(11) Número de Publicação: **PT 2139187 E**

(51) Classificação Internacional:
H04L 29/06 (2011.01) ***H04L 29/12*** (2011.01)

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

(22) Data de pedido: **2008.03.19**

(30) Prioridade(s): **2007.07.20 CN 200710129994**

(43) Data de publicação do pedido: **2009.12.30**

(45) Data e BPI da concessão: **2011.08.31 215/2011**

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

(72) Inventor(es):
ZHENHAI LI **CN**

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

(54) Epígrafe: **MÉTODO, SISTEMA DE COMUNICAÇÃO E DISPOSITIVO PARA PROCESSAMENTO DE PACOTES ARP**

(57) Resumo:
SÃO DIVULGADOS UM MÉTODO, UM SISTEMA DE COMUNICAÇÃO E UM DISPOSITIVO DE PROCESSAMENTO DE PACOTES ARP (ADDRESS RESOLUTION PROTOCOL - PROTOCOLO DE RESOLUÇÃO DE ENDEREÇOS). O MÉTODO INCLUI: A RECEÇÃO DE UM PACOTE ARP E A AVALIAÇÃO DO TIPO DO PACOTE ARP; QUANDO O PACOTE ARP É UM PEDIDO ARP, A RESPOSTA AO PEDIDO ARP SE UMA ENTRADA CORRESPONDENTE AO PEDIDO ARP FOR ENCONTRADA NUMA TABELA ARP CONFIGURADA LOCALMENTE; E QUANDO O PACOTE ARP É UMA RESPOSTA ARP, A COMUNICAÇÃO DA RESPOSTA ARP SE UMA ENTRADA CORRESPONDENTE À RESPOSTA ARP FOR ENCONTRADA NA TABELA ARP CONFIGURADA LOCALMENTE E UM PARÂMETRO DE COMUNICAÇÃO NA ENTRADA INDICAR PERMISSÃO DE COMUNICAÇÃO; OU A REJEIÇÃO DA RESPOSTA ARP SE NENHUMA ENTRADA CORRESPONDENTE À RESPOSTA ARP FOR ENCONTRADA NA TABELA ARP.

RESUMO

"MÉTODO, SISTEMA DE COMUNICAÇÃO E DISPOSITIVO PARA PROCESSAMENTO DE PACOTES ARP"

São divulgados um método, um sistema de comunicação e um dispositivo de processamento de pacotes ARP (Address Resolution Protocol - Protocolo de Resolução de Endereços). O método inclui: a receção de um pacote ARP e a avaliação do tipo do pacote ARP; quando o pacote ARP é um pedido ARP, a resposta ao pedido ARP se uma entrada correspondente ao pedido ARP for encontrada numa tabela ARP configurada localmente; e quando o pacote ARP é uma resposta ARP, a comunicação da resposta ARP se uma entrada correspondente à resposta ARP for encontrada na tabela ARP configurada localmente e um parâmetro de comunicação na entrada indicar permissão de comunicação; ou a rejeição da resposta ARP se nenhuma entrada correspondente à resposta ARP for encontrada na tabela ARP.

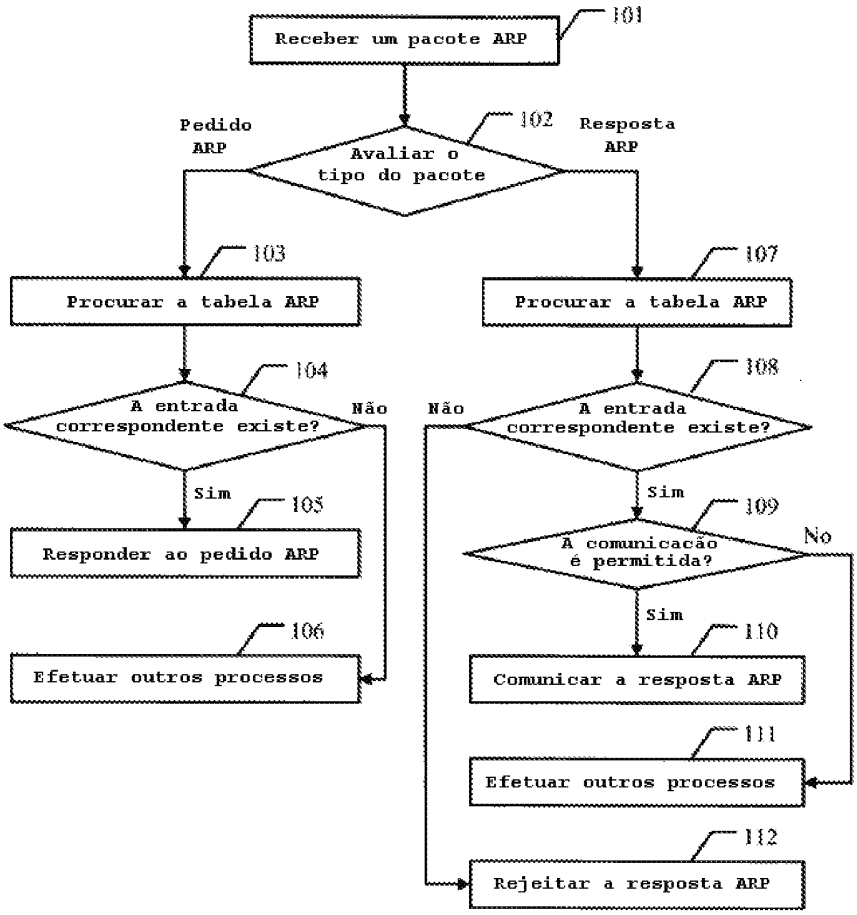
Receber um pacote ARP
101
Avaliar o tipo do pacote
102
Pedido ARP
Resposta ARP
Procurar a tabela ARP
103
A entrada correspondente existe?
104
Não
Sim
Responder ao pedido ARP
105
Efetuar outros processos
106
Procurar a tabela ARP
107
A entrada correspondente existe?
108
Não
Sim
A comunicação é permitida?
109
No
Sim
Comunicar a resposta ARP
110
Efetuar outros processos
111
Rejeitar a resposta ARP
112

FIG. 1

DESCRIÇÃO
"MÉTODO, SISTEMA DE COMUNICAÇÃO E DISPOSITIVO PARA PROCESSAMENTO DE PACOTES ARP"

Campo da Invenção

A presente invenção refere-se a comunicações e, em particular, a um método, um sistema de comunicação e um dispositivo de processamento de pacotes ARP (Address Resolution Protocol).

Antecedentes da Invenção

O ARP é um dos protocolos de camada inferior no conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de Controlo de Transmissão/Protocolo de Internet). O ARP foi concebido para converter um endereço IP num endereço físico Ethernet, nomeadamente um endereço MAC (Media Access Control - Controlo de Acesso de Suporte).

As comunicações entre dispositivos Ethernet utilizam endereços MAC para o endereçamento, enquanto várias aplicações TCP/IP utilizam endereços IP para o endereçamento. É necessário que vários pacotes de dados sejam finalmente encapsulados em tramas Ethernet para a transmissão. Por conseguinte, antes de efetuar comunicações IP, é necessário obter o endereço MAC do outro lado através da resolução do endereço IP do outro lado. O protocolo responsável pelo processo de resolução é o ARP.

Para acelerar a conversão de endereços, um dispositivo de rede utiliza a tecnologia de cache ARP ao implementar o ARP e utiliza uma estrutura de tabela para colocar em cache uma

determinada quantidade de relações de mapeamento de endereços localmente. Em geral, a tabela é conhecida como tabela ARP.

Contudo, na rede existente, existem habitualmente ataques de rede baseados em ARP. Da perspetiva da origem do ataque, os ataques ARP dividem-se nos seguintes dois tipos:

1. Fraude de endereço: a pessoa que efetua o ataque envia um pedido ARP ou uma resposta ARP com uma relação de mapeamento de endereço errado para alterar a tabela ARP do anfitrião ou da porta de conexão. Por conseguinte, a porta de conexão ou o anfitrião envia o pacote para um endereço físico errado e o ataque funciona.

2. Ataque DoS (Denial of Service) ARP: geralmente, o ataque DoS ARP visa os dispositivos da porta de conexão (tais como um *router* ou um comutador). Os pacotes ARP são, de uma forma geral, processados no plano de controlo do dispositivo. Habitualmente, o plano de controlo utiliza uma CPU universal como um motor de processamento. A CPU universal é caracterizada por ter um processamento sofisticado, mas um desempenho limitado. Devido às demasiadas tarefas de processamento, a CPU no plano de controlo tem tendência para ficar sobrecarregada ou avariar. Tendo em conta a fraqueza anterior, a pessoa que efetua o ataque DoS ARP envia pacotes ARP de tráfego elevado para o dispositivo da porta de conexão, de modo a tornar o plano de controlo do dispositivo extremamente ocupado e incapaz de processar pacotes ARP normais, e o ataque funciona.

Em seguida, é apresentado um método de processamento de pacotes ARP no estado da técnica:
Primeiro, o endereço IP de cada pacote ARP é verificado no plano de encaminhamento e os pacotes ARP ilegais são rejeitados.

A verificação do endereço IP inclui:

1. Verificação do endereço IP de destino: verificar se o endereço IP de destino corresponde ao endereço IP no segmento de rede da porta de conexão; caso contrário, rejeitar o pacote; e

2. Verificação do endereço IP de origem: verificar se o endereço IP de origem é um endereço IP “legal”. “Legal” significa que o endereço IP já esteve nas entradas da tabela ARP. Para esses pacotes, a prioridade de envio é elevada; para outros pacotes ARP, a prioridade de envio é baixa.

Contudo, a tecnologia anterior é incapaz de impedir os ataques com endereços IP legais.

Para superar o defeito da solução anterior, outro método de processamento de pacotes ARP no estado da técnica é:
a resposta ao pedido ARP no plano de encaminhamento diretamente mediante a utilização da capacidade de processamento de alta velocidade do processador de rede no plano de encaminhamento.

Os pacotes ARP classificam-se em pedido ARP e resposta ARP. A solução anterior trata apenas do pedido ARP e é incapaz de resolver o problema dos ataques de tráfego elevado utilizando a resposta ARP. O pedido de patente US

2006/0209818 divulga métodos e dispositivos para impedir a corrupção de cache ARP.

Resumo da Invenção

A presente invenção fornece um método, um sistema de comunicação e um dispositivo de processamento de pacotes ARP para impedir ataques de rede iniciados com pacotes ARP.

Como um primeiro aspeto da invenção, o método de processamento de pacotes ARP inclui:

a receção de um pacote ARP e a avaliação do tipo do pacote ARP;

quando o pacote ARP é um pedido ARP, a resposta ao pedido ARP se uma entrada ARP correspondente ao pedido ARP for encontrada numa tabela ARP local; e

quando o pacote ARP é uma resposta ARP, a comunicação da resposta ARP se uma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP local e o parâmetro de comunicação no ARP correspondente à entrada de resposta ARP indicar permissão de comunicação; ou a rejeição da resposta ARP se nenhuma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP; em que a tabela ARP local é fornecida por um processador de plano de controlo a um processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

Como um segundo aspeto da invenção, o sistema de comunicação inclui:
um processador de plano de encaminhamento, configurado para receber um pacote ARP (Address Resolution Protocol) e

avaliar o tipo do pacote ARP; quando o pacote ARP é um pedido ARP, responder ao pedido ARP se uma entrada ARP correspondente ao pedido ARP for encontrada numa tabela ARP local; quando o pacote ARP é uma resposta ARP, comunicar a resposta ARP se uma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP local e um parâmetro de comunicação na entrada ARP correspondente à resposta ARP indicar permissão de comunicação; ou rejeitar a resposta ARP se nenhuma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP; e

um processador de plano de controlo, configurado para receber a resposta ARP ou o pedido ARP comunicado pelo processador de plano de encaminhamento;

em que a tabela ARP local é fornecida por um processador de plano de controlo a um processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

De acordo com a presente invenção, o processador de plano de encaminhamento pode responder a um pedido ARP recebido diretamente em vez de gerar uma entrada ARP de acordo com o pedido ARP, eliminando assim a possibilidade de utilizar o pedido ARP para praticar fraude de endereço na tabela ARP. Além disso, ao receber uma resposta ARP, o processador de plano de encaminhamento comunica apenas a resposta ARP com permissão de comunicação na tabela ARP, eliminando assim a possibilidade de ataques utilizando múltiplas respostas ARP.

Descrição Breve das Figuras

A FIG. 1 é um fluxograma de um método de processamento de pacotes ARP numa forma de realização da presente invenção.

A FIG. 2 é um fluxograma de processamento de um pedido ARP numa forma de realização da presente invenção.

A FIG. 3 é um fluxograma de processamento de uma resposta ARP numa forma de realização da presente invenção.

A FIG. 4 ilustra um sistema de comunicação numa forma de realização da presente invenção.

A FIG. 5 ilustra um processador de plano de encaminhamento numa forma de realização da presente invenção.

Descrição Detalhada da Invenção

As formas de realização da presente invenção fornecem um método, um sistema de comunicação e um processador de plano de encaminhamento de processamento de pacotes ARP para impedir ataques de rede utilizando pacotes ARP.

A FIG. 1 é um fluxograma de um método de processamento de pacotes ARP numa forma de realização da presente invenção. O método inclui:

101. Receber um pacote ARP.

O processador de plano de encaminhamento recebe um pacote ARP enviado por um dispositivo externo.

Em geral, um dispositivo de comunicação de dados topo de gama (como, por exemplo, *routers* ou comutadores topo de gama) inclui três planos relativamente independentes: plano de controlo, plano de encaminhamento e plano de gestão.

O plano de controlo utiliza geralmente uma CPU universal como motor de processamento e é responsável por processar protocolos sofisticados (como, por exemplo, um protocolo de direcionamento).

O plano de encaminhamento é responsável pelo encaminhamento de dados de alta velocidade.

O plano de gestão é responsável pela gestão de rede, pelas linhas de comando, pelos registos e alarmes.

Nesta forma de realização, o processador de plano de encaminhamento pode ser um sistema de processamento composto por uma CPU de núcleo único ou de múltiplos núcleos, um processador de rede ou um processador ASIC (Application Specific Integrated Circuit - Circuito Integrado de Aplicação Específica) e os periféricos necessários para o funcionamento desses componentes. Alguns exemplos de periféricos são: Memória de Acesso Aleatório (RAM - Random Access Memory), Memória Endereçável de Conteúdo Ternária (TCAM - Ternary Content Addressable Memory) ou memória Flash.

102. Avaliar o tipo do pacote ARP. Se o pacote ARP for um pedido ARP, é realizado o passo 103; se o pacote ARP for uma resposta ARP, é realizado o passo 107.

A forma como avaliar o tipo do pacote ARP baseia-se no estado da técnica e não é aqui descrita em mais detalhe.

103. Procurar a tabela ARP.
A tabela ARP no processador de plano de encaminhamento é procurada de acordo com o pedido ARP obtido.

Nesta forma de realização, a tabela ARP no processador de plano de encaminhamento pode ser fornecida pelo processador de plano de controlo ao processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

Nesta forma de realização, a relação correspondente entre o endereço IP da interface da porta de conexão e o endereço MAC é incluída na entrada da tabela ARP. Quando o protocolo VRRP (Virtual Router Redundancy Protocol - Protocolo de Redundância de Router Virtual) está ativado na interface, a entrada necessita de ser mantida de acordo com a alteração de estado do VRRP.

É possível definir um *bit* de sinalização numa entrada da tabela ARP para indicar se a entrada é uma entrada ARP da porta de conexão ou uma entrada ARP de *proxy*.

104. Avaliar se uma entrada correspondente ao pedido ARP obtido se encontra na tabela ARP; se sim, é realizado o passo 105; caso contrário, é realizado o passo 106.

A forma como avaliar será detalhada na forma de realização subsequente mais à frente.

105. Responder ao pedido ARP.
Se uma entrada correspondente ao pedido ARP obtido for encontrada na tabela ARP, o processador de plano de encaminhamento responde ao pedido ARP. A forma como responder será detalhada na forma de realização subsequente mais à frente.

106. Efetuar outros processos.

Se nenhuma entrada correspondente ao pedido ARP obtido for encontrada na tabela ARP, o processador de plano de encaminhamento efetua outros processos. Esses processos serão detalhados na forma de realização subsequente mais à frente.

107. Procurar a tabela ARP.
A tabela ARP no processador de plano de encaminhamento é procurada de acordo com a resposta ARP obtida.

Nesta forma de realização, a tabela ARP no processador de plano de encaminhamento pode ser fornecida pelo processador de plano de controlo ao processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

108. Avaliar se uma entrada correspondente à resposta ARP obtida se encontra na tabela ARP; se sim, é realizado o passo 109; caso contrário, é realizado o passo 112.

109. Avaliar se o parâmetro de comunicação na entrada correspondente indica permissão de comunicação. Se o parâmetro de comunicação indicar permissão, é realizado o passo 110; caso contrário, é realizado o passo 111.

110. Comunicar a resposta ARP.
Quando o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação, o processador de plano de encaminhamento comunica a resposta ARP ao processador de plano de controlo.

111. Efetuar outros processos.

Se o parâmetro de comunicação na entrada correspondente à resposta ARP indicar sem permissão de comunicação, o processador de plano de encaminhamento efetua outros processos. Esses processos serão detalhados na forma de realização subsequente mais à frente.

112. Rejeitar a resposta ARP.
Se nenhuma entrada correspondente à resposta ARP obtida existir na tabela ARP, a resposta ARP é rejeitada.

Na forma de realização anterior, o processador de plano de encaminhamento responde ao pedido ARP recebido diretamente em vez de gerar uma entrada ARP de acordo com o pedido ARP, eliminando assim a possibilidade de utilizar o pedido ARP para praticar fraude de endereço na tabela ARP. Além disso, ao receber uma resposta ARP, o processador de plano de encaminhamento comunica apenas a resposta ARP com permissão de comunicação na tabela ARP, eliminando assim a possibilidade de ataques utilizando múltiplas respostas ARP.

O método para processar cada tipo de pacote ARP é explicado abaixo em detalhe:

I. Processar um pedido ARP
A FIG. 2 é um fluxograma de um método de processamento de pedidos ARP numa forma de realização da presente invenção. O método inclui:

201. Receber um pedido ARP.
O processador de plano de encaminhamento recebe um pedido ARP enviado por um dispositivo externo.

202. Filtrar o pedido ARP se o endereço MAC de origem do pedido ARP for um endereço não *unicast*.

A forma como filtrar o pedido ARP baseia-se no estado da técnica e não é aqui descrita em mais detalhe.

203. Procurar a tabela ARP.
Os parâmetros, tais como o número de porta, o ID VLAN (Virtual Local Area Network - Rede Local Virtual) e o endereço IP de destino são obtidos a partir do pedido ARP recebido, e a tabela ARP armazenada localmente no processador de plano de encaminhamento é procurada de acordo com os parâmetros obtidos.

204. Avaliar se uma entrada correspondente ao pedido ARP obtido se encontra na tabela ARP; se sim, é realizado o passo 205; caso contrário, é realizado o passo 208.

205. Avaliar se o pedido ARP é um pedido ARP da porta de conexão ou um pedido ARP de *proxy*; se sim, é realizado o passo 206; caso contrário, é realizado o passo 207.

A avaliação é implementada verificando se existe um *bit* de sinalização "entrada ARP da porta de conexão ou entrada ARP de *proxy*" na entrada correspondente.

206. Responder ao pedido ARP.
Se o pedido ARP for um pedido ARP da porta de conexão ou um pedido ARP de *proxy*, o processador de plano de encaminhamento responde ao pedido ARP para o dispositivo externo. A resposta é implementada através da edição do pedido ARP, de modo a tornar o pedido ARP numa resposta ARP, ou da criação de uma nova resposta ARP cujo endereço

MAC de origem seja o endereço MAC nesta entrada ARP. A resposta ARP editada ou a resposta ARP recentemente criada é enviada através de uma porta especificada na entrada ARP.

Nesta forma de realização, no processo de resposta ao pedido ARP, o processador de plano de encaminhamento não gera uma entrada ARP de acordo com o endereço IP de origem ou o endereço MAC no pedido ARP, mas efetua processamento sem estado para o pedido ARP.

207. Rejeitar o pedido ARP.
O pedido ARP recebido é rejeitado.

208. Avaliar se a função ARP de *proxy* está ativada na interface que recebeu o pedido ARP; se a função ARP estiver ativada, é realizado o passo 209; caso contrário, é realizado o passo 207.

209. Limitar a velocidade do pedido ARP e comunicar o pedido ARP.

Se a função ARP de *proxy* estiver ativada na interface que recebeu o pedido ARP, o processador de plano de encaminhamento limita a velocidade do pedido ARP e, em seguida, comunica o pedido ARP ao processador de plano de controlo.

Nesta forma de realização, a forma como avaliar se o pedido ARP é um pedido ARP da porta de conexão ou um pedido ARP de *proxy* pode ser implementada através da procura da tabela de encaminhamento ou de outras tabelas que incluam essas informações. O processo detalhado é semelhante ao da forma de realização anterior.

Nesta forma de realização, depois de o processador de plano de encaminhamento limitar a velocidade do pedido ARP recebido e comunicar o pedido ARP ao processador de plano de controlo no passo 209, o processador de plano de controlo trata do pedido ARP de *proxy* e, em seguida, fornece a entrada ARP de *proxy* ao processador de plano de encaminhamento de acordo com a configuração. O endereço MAC na entrada ARP de *proxy* é o endereço MAC da porta de conexão. Subsequentemente, quando o pedido ARP correspondente à entrada ARP de *proxy* for recebido, o processador de plano de encaminhamento pode tratar do pedido ARP diretamente sem o enviar ao processador de plano de controlo. Por conseguinte, a velocidade de processamento é aumentada, e a capacidade de impedir ataques de pedido ARP é melhorada no caso de a função ARP de *proxy* estar ativada.

Nesta forma de realização, no processo de resposta ao pedido ARP, o processador de plano de encaminhamento não gera uma entrada ARP de acordo com o endereço IP de origem ou o endereço MAC no pedido ARP, impedindo assim os ataques ARP que utilizam o pedido ARP para praticar fraude de endereço MAC.

II. Processar uma resposta ARP

A FIG. 3 é um fluxograma de um método de processamento de respostas ARP numa forma de realização da presente invenção. O método inclui:

301. Receber uma resposta ARP.

O processador de plano de encaminhamento recebe uma resposta ARP enviada por um dispositivo externo.

302. Procurar a tabela ARP.
O endereço IP de origem é obtido a partir da resposta ARP recebida, e a tabela ARP armazenada localmente no processador de plano de encaminhamento é procurada de acordo com o endereço IP de origem obtido.

303. Avaliar se uma entrada correspondente à resposta ARP obtida se encontra na tabela ARP; se sim, é realizado o passo 304; caso contrário, é realizado o passo 307.

304. Avaliar se o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação. Se o parâmetro de comunicação indicar permissão, é realizado o passo 305; caso contrário, é realizado o passo 306 ou 307.

305. Comunicar a resposta ARP.
Quando o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação, o processador de plano de encaminhamento comunica a resposta ARP ao processador de plano de controlo.

Nesta forma de realização, o processador de plano de encaminhamento comunica a resposta ARP ao processador de plano de controlo. O processador de plano de controlo trata da resposta ARP e, em seguida, modifica o parâmetro de comunicação na entrada correspondente à resposta ARP para “sem permissão de comunicação” na tabela ARP.

306. Limitar a velocidade da resposta ARP e, em seguida, comunicar a resposta ARP.
O processador de plano de encaminhamento limita a velocidade da resposta ARP de acordo com a regra de

processamento predefinida e, em seguida, comunica a resposta ARP ao processador de plano de controlo.

307. Rejeitar a resposta ARP.

Nesta forma de realização, se o parâmetro de comunicação na entrada correspondente à resposta ARP indicar sem permissão de comunicação no passo 304, é escolhido realizar o passo 306 ou 307 de acordo com a regra de processamento predefinida. Por exemplo, em circunstâncias normais, o endereço MAC do dispositivo não muda frequentemente. Por conseguinte, é possível escolher a política de rejeição. Em circunstâncias especiais em que seja necessário que o endereço MAC mude com frequência, é possível escolher a política de limitação de velocidade. A política de rejeição é mais eficaz do que a política de limitação de velocidade no impedimento da fraude de endereço. Por conseguinte, a política de rejeição é preferida, exceto em circunstâncias especiais.

Nesta forma de realização, a política de limitação de velocidade ou a política de rejeição é implementada através da procura da tabela relevante. Aqui, o tipo da tabela não é limitado.

Conforme ilustrado na FIG. 4, um sistema de comunicação fornecido numa forma de realização da presente invenção inclui:

um dispositivo externo 401, adaptado para enviar um pedido ARP e uma resposta ARP;

um processador de plano de encaminhamento 402, adaptado para avaliar o tipo do pacote ARP recebido; quando o pacote

ARP é um pedido ARP, procurar a tabela ARP local e responder ao pedido ARP de acordo com a entrada correspondente ao pedido ARP na tabela ARP; quando o pacote ARP é uma resposta ARP, procurar a tabela ARP local e avaliar se o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação de acordo com a entrada correspondente à resposta ARP na tabela ARP; se o parâmetro de comunicação indicar permissão de comunicação, comunicar a resposta ARP; se nenhuma entrada correspondente à resposta ARP for encontrada na tabela ARP, rejeitar a resposta ARP; e

um processador de plano de controlo 403, adaptado para receber a resposta ARP ou o pedido ARP comunicado pelo processador de plano de encaminhamento 402.

A FIG. 5 ilustra um processador de plano de encaminhamento numa forma de realização da presente invenção. O processador de plano de encaminhamento inclui:

uma unidade de avaliação 501, adaptada para avaliar o tipo de um pacote ARP recebido;

uma primeira unidade de procura 502, adaptada para procurar a tabela ARP local quando o pacote ARP é um pedido ARP;

uma unidade de resposta 503, adaptada para responder ao pedido ARP se uma entrada correspondente ao pedido ARP for encontrada na tabela ARP;
uma segunda unidade de procura 504, adaptada para procurar a tabela ARP local quando o pacote ARP é uma resposta ARP;

uma unidade de rejeição 506, adaptada para rejeitar a resposta ARP se nenhuma entrada correspondente à resposta ARP for encontrada na tabela ARP;
uma unidade de limitação de velocidade 509, adaptada para limitar a velocidade do pacote ARP e comunicar o pacote ARP ao processador de plano de controlo;
uma unidade de avaliação de interface 508, adaptada para avaliar se a função ARP de *proxy* está ativada na interface que recebe o pedido ARP se nenhuma entrada correspondente ao pedido ARP recebido for encontrada na tabela ARP; se a função ARP de *proxy* estiver ativada, dar instruções à unidade de limitação de velocidade 509 para limitar a velocidade do pacote ARP e comunicar o pacote ARP; se a função ARP de *proxy* não estiver ativada, dar instruções à unidade de rejeição 506 para rejeitar o pedido ARP;
uma unidade de verificação 505, adaptada para avaliar se o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação quando uma entrada correspondente à resposta ARP é encontrada na tabela ARP; e
uma unidade de comunicação 507, adaptada para comunicar a resposta ARP ao processador de plano de controlo quando o parâmetro de comunicação na entrada correspondente à resposta ARP indica permissão de comunicação.

Na aplicação prática, podem ser combinadas numa unidade várias unidades que implementem funções semelhantes nas formas de realização da presente invenção. Por exemplo, a primeira unidade de procura 502 e a segunda unidade de procura 504 podem ser implementadas numa unidade.

É evidente para os peritos na especialidade que todos ou parte dos passos do método nas formas de realização

anteriores podem ser implementados através de equipamento informático que recebe instruções de um programa. O programa pode ser armazenado num suporte de armazenamento legível por computador. Ao ser executado, o programa efetua estes passos: o processador de plano de encaminhamento avalia o tipo de um pacote ARP recebido; quando o pacote ARP é um pedido ARP, o processador de plano de encaminhamento procura a tabela ARP local e, se uma entrada correspondente ao pedido ARP for encontrada na tabela ARP, responde ao pedido ARP diretamente; quando o pacote ARP é uma resposta ARP, o processador de plano de encaminhamento procura a tabela ARP local e, se uma entrada correspondente à resposta ARP for encontrada na tabela ARP, avalia se o parâmetro de comunicação na entrada indica permissão de comunicação; se o parâmetro de comunicação indicar permissão de comunicação, o processador de plano de encaminhamento comunica a resposta ARP ao processador de plano de controlo; se nenhuma entrada correspondente à resposta ARP for encontrada na tabela ARP, o processador de plano de encaminhamento rejeita a resposta ARP.

O suporte de armazenamento pode ser uma Memória Só de Leitura (ROM - Read-Only Memory), um disco magnético ou um CD (Compact Disk - Disco Compacto).

Um método, um sistema de comunicação e um processador de plano de encaminhamento de processamento de pacotes ARP de acordo com a presente invenção são descritos acima. Embora a invenção seja descrita através de várias formas de realização exemplares, a invenção não está limitada a essas formas de realização.

Lisboa, 27 de Outubro de 2011

REIVINDICAÇÕES

1. Um método de processamento de pacotes ARP (Address Resolution Protocol), caracterizado por compreender:

a receção (101) de um pacote ARP e a avaliação do tipo do pacote ARP;

quando o pacote ARP é um pedido ARP, a resposta (105) ao pedido ARP se uma entrada ARP correspondente ao pedido ARP for encontrada numa tabela ARP local; e

quando o pacote ARP é uma resposta ARP, a comunicação (110) da resposta ARP se uma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP local e um parâmetro de comunicação na entrada ARP correspondente à resposta ARP indicar permissão de comunicação; ou a rejeição (112) da resposta ARP se nenhuma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP;

em que a tabela ARP local é fornecida por um processador de plano de controlo a um processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

2. O método de processamento de pacotes ARP de acordo com a reivindicação 1, caracterizado por compreender ainda:

quando o pacote ARP é o pedido ARP, a avaliação sobre se uma função ARP de *proxy* está ativada numa interface que recebe o pedido ARP se nenhuma entrada ARP correspondente ao pedido ARP for encontrada na tabela ARP;

se a função ARP de *proxy* estiver ativada, a limitação da velocidade do pedido ARP e, em seguida, a comunicação do pedido ARP a um processador de plano de controlo; e

se a função ARP de *proxy* não estiver ativada, a rejeição do pedido ARP.

3. O método de processamento de pacotes ARP de acordo com a reivindicação 1, caracterizado por compreender ainda:

quando o pacote ARP é a resposta ARP (301), se a entrada ARP correspondente à resposta ARP for encontrada na tabela ARP (302) e o parâmetro de comunicação na entrada ARP correspondente à resposta ARP indicar sem permissão de comunicação (304),

a limitação (306) da velocidade da resposta ARP e, em seguida, a comunicação da resposta ARP a um processador de plano de controlo ou a rejeição (307) da resposta ARP.

4. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 a 3, caracterizado por compreender ainda:

se o pacote ARP for o pedido ARP,

a procura da tabela ARP de acordo com um número de porta do pedido ARP, um ID VLAN (Virtual Local Area Network) e um endereço IP (Internet Protocol) de destino.

5. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 a 3, em que antes da resposta ao pedido ARP, o método é caracterizado por compreender ainda:

se a entrada ARP correspondente ao pedido ARP não for uma entrada ARP da porta de conexão ou uma entrada ARP de *proxy* (205), a rejeição do pedido ARP (207).

6. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 a 3, caracterizado por compreender ainda:

se o pacote ARP for uma resposta ARP, a procura da tabela ARP de acordo com um endereço IP (Internet Protocol) de origem da resposta ARP.

7. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 a 3, em que após a comunicação da resposta ARP, o método é caracterizado por compreender ainda:

a modificação do parâmetro de comunicação na entrada ARP correspondente à resposta ARP na tabela ARP para sem permissão de comunicação.

8. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 ou 2, caracterizado por a entrada ARP correspondente ao pedido ARP compreender: a relação correspondente entre o endereço IP de uma interface da porta de conexão e o endereço MAC da porta de conexão.

9. O método de processamento de pacotes ARP de acordo com qualquer uma das reivindicações 1 ou 3, caracterizado por a entrada ARP correspondente à resposta ARP compreender: o parâmetro de comunicação a indicar permissão de comunicação.

10. Um sistema de comunicação, caracterizado por compreender:

um processador de plano de encaminhamento (402), configurado para receber um pacote ARP (Address Resolution Protocol) e avaliar o tipo do pacote ARP; quando o pacote ARP é um pedido ARP, responder ao

pedido ARP se uma entrada ARP correspondente ao pedido ARP for encontrada numa tabela ARP local; quando o pacote ARP é uma resposta ARP, comunicar a resposta ARP se uma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP local e um parâmetro de comunicação na entrada ARP correspondente à resposta ARP indicar permissão de comunicação; ou rejeitar a resposta ARP se nenhuma entrada ARP correspondente à resposta ARP for encontrada na tabela ARP; e

um processador de plano de controlo (403), configurado para receber a resposta ARP ou o pedido ARP comunicado pelo processador de plano de encaminhamento;

em que a tabela ARP local é fornecida por um processador de plano de controlo a um processador de plano de encaminhamento ou configurada no processador de plano de encaminhamento diretamente.

11. O sistema de comunicação de acordo com a reivindicação 10, caracterizado por o processador de plano de encaminhamento (402) compreender:

uma unidade de avaliação (501), configurada para avaliar o tipo de um pacote ARP (Address Resolution Protocol) recebido;

uma primeira unidade de procura (502), configurada para procurar uma tabela ARP local quando a unidade de avaliação determina que o pacote ARP é um pedido ARP;

uma unidade de resposta (503), configurada para responder ao pedido ARP se a primeira unidade de procura encontrar uma entrada ARP correspondente ao pedido ARP;

uma segunda unidade de procura (504), configurada para procurar a tabela ARP local quando a unidade de

avaliação determina que o pacote ARP é uma resposta ARP; e

uma unidade de rejeição (506), configurada para rejeitar a resposta ARP se a segunda unidade de procura não encontrar nenhuma entrada correspondente à resposta ARP.

12. O sistema de comunicação de acordo com a reivindicação 11, caracterizado por o processador de plano de encaminhamento (402) compreender ainda:

uma unidade de limitação de velocidade (509), configurada para limitar a velocidade do pacote ARP e comunicar o pacote ARP a um processador de plano de controlo;

uma unidade de avaliação de interface (508), configurada para avaliar se uma função ARP de *proxy* está ativada numa interface que recebe o pedido ARP quando a primeira unidade de procura não encontra nenhuma entrada ARP correspondente ao pedido ARP recebido na tabela ARP; se a função ARP de *proxy* estiver ativada, dar instruções à unidade de limitação de velocidade para limitar a velocidade do pedido ARP e comunicar o pedido ARP; se a função ARP de *proxy* não estiver ativada, dar instruções à unidade de rejeição para rejeitar o pedido ARP.

13. O sistema de comunicação de acordo com qualquer uma das reivindicações 11 ou 12, caracterizado por o processador de plano de encaminhamento (402) compreender ainda:

uma unidade de verificação (505), configurada para avaliar se um parâmetro de comunicação na entrada ARP correspondente à resposta ARP indica permissão de

comunicação quando a entrada ARP correspondente à resposta ARP é encontrada na tabela ARP; e

uma unidade de comunicação (507), configurada para comunicar a resposta ARP quando o parâmetro de comunicação na entrada ARP correspondente à resposta ARP indica permissão de comunicação.

14. O sistema de comunicação de acordo com qualquer uma das reivindicações 10 a 12, caracterizado por a entrada ARP correspondente ao pedido ARP compreender: a relação correspondente entre o endereço IP de uma interface da porta de conexão e o endereço MAC da porta de conexão.

15. O sistema de comunicação de acordo com qualquer uma das reivindicações 10 a 13, caracterizado por a entrada ARP correspondente à resposta ARP compreender: o parâmetro de comunicação a indicar permissão de comunicação.

Lisboa, 27 de Outubro de 2011

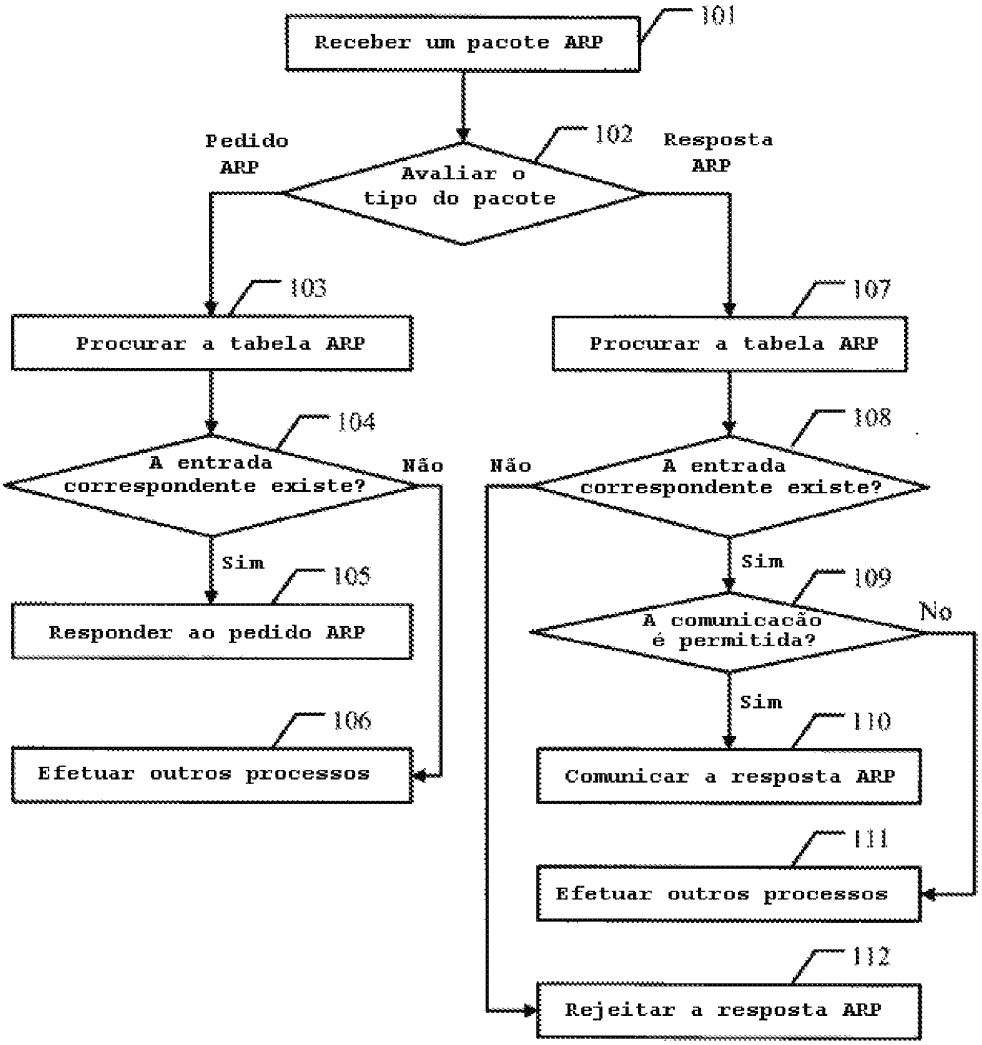
Receber um pacote ARP
101
Avaliar o tipo do pacote
102
Pedido ARP
Resposta ARP
Procurar a tabela ARP
103
A entrada correspondente existe?
104
Não
Sim
Responder ao pedido ARP
105
Efetuar outros processos
106
Procurar a tabela ARP
107
A entrada correspondente existe?
108
Não
Sim
A comunicação é permitida?
109
No
Sim
Comunicar a resposta ARP
110
Efetuar outros processos
111
Rejeitar a resposta ARP
112

FIG. 1

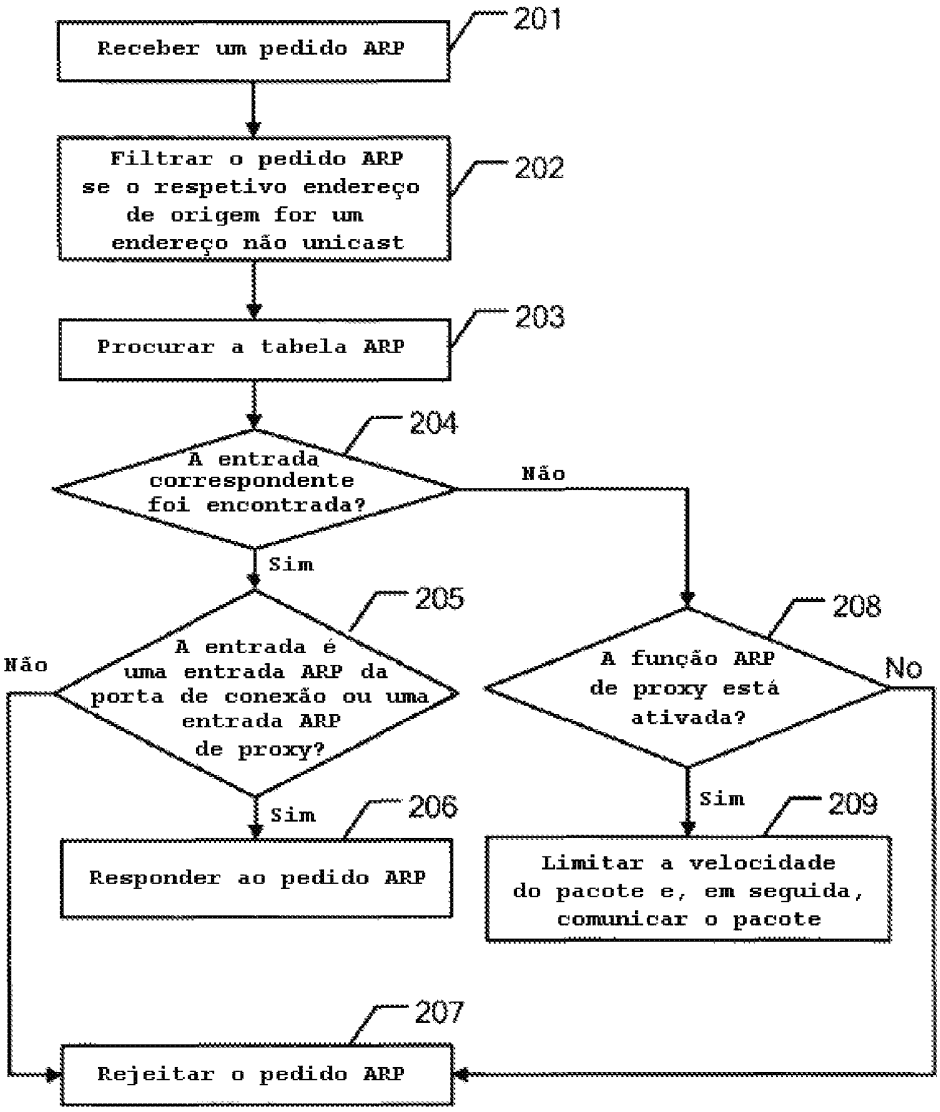
Receber um pedido ARP
201
Filtrar o pedido ARP se o respetivo endereço de origem for um endereço não unicast
202
Procurar a tabela ARP
203
A entrada correspondente foi encontrada?
204
Não
Sim
A entrada é uma entrada ARP da porta de conexão ou uma entrada ARP de proxy?
205
Não
Sim
Responder ao pedido ARP
206
A função ARP de proxy está ativada?
208
No
Sim
Limitar a velocidade do pacote e, em seguida, comunicar o pacote
209
Rejeitar o pedido ARP
207

FIG. 2

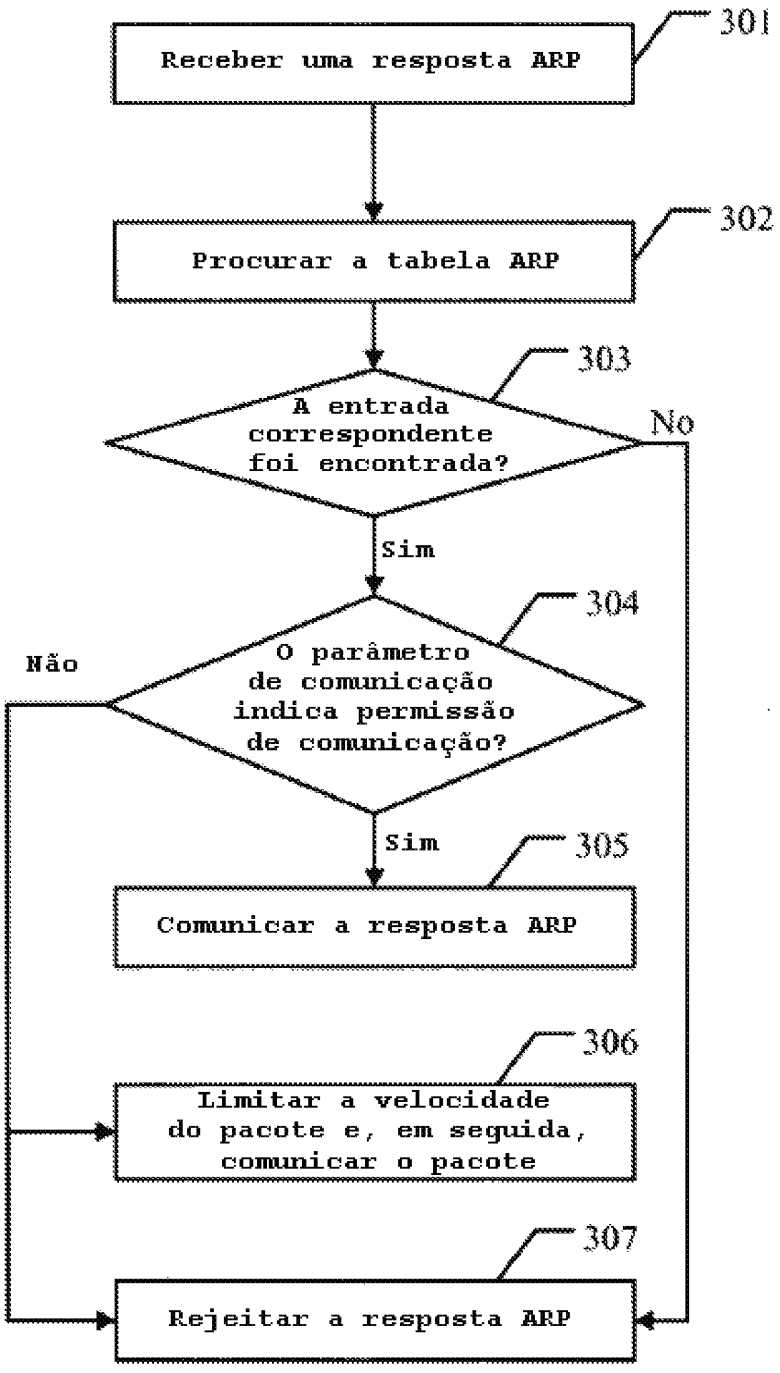
Receber uma resposta ARP
301
Procurar a tabela ARP
302
A entrada correspondente foi encontrada?
303
No
Sim
O parâmetro de comunicação indica permissão de comunicação?
304
Não
Sim
Comunicar a resposta ARP
305
Limitar a velocidade do pacote e, em seguida, comunicar o pacote
306
Rejeitar a resposta ARP
307

FIG. 3

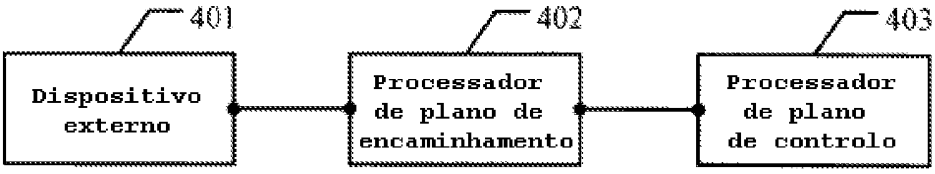
401
Dispositivo externo
402
Processador de plano de encaminhamento
403
Processador de plano de controlo

FIG. 4

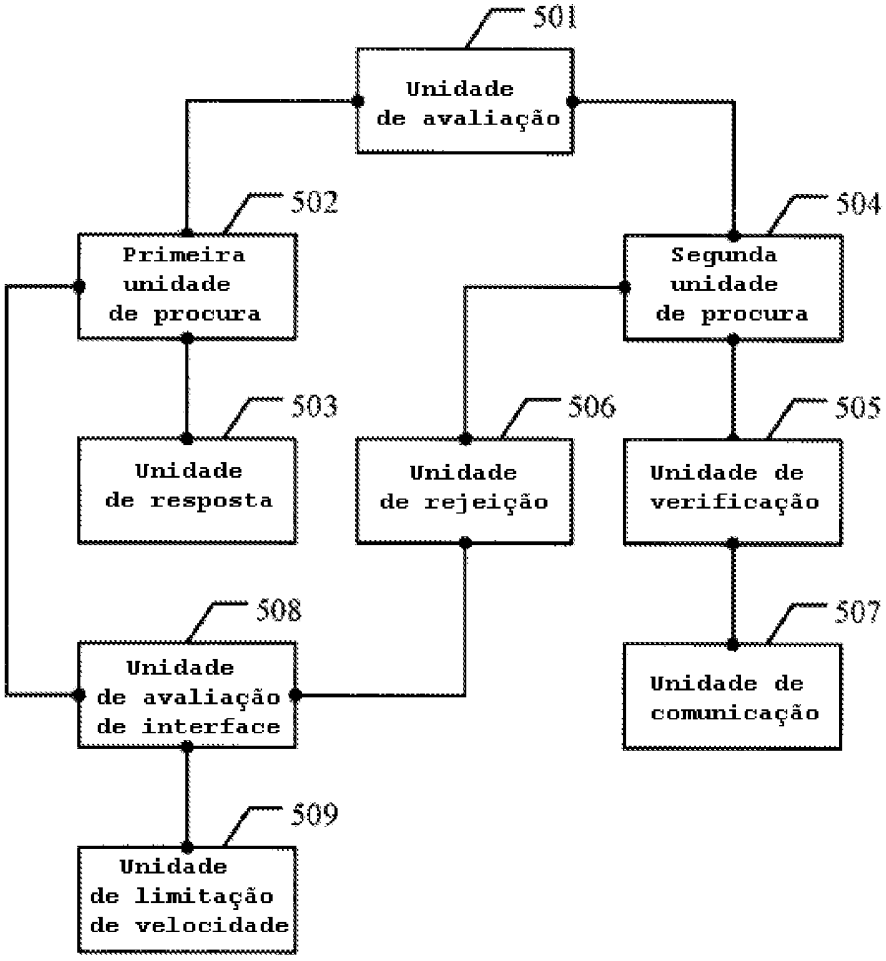
501
Unidade de avaliação
502
Primeira unidade de procura
503
Unidade de resposta
504
Segunda unidade de procura
505
Unidade de verificação
506
Unidade de rejeição
507
Unidade de comunicação
508
Unidade de avaliação de interface
509
Unidade de limitação de velocidade

FIG. 5