor de acesso e um servidor de autenticação DHCP; em que

o servidor de acesso está adaptado para receber a mensagem de Descoberta de DHCP enviada a partir do cliente DHCP, inserir a informação de localização do cliente DHCP na mensagem de Descoberta de DHCP e enviar

a mensagem de Descoberta de DHCP com a informação de localização para o servidor de autenticação DHCP;

caracterizado por:

o servidor de autenticação DHCP tem uma função de autenticação configurada localmente, e está adaptado para receber a mensagem de Descoberta de DHCP com a informação de localização do cliente DHCP e realizar uma autenticação do cliente DHCP baseada na informação de localização e na informação de identificação guardada para um assinante válido localmente; e enviar uma mensagem DHCP com informação de endereço que seja atribuída ao cliente DHCP que validou a autenticação através do servidor de acesso.

8. O sistema de acordo com a reivindicação 7, em que, o servidor de autenticação é o servidor de autenticação conforme descrito na reivindicação 5.

Lisboa, 26 de Abril de 2012

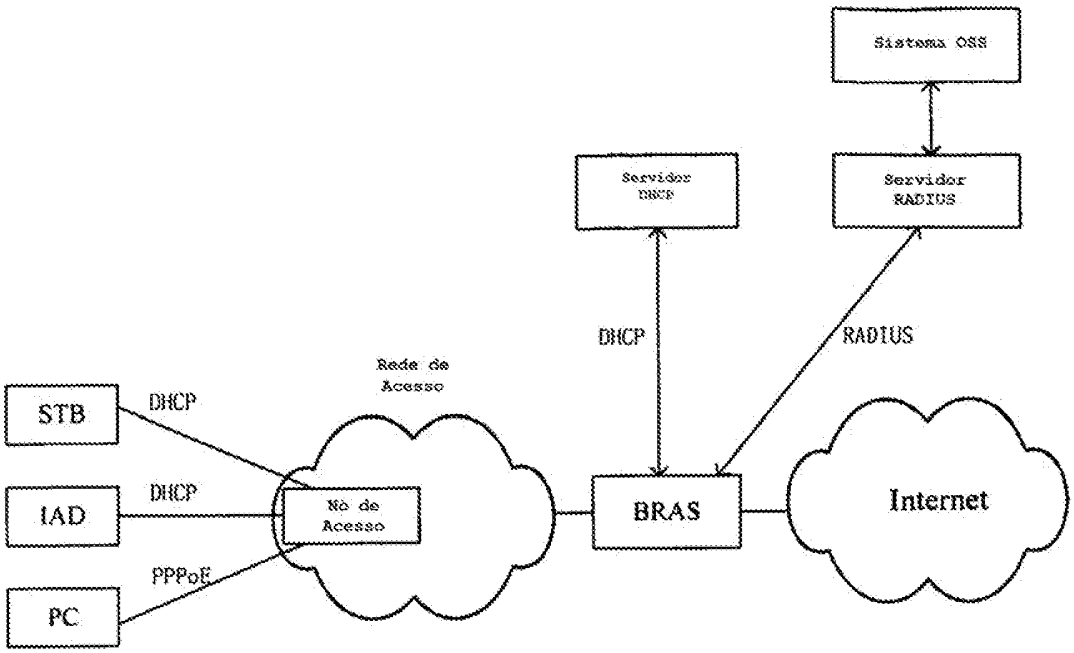

Sistema OSS
Servidor DHCP
Servidor RADIUS
DHCP
RADIUS
Rede de Acesso
STB
DHCP
IAD
DHCP
PC
PPPoE
Nó de Acesso
BRAS
Internet

Fig. 1

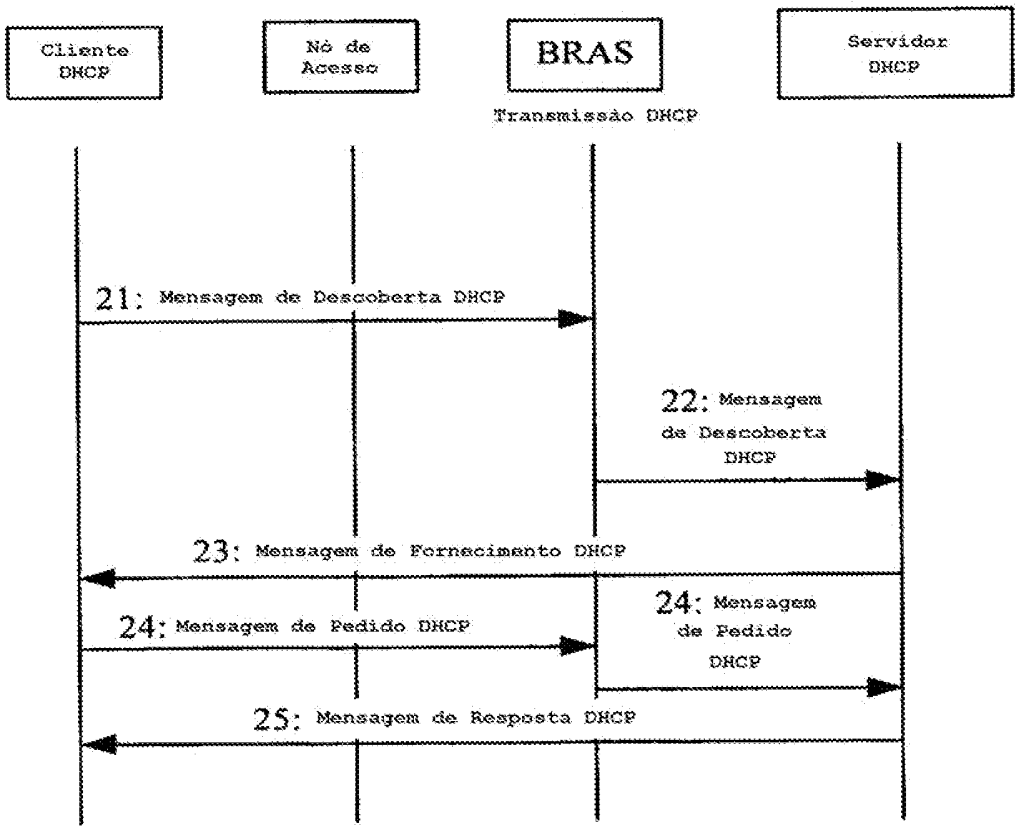

Cliente DHCP
Nó de Acesso
BRAS
Transmissão DHCP
Servidor DHCP
21: Mensagem de Descoberta DHCP
22: Mensagem de Descoberta DHCP
23: Mensagem de Fornecimento DHCP
24: Mensagem de Pedido DHCP
24: Mensagem de Pedido DHCP
25: Mensagem de Resposta DHCP

Fig. 2

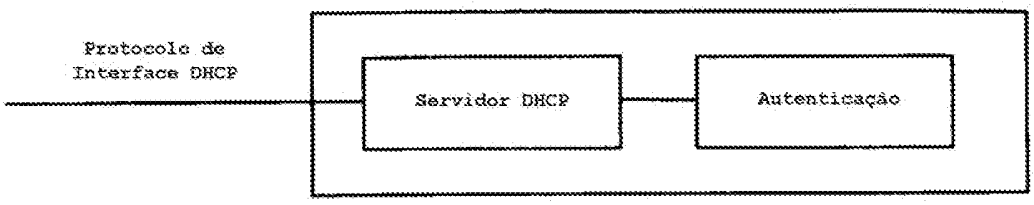

Protocolo de
Interface DHCP
Servidor DHCP
Autenticação

Fig. 3

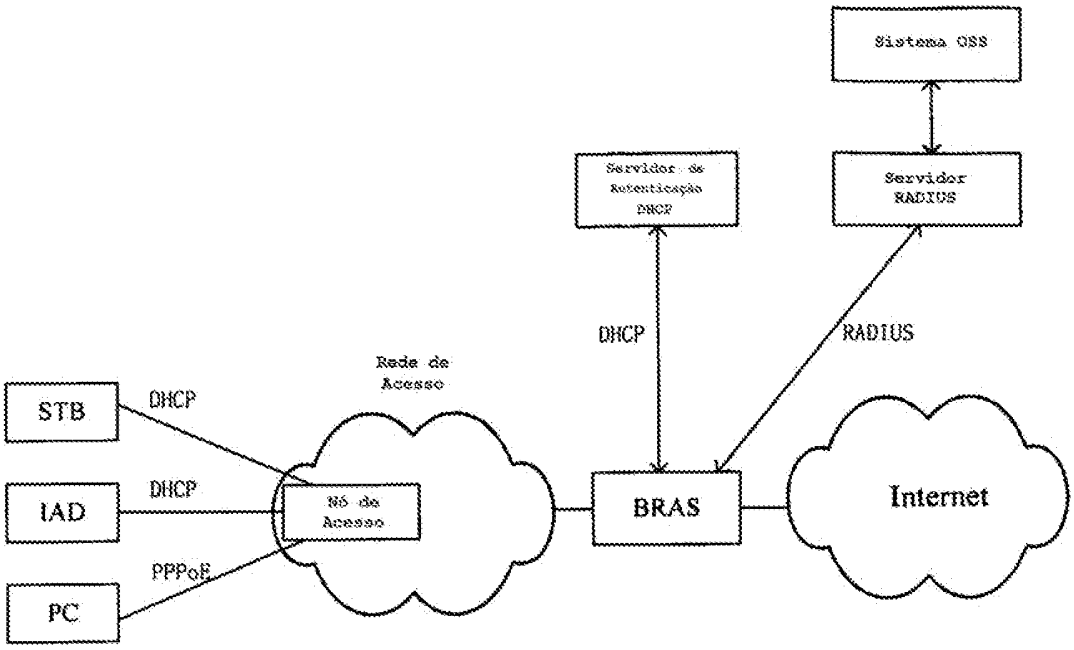

Sistema OSS
Servidor de
Autenticação
DHCP
Servidor
RADIUS
DHCP
RADIUS
Rede de
Acesso
STB
DHCP
IAD
DHCP
PC
PPPoE
Nó de
Acesso
BRAS
Internet

Fig. 4

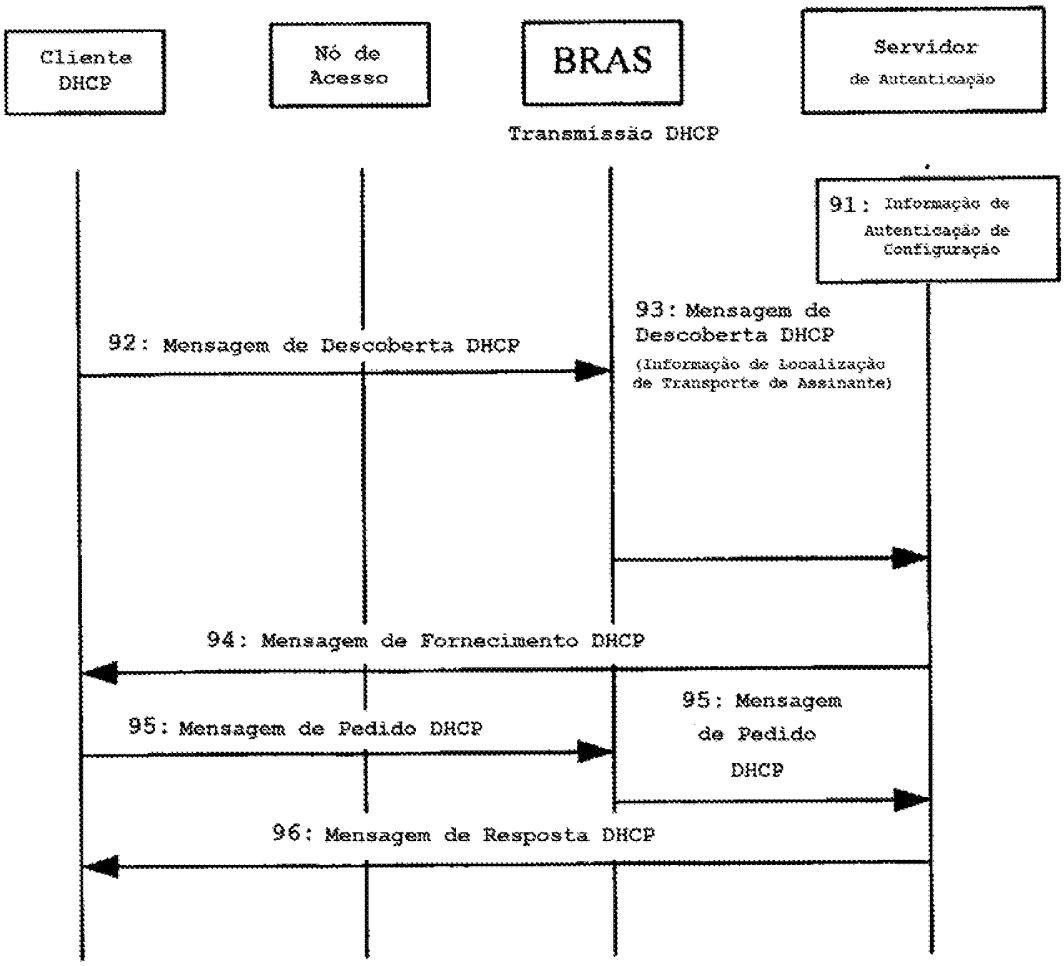

Cliente DHCP
Nó de Acesso
BRAS
Servidor de Autenticação
Transmissão DHCP
91: Informação de Autenticação de Configuração
92: Mensagem de Descoberta DHCP
93: Mensagem de Descoberta DHCP
(Informação de Localização de Transporte de Assinante)
94: Mensagem de Fornecimento DHCP
95: Mensagem de Pedido DHCP
95: Mensagem de Pedido DHCP
96: Mensagem de Resposta DHCP

Fig. 5