

**Fees**

- ☒ No fee is owed by the applicant(s).  
☐ Charge Deposit Account No. 12-1216 in the amount of \$180.00 (37 CFR 1.17(p)).

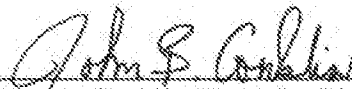
**Authorization to Charge Additional Fees**

- ☒ If any additional fees are owed in connection with this communication, please charge Deposit Account No. 12-1216.

**Instructions as to Overpayment**

- ☒ Credit Account No. 12-1216.  
☐ Refund

Respectfully submitted,



John B. Conklin, Reg. No. 30,369

Telephone: 312-616-5600

Facsimile: 925-482-0110

Date: May 11, 2015





Espacenet

Bibliographic data: US2007258449 (A1) — 2007-11-08

Packet routing with payload analysis, encapsulation and service module vectoring

No documents available for this priority number.

Inventor(s): BENNETT JAMES D [US] + (BENNETT JAMES D)

Applicant(s): BROADCOM CORP [US] + (BROADCOM CORPORATION, A CALIFORNIA CORPORATION, ; BROADCOM CORPORATION)

Classification: - international: H04L12/56  
- cooperative: H04L63/145

Application number: US20060429477 20060505

Priority number (s): US20060429477 20060505

Also published as: US7948977 (B2) EP1853025 (A1) TW200816712 (A)  
TWI363530 (B) CN101068253 (A) more

Abstract of US2007258449 (A1)

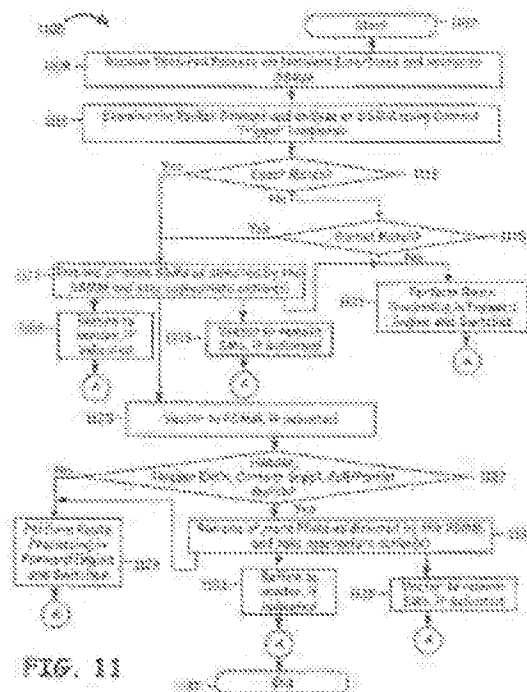


FIG. 11

An Internet infrastructure with network devices and end point devices containing service module manager and service modules, that supports packet analysis, encapsulation and vectoring, and interleaving applications. The network device that supports packet content analysis on arriving packet, consists of a plurality of packet switched interface circuitries, user interface circuitry, local storage comprising the service module manager software and a plurality of local service modules, and processing circuitry communicatively coupled to each of the packet switched interfaces, local storage and user interface circuit. The processing circuitry executes service module manager and thus analyzes the packet content and applies one or more selected local service module processing using the packet. The processing circuitry thus takes one or more actions on the packet. A packet switching exchange that supports packet content analysis, encapsulation and vectoring on arriving packet, consisting a plurality of interconnecting switches, a plurality of line cards, general primary processing card. A client device that supports packet content analysis on arriving packet containing a plurality of network interfaces, user interface circuitry, local storage and processing circuitry communicatively coupled to each of the network interfaces, local storage and user interface circuitry.

[19] 中华人民共和国国家知识产权局



# [12] 发明专利申请公布说明书

[21] 申请号 200710103149.2

[51] Int. Cl.

H04L 29/06 (2006.01)

H04L 12/56 (2006.01)

[43] 公开日 2007 年 11 月 7 日

[11] 公开号 CN 101068253A

[22] 申请日 2007.4.28

[21] 申请号 200710103149.2

[30] 优先权

[32] 2006.5.5 [33] US [31] 11/429,477

[32] 2006.5.5 [33] US [31] 11/429,478

[32] 2006.6.23 [33] US [31] 11/474,033

[32] 2006.7.20 [33] US [31] 11/491,052

[32] 2006.8.18 [33] US [31] 11/506,661

[71] 申请人 美国博通公司

地址 美国加州尔湾市奥尔顿公园路 16215 号  
92618-7013

[72] 发明人 詹姆斯·D·贝内特

[74] 专利代理机构 深圳市顺天达专利商标代理有限公司

代理人 蒙晓红 李 强

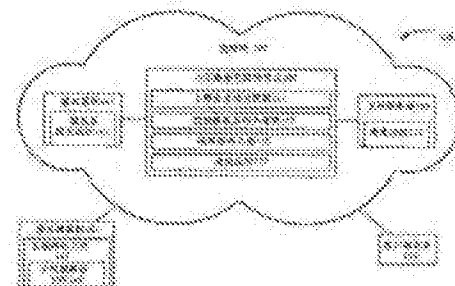
权利要求书 2 页 说明书 25 页 附图 10 页

## [54] 发明名称

通信结构、中间路由节点及其执行的方法

## [57] 摘要

本发明涉及一种通信架构、中间路由节点及其执行的方法。在通信架构中，若源端设备不包含恶评内容(例如，恶意程序，或非法内容、服务或传输)，中间节点支持将数据包从源端设备发送至目的端设备。该中间节点，例如交换机、路由器、接入点、桥接器或网关，包含多个预定模板和相应的隔离服务功能。通过将接收到的数据包与多个预定模板及相关逻辑进行比较，该中间节点识别出恶评源端设备，例如恶评服务器和恶评内容。该模板有一个或者多个域名、IP 地址或 URL 等的至少一部分作为目标。一旦被识别，本地和/或远端隔离服务功能则尝试在源端设备和目的端设备中抵拒、警告、消除和/或阻止该恶评内容。该警告可包括有人为口令以避免被恶意程序代替。





1、一种将数据包从源端设备发往目的端设备的通信架构，所述源端设备具有域名和当前网络地址，其特征在于，所述通信架构包括：

域名服务器，用于存储与所述源端设备对应的域名及当前网络地址；

中间路由节点；

存储在上述中间路由节点中的多个模板，其中的第一模板从域名服务器的相关存储器中使用所述源端设备的域名进行更新，所述第一模板将所述源端设备的当前网络地址作为目标；

隔离服务功能块；

所述中间路由节点在接收到来自所述源端设备的数据包后，成功地所述数据包与第一模板进行匹配；以及

所述中间路由节点通过触发所述隔离服务功能对成功匹配进行响应。

2、根据权利要求1所述的通信架构，其特征在于，所述源端设备包括恶评服务器，所述多个模板中的所述第一模板通过将当前网络地址作为目标从而将所述恶评服务器作为目标。

3、根据权利要求1所述的通信架构，其特征在于，所述源端设备是服务器群。

4、根据权利要求1所述的通信架构，其特征在于，所述隔离服务功能块传送人为口令。

5、一种用于将数据包从源端设备发往目的端设备的通信架构中的中间路由节点，其中所述源端设备具有网络识别符，且所述源端设备包含恶评内容，其特征在于，所述中间路由节点包括：

通信接口；

包含多个模板的存储器；

所述多个模板中将所述网络识别符的至少一部分作为目标的第一模板；

与所述存储器及通信接口相连的处理电路，用于对从所述源端设备接收的数据包进行比较时，将所述数据包与多个模板中的所述第一模板匹配；以

及

所述处理电路至少部分地基于所述匹配结果,触发隔离功能以作出响应。

6、根据权利要求5所述的中间路由节点,其特征在于,所述中间路由节点包括路由器。

7、根据权利要求5所述的中间路由节点,其特征在于,所述中间路由节点包括接入点。

8、根据权利要求5所述的中间路由节点,其特征在于,所述处理电路基于与所述多个模板中所述第一模板以及第二模板的匹配结果,触发所述隔离功能以作出响应,其中所述第二模板将统一资源定位符的至少一部分作为目标。

9、一种通过分组交换通信路径中的中间网络节点执行的方法,所述中间网络节点通信连接在源端设备和目的端设备之间,所述源端设备具有网络识别符和恶评内容,其特征在于,所述方法包括:

接收包含所述网络识别符的数据包;

将所述数据包与多个模板进行比较;

将所述数据包的至少一部分与所述多个模板中的第一模板匹配;

至少部分地基于所述匹配结果,触发隔离功能以作出响应。

10、根据权利要求9所述的方法,其特征在于,所述方法进一步包括:在本地执行所述隔离功能的至少一部分。

## 通信架构、中间路由节点及其执行的方法

### 技术领域

本发明涉及通信基础架构，更具体地说，涉及报文分组交换通信网络中的交换节点的操作。

### 背景技术

因特网终端设备使用包括网络节点的因特网来交换音频、视频和数据包，这种交换通常是没限制的。因特网基础架构通常包括网络节点如路由器、交换机、分组交换机、接入点以及因特网服务提供商网络（ISPN）、因特网通信路径和终端设备。终端设备包括个人计算机或者笔记本电脑、服务器、机顶盒、手持数据设备/通信设备以及其他的客户端设备等。在无限制的环境中，终端设备通常成为恶意程序的目标，该恶意程序包括病毒和恶意代码。此外，终端设备也有意地或者无意地成为这些恶意代码的传播源。通常，恶意程序一旦感染终端设备，就会不为用户所察觉地在终端设备复制，从而重复感染因特网基础架构。

但是，终端设备通常不能消除这些数据包或者数据包流（packet flow）。例如，很多烦人的广告弹出窗口欺骗用户点击错误的按钮，而不知道这些弹出窗口使用各种恶意代码来感染终端设备。这些不想要的代码是恶意的，其将个人数据传输到未知的服务器，导致个人数据可能被滥用。在其它情况下，终端设备的用户会安装病毒检测、隔离和/或删除的软件包，用户通常购买多种病毒处理软件包，因为当前软件包通常不能处理日益增加的病毒列表。虽然这些软件包有时候是免费的，但是，大多数情况下还是相当昂贵的，尤其是考虑到需要负担多种软件包之时。

从以下的描述和附图中，可以得到对本发明的各种优点、各个方面、创新特征、及其实施例细节的更深入的理解。

## 发明内容

本发明提供了一种装置及操作方法，将在其后对附图的简要说明。对具体实施方式部分的详细说明，以及权利要求中进行阐述。

在本发明中，一种将多个数据包从具有源端地址的源端设备发送到具有目的端地址的目的端设备的通信架构，包括具有多个交换设备的通信路径，多个预定义的模板和相关逻辑，以及多个隔离服务功能块。该源端设备发送数据包至多个交换设备中的第一交换设备，该数据包包含有源端地址和目的端地址。该第一交换设备通过将数据包与所述多个预定义的模板进行比较，将该源端地址标识为传播恶意程序的源地址，并应用相关逻辑，以及执行所述相关逻辑内指示的选定的隔离服务功能处理。最后，该第一交换设备执行相关逻辑内指示的选定的隔离服务功能处理。该源端地址可代表一个或者多个主域（home-domain）路径文件或子域（sub-domain）路径文件，且所有文件位于服务器或服务器群上。

在本发明中，一种互联网中用于将多个数据包从具有源端地址的源端设备发送到具有目的端地址的目的端设备的网络节点电路，包括接口电路、存储器，和与接口电路通信连接的处理电路。该处理电路通过将数据包与多个预定义的模板进行比较，将该源端地址标识为传播恶意程序的源地址，并应用相关逻辑，以及执行所述相关逻辑内指示的选定的隔离服务功能处理。

根据本发明的一个方面，提供了一种将数据包从源端设备发往目的端设备的通信架构，所述源端设备具有域名和当前网络地址，所述通信架构包括：

域名服务器，用于存储与所述源端设备对应的域名及当前网络地址；

中间路由节点；

存储在所述中间路由节点中的多个模板，其中的第一模板从域名服务器的相关存储器中使用所述源端设备的域名进行更新，所述第一模板将所述源端设备的当前网络地址作为目标；

隔离服务功能块；

所述中间路由节点在接收到来自所述源端设备的数据包后，成功地将所

述数据包与第一模板进行匹配；以及

所述中间路由节点通过触发所述隔离服务功能对成功匹配进行响应。

优选地，所述源端设备包括恶评服务器（notorious server），所述多个模板中的所述第一模板通过将当前网络地址作为目标从而将所述恶评服务器作为目标。

优选地，所述源端设备是服务器群。

优选地，所述隔离服务功能块传送人为口令（human challenge）。

优选地，所述隔离服务功能块传送警告消息。

优选地，所述源端设备提供恶意内容，所述隔离服务功能块使所述恶评内容无效。

优选地，所述源端设备提供恶意内容，所述隔离服务功能块删除所述恶评内容。

优选地，所述隔离服务功能块至少部分位于所述中间路由节点内。

优选地，所述隔离服务功能块至少部分位于支持服务器内。

优选地，所述目的端设备支持所述隔离服务功能。

根据本发明的另一个方面，提供了一种用于将数据包从源端设备发往目的端设备的通信架构中的中间路由节点，其中所述源端设备具有网络识别符，且所述源端设备包含恶评内容，所述中间路由节点包括：

通信接口；

包含多个模板的存储器；

所述多个模板中将所述网络识别符的至少一部分作为目标的第一模板；

与所述存储器及通信接口相连的处理电路，用于对从所述源端设备接收的数据包进行比较时，将所述数据包与多个模板中的所述第一模板匹配；以及

所述处理电路至少部分地基于所述匹配结果，触发隔离功能以作出响应。

优选地，所述中间路由节点包括路由器。

优选地，所述中间路由节点包括接入点。

优选地，所述处理电路基于与所述多个模板中所述第一模板以及第二模板的匹配结果，触发所述隔离功能以作出响应，其中所述第二模板将统一资源定位符（URL）的至少一部分作为目标。

优选地，所述处理电路基于与所述多个模板中所述第一模板以及第二模板的匹配结果，触发所述隔离功能以作出响应，其中所述第二模板将所述恶评内容的名称的至少一部分作为目标。

优选地，所述处理电路基于与所述多个模板中所述第一模板以及第二模板的匹配结果，触发所述隔离功能以作出响应，其中所述第二模板将所述恶评内容的目录路径的至少一部分作为目标。

根据本发明的又一个方面，提供了一种通过分组交换通信路径中的中间网络节点执行的方法，所述中间网络节点通信连接在源端设备和目的端设备之间，所述源端设备具有网络识别符和恶评内容，所述方法包括：

接收包含所述网络识别符的数据包；

将所述数据包与多个模板进行比较；

将所述数据包的至少一部分与所述多个模板中的第一模板匹配；

至少部分地基于所述匹配结果，触发隔离功能以作出响应。

优选地，所述方法进一步包括：在本地执行所述隔离功能的至少一部分。

优选地，所述隔离功能的触发包括：发送请求给支持服务器以执行所述隔离功能的至少一部分。

优选地，所述方法进一步包括：基于与域名服务器的交互，更新所述多个模板中的所述第一模板。

优选地，所述方法进一步包括：将所述数据包的至少一部分与所述多个模板中的第二模板进行匹配，且基于与所述多个模板中所述第一模板以及第二模板的匹配结果，触发所述隔离功能以作出响应。

优选地，所述多个模板中的所述第一模板将所述网络识别符作为目标。

优选地，所述多个模板中的所述第一模板将与所述恶评内容相关的统一资源定位符的至少一部分作为目标。

本发明的其他优点、目的和新颖性特征，及其详细的图解说明，将在接下来的描述和图示中得到更充分的阐释。

### 附图说明

图 1 是根据本发明构建的通信架构的示意图，其中，中间数据包路径节点中断从已知的作为恶意程序源的主域路径地址、子域路径地址、整个服务器或者服务器群发起的数据包的路由，并结合外部服务器和/或服务器群执行隔离服务功能处理；

图 2 是图 1 的通信架构内的终端设备和中间数据包路径节点的功能框图；

图 3 是图 1 的通信架构的一个实施例的示意图，其中示出了终端设备、中间数据包路径节点和服务器或服务器群的细节；

图 4 是根据图 1 和图 3 构建的网络节点（交换机/路由器/ISPN/AP）的框图；

图 5 是另一网络节点（交换机/路由器/ISPN/AP）的框图，这种网络节点没有安装本发明的组件以与相邻节点交互来完成隔离服务功能处理；

图 6 是根据图 1 和图 3 构造的路由器的示意图；

图 7 是根据图 1 和图 3 构造的终端设备（服务器和/或客户端）的示意图；

图 8 是图 4、5 和 6 的网络设备的总的功能流程图；

图 9 是图 4、5 和 6 的网络设备执行的详细流程图；

图 10 是图 4、5 和 6 内的恶意程序识别电路的功能流程图。

### 具体实施方式

图 1 是根据本发明构建的通信架构的一个实施例的示意图，其中，中间数据包路径节点检测与以下已知源相关的数据包路由尝试：1) 恶意程序；2) 非法内容；或者 3) 非法传播。在检测到这些数据包时，中间数据包路径节点 109 调用隔离服务功能块。隔离服务功能块可包含在中间数据包路径节点、外部支持服务器或者服务器集群，以及源端设备或者目的端设备的一个或者多个中。不管隔离服务功能块存储在哪里，该隔离服务功能块选择性地包括但

不限于：发送消息给源端设备和/或目的端设备，向源端和/或目的端设备发送“人为口令”(human challenge)机制，中断或者放弃正在进行的数据包的传输。在本说明书中，术语“恶意程序”包括不想要的或者不适当的广告程序或者病毒文件等。“非法内容”包括国家的法律禁止的内容，例如赌博、儿童色情等。“非法传播”涉及其他的合法内容的未经授权传播，例如未经授权传播版权保护的材料。恶意程序、非法内容以及非法传播的内容在此统称为“恶评内容”(notorious content)。已知的和经常重复的恶意程序、非法内容以及非法传播的源在本说明书中称为“恶评源”。在本说明书中，术语“内容”的意思还包括“服务”，例如“恶评内容”包括“恶评服务”。

恶意程序还包括有病毒、蠕虫、特洛伊木马的程序代码，或者简单地是不想要的广告程序。这些恶意程序代码以它们破坏客户端设备 153 的正常功能为特征，例如使设备变慢，通过烦人的弹出窗口和广告干扰用户，将私人信息传输到设备外，改变用户对设备的设定，改变注册内容等。

为了识别恶评源，中间数据包路径节点使用多个模板与所接收的每个数据包进行比较。一些模板尝试识别单个恶评服务器，而其他模板尝试识别恶评服务器群。例如，另一些模板以单个文件为目标，例如基于 URL (统一资源定位符) 如 HTTP (超文本传输协议) IP 地址、路径或者文件名或者 FTP (文件传输协议) 地址、文件夹和文件名，这种以文件为目标的模板称为“路径文件模板”或者“以路径文件为目标的模板”。其它类型的模板尝试捕获指定路径的所有文件，例如，FTP 文件夹中的所有文件，或特定 HTTP 路径中的所有文件。在本说明书中，这种模板称为“路径模板”或者“以路径为目标的模板”。同样，某些模板以指定路径的所有文件为目标，包括子路径和子文件夹，这种模板称为“子路径模板”或者“以子路径为目标的模板”。

各种协议 (例如，FTP 和 HTTP) 都使用一系列步骤在一个设备与另一个设备之间建立连接，例如，在源端设备和目的端设备如服务器和客户端之间建立连接。作为这些步骤的一部分，标识 URL 的数据包通常是模板的目标。类似地，当仅知道域名时，要确定其 IP 地址，就使用 UDP (用户数据报协议) 与域名服务器联系。发送到域名服务器的数据包也是目标，这样，专用于匹



配域名的模板能够成功地进行匹配。其他模板构建用于以当前 IP 地址为目标（在 IP 地址随时间而变化时），这就要求通过使用域名访问域名服务器来进行至少周期性地更新。

模板至少以三种方式创建。第一，系统管理员通过人工接口创建模板。第二，基于之前的数据包有效载荷中检测到的恶评内容自动地（在或者不在系统管理员的干涉下）创建模板。第三，独立第三方（值得信赖的病毒检测公司、警察或者版权持有者）进行配合以添加模板（根据配置的情况，可在或者不在系统管理员的干涉下进行）。例如，已知的在国外合法地运营的赌博站点，当出站数据包（例如，目标设备的地址）落入特定国家时，该站点就是非法运营的。为了隔离这种非法运营，该特定国家的当局可以通过基于计算机通过因特网直接输入目标模板，或者请求系统管理员输入目标模板。例如，目标模板内容包括赌博站点的域名、赌博站点的 IP（因特网协议）地址、该特定国家内的客户端设备使用的 IP 地址范围。中间节点通过比较赌博站点的 IP 地址和数据包中的源地址或者目的地址，随后比较客户端设备的源地址范围或者目的地址范围，能够推断是否需要进行隔离。类似地，例如，通过匹配中间数据包路径节点，对已知的尝试自我传播的病毒进行重复检测。重复检测之后，尝试警告和帮助客户端设备的用户，或者服务器的管理员，隔离关联的客户端设备、服务器或者路径，以免必须匹配数据包有效载荷的内容模板。其他的恶评内容和恶评源也可进行类似的识别和隔离。

具体来说，因特网 107 中的多个中间数据包路径节点（或者称为中间节点或者中间路由节点）109 识别恶评服务器和恶评内容。在某些情况之下，例如服务器提供无价值的服务，那么，该服务器被标识为恶评服务器，导致在主模板和关联逻辑 111 中添加两个主模板。其中的第一模板用于匹配服务器的域名，第二模板用于匹配该服务器的 IP 地址。添加这些模板后，任何的中间数据包路径节点 109 在将所接收的数据包与其中任一个模板成功匹配后，将作出响应，触发本地隔离功能 115 或者远程隔离功能 117。

一个典型的例子涉及客户端设备 153 上的浏览器发送 UDP 数据包到域名服务器（DNS）141。在 UDP 数据包中，通过域名标识出恶评服务器，例如服

服务器群 151 中的服务器。这样的数据包通常包括有基于域名的 IP 地址请求。DNS 141 通常响应这些数据包，使用该域名查找当前注册的 IP 地址。域名和对应的当前 IP 地址 143 由 DNS 141 进行关联存储。但是，当一个中间数据包路径节点 109 接收到标识恶评服务器的域名的 UDP 数据包时，以该域名为目标的模板将相匹配，并触发隔离服务功能。

另一个例子涉及客户端设备 153 或者恶评服务器发送数据包，该数据包由一个中间数据包路径节点 109 接收。该中间数据包路径节点 109 使用恶评服务器的当前 IP 地址与该数据包的源地址或者目的地址进行匹配，并调用本地或者远程隔离功能做出响应。因为当前 IP 地址经常改变，所以通过使用对应域名与 DNS 141 进行交互，周期性地更新依赖于当前 IP 地址的模板。

当服务器提供恶评内容且尚未被指认为恶评服务器时（例如，服务器也提供一些有价值的内容，或者相关的内容提供商没有进行监管时），除了匹配上面提到的两个模板的至少一个模板之外，还使用与该服务器中的恶评内容内的名称和位置有关的其它模板。这些模板以文件夹路径、文件名、文件夹内容、子文件夹内容为目标。典型例子涉及使用 URL 的 TCP 或者 FTP 请求。进行这种请求的客户端设备 153 将识别出：1) 服务器的 IP 地址；2) 该服务器上到目标内容的文件夹路径；以及 3) 恶评内容的文件名。任何接收该数据包的中间数据包路径节点 109 将找到与该 IP 地址的匹配（在这种情况下，这还不足以触发隔离功能），且更重要的是，还匹配一个或多个文件夹路径的至少一部分以及恶评内容的文件名。这两种匹配一起促使接收数据包的中间数据包路径节点 109 触发本地或者远程隔离功能。

在某些情况中，创建的模板以非恶评服务器的恶评内容为目标，该目标可以是恶评内容的实际名字（文件名或者服务名）。该模板（或者其他关联的模板）也可以以完整的文件夹路径为目标。在某些情况中，有很多文件/服务路径都具有共同的根路径，模板可能仅仅以该根路径为目标，以确保捕获落入该根路径或者其下的任何子文件夹的任何内容。模板结构中也可以使用与搜索有关的通配符，例如“\*”或者“？”。能够以多种方式构造主和次级模板及其关联的逻辑，以充分地确定需要隔离功能。

本说明书所用的源地址表示主域路径文件 147、子域路径文件 149 以及全体服务器或者服务器群中的文件。就是说，源地址整体上或者局部上表示地址树结构的根，或者地址树结构的分支，帮助确定主域路径文件 147、子域路径文件 149、全体服务器或者服务器群中的文件。服务器 151 在运行时产生服务器页面 (server page)，或者基于请求传送预先构建的服务器页面，并还可使用恶意程序将令人讨厌的文件，页面或者其他恶评内容通过网络发送到客户端系统。

在识别出恶评服务器或者恶评内容之后，中间数据包路径节点 109 (以下简称中间节点) 触发本地或者远程隔离服务功能。该功能可针对特定恶评服务器或者恶评内容进行专门设计，或者可设计为服务于一个或所有类型的恶评服务器和恶评内容。典型的隔离功能包括：1) 临时或者永久的中断数据包传输；2) 与恶评内容的预期接收方通信；3) 与恶评服务器或者提供恶评内容的服务器进行通信；4) 在可能的情况下禁止恶评内容或者使恶评内容失效 (或者，至少提供这方面的功能)。所述通信通常包括：a) 人为口令机制以防止任何有关的恶意程序拦截用户接口以及隐藏通信；b) 告警消息；c) 标识恶评内容或者恶评服务器的性质；d) 清除客户端系统或者服务器系统中与恶评内容或者恶评服务器有关的任何内容；以及 e) 向客户端系统或者服务器系统提供免疫或者防护功能，例如防火墙等。

在应用隔离服务功能时，中间节点 109 获得支持服务器 169 的帮助，将具有源地址的数据包引导到支持服务器 169 以进行远程隔离处理。支持服务器 169 可独立地应用隔离功能，或者在中间节点 109 的支持下应用隔离功能。中间节点 109 通过应用与触发器关联的逻辑，确定是否应用本地和/或远程隔离功能。在该隔离处理中，客户端设备 151 也可提供帮助。例如，可以在网页浏览器或者在客户端设备 151 上运行的另一可靠程序代码中构建功能模块，支持与中间节点 109 或者支持服务器 169 内的隔离服务功能进行交互。例如，所述交互包括接收和显示隔离消息以及人为口令，以及帮助客户端设备 151 的清理应用程序和防火墙程序。

中间节点 109 可以是任何的将数据包从服务器 151 路由到客户端设备 153

的交换设备。例如，中间节点 109 可以是接入点、路由器或者数据分组交换设备。就是说，终端设备之间的路由路径包括个人接入点、服务提供商接入点、其他服务提供商设备以及多个骨干节点，所有这些都使用中间节点 109 表示。

在本发明的多数实施例中，中间节点 109 执行一系列活动。首先，中间节点 109 尝试识别恶评服务器以及恶评内容。其次，中间节点 109 尝试防止恶评内容对客户端设备 153 产生不利影响。第三，对于受到不利影响（以及通常被感染的）客户端设备，中间节点 109 尝试移除这种不利影响。第四，中间节点 109 中断与恶评服务器或者与恶评内容有关的数据包流。最后，中间节点 109 尝试从服务器系统中清除该恶评内容。

本地和/或远程隔离服务功能帮助服务器 151 清除恶评内容，例如，从主域路径文件 147、子域路径文件 149、整个服务器或者服务器群内文件中移除病毒或者恶意文件，或者移除所有的文件。类似的帮助还提供给客户端设备 153。为了移除或者净化一些恶评内容，可编写独立的应用程序，通过隔离服务的通信提供并允许下载这种应用程序。在其他一些情形下，提供文字说明以便用户或者系统管理员能够实施清除处理或者净化处理。作为隔离服务功能处理的一部分，中间节点 109 能够在提供/不提供给用户口令机制的情况下向服务器 151 和客户端设备 153 发送消息。这些消息可包括与恶意程序或者其他恶评内容有关的信息、警报、所进行的中断处理和帮助。这些消息能够在浏览器或者操作系统的帮助下以弹出窗口的形式向服务器 151 或者客户端设备 153 的用户显示。

为了识别出已知的恶意源的源地址，中间节点 109 包含有主模板和关联逻辑 111、次级模板和关联逻辑 113。主模板和次级模板包含有能够识别出表示主域路径文件 147、子域路径文件 149、整个服务器或者服务器群的文件的源地址的比特序列，采用数据库中的域名、IP 地址、DNS 句柄（即，域名）或者文件名的形式。这些模板帮助识别源地址。对于每个模板，都具有关联的逻辑，这些逻辑有效地将数据包引导到一个或多个隔离服务功能 115，或者引导到位于支持服务器 169 的外部隔离服务功能 171。除了主模板和关联的逻

辑 111、次级模板和关联的逻辑 113、隔离服务功能 115 之外，中间节点 109 也包括有通信应用程序 117，通信应用程序 117 产生具有人为口令机制的消息并将消息传输到服务器 151 或者客户端设备 153 的屏幕。模块 111、113、115、117 和 171 进行处理的一个实施里的详细描述将结合图 2 给出。要注意的是，所示的支持服务器 169 代表通信地连接到中间节点 109 的，处于相同位置的服务器，或者表示远程的外部提供商的服务器。

为了产生表示主域路径文件 147、子域路径文件 149、整个服务器或者服务器群中的文件的源地址的模板，中间节点 109 或者支持服务器 169 在接收到数据包时，识别其中的恶意程序或者其他恶评内容。恶评程序的特征是包括一个或者多个有效载荷比特序列，数据包中存储这种比序列则表示数据包有效载荷中至少存在一部分特定的恶意程序。恶意程序的另一特征是包括有与重复发布恶意程序的已知终端设备的地址相匹配的源地址。类似地，恶意程序的特征还包括相匹配的文件名文本序列或者其他有效载荷或辅助的数据包字段，至少部分的表示可能存在恶意程序。当来自服务器 151 的这种数据包达任何的中间节点 109 之时，将数据包内容与一个或多个主模板进行比较，如果出现了与恶意程序匹配，就应用关联的逻辑。如果在使用主模板比较时检测到存在恶意程序的可能性，就将数据包内容与次级模板进行比较并应用关联的逻辑，以此重复下去，直到得出结论为止。该数据包中的源地址以模板的形式存储并生成关联的逻辑。除了上述自动生成模板的方法，还可以手动产生模板，即通过收集与恶意程序有关的统计值并据此产生模板。

一旦识别出源地址，隔离服务功能 115 或者 117，结合通信应用程序 117 执行各种预定的任务。例如，通信应用程序 117 将发送警告给参与交换并继续传送数据包的两终端设备中的一方或双两。或者，也可以在有告警或者无告警的情况在丢弃该数据包。在识别出源地址后，与模板有关的逻辑将数据包引导到一个或多个隔离服务功能 115 或 171，接着该隔离服务功能 115 以逐步的方式执行多级处理中的一个或多个处理。例如，如果服务器 151 的侵犯是良性的，例如烦人的弹出广告，那么，就丢弃数据包，并将与服务器 151 有关的合适的警告消息发送到服务器 151 以及客户端设备 153。通常，这种网

页和弹出广告误导用户点击错误的按钮，用户不知道这种行为导致终端设备受恶意程序感染。对于这种低风险因素级，隔离服务功能块 115 或者 171 采用不太严格的行为，例如不允许下载网页，禁止某些方面的网页，或者禁止误导用户的弹出窗口，并可发送或不发送消息。

当服务器 151 尝试重复地发送恶意程序时，或者在恶意程序处于高风险级时，隔离服务功能块 115 的处理将采取严厉的措施，例如向服务器 151 发送警告消息，通知将中断路由，直到修复了恶意程序或者其他的恶评内容问题为止。这种警告消息也包括有与可用于修复该问题的帮助有关的信息。服务器 151 的用户能够下载隔离功能块，可从外部服务器 169 或者中间节点 109 获得的隔离功能块与消息一起，允许服务器 151 和客户端设备的用户自己学习以及修复恶意程序。这些下载的隔离功能块是可执行或可编译的代码，在用户接受的情况下发送到终端设备，可由操作系统或者网页浏览器运行。此外，在某些其它情况下，例如当恶意程序导致严重损坏客户端设备 153 的功能时，中间节点 109 使用已知的有益代码替换该恶意程序，并将它们传输到客户端设备 153，同时对服务器 151 采取一定的措施。另外，中间节点 109 采取的最大援助包括隔离服务器本身，也可以隔离服务器群。

通信应用程序 117 发送的消息包括有标题如“恶意程序警告”，以及有关该恶意程序的类型的简要描述，发送者和接收者的 IP 地址和/或域名、恶意程序类型、风险因素和其他一些细节。另外，该消息对中间节点 109 遇到的情况给出简要描述，例如“下载的网页/文件正在进行防恶意程序处理，请稍后……”；或者在检测到恶意程序时提示“对不起，该服务器是恶意程序源，不能下载网页和/或文件”，或者“正在发送到文件包含恶意程序……”。消息中也可以包括有与风险因素有关的信息，以及与源于该服务器 151 的恶意程序的行为有关的信息，例如“已经知道下列服务器发送：恶意程序 1<恶意程序类型和代码序号>：具有高风险因素，影响你的 PC 注册表，并可能使<一个或多个应用程序的有关行为>失效；恶意程序 2<恶意程序类型和代码序号>：具有中等风险因素，产生烦人的和误导用户的弹出窗口。”消息中有关的帮助可以是“要修复来自该服务器的恶意程序<恶意程序类型和代码序号>，请点

击下面的按钮”，点击该按钮将提供隔离功能下载或者将客户端设备 153 引导到另一个可下载的网站。对于其它类型的恶评内容，也提供类似的消息和有关的功能。

当恶意程序代码尝试自我复制或者尝试误导中间节点 109 时，通信应用程序将使用人为口令机制。人为口令包括几个数字或者字母，其方向与计算机上显示的文字、数字不同。人为口令机制期望自然人用户键入这些文字和数字的组合，并同意传输这些数据包。这个过程可允许传输具有相似文件名或者代码段但是未必是恶意的或者误导用户的数据包。通过人为口令机制，中间网络节点 109 在必要时还收集一些用户信息以进行进一步的处理。另外，中间节点 109 能够在提供人为口令机制的同时发送与恶意程序有关的消息、信息、警告以及帮助。与恶意程序有关的信息包括服务器（可以是一个服务器）、域名、IP 地址、恶意程序名称和代码、恶意程序的功能及其如何感染客户端设备、与服务器及恶意程序有关的统计值、以及可用于修复该恶意程序的方法。

例如，根据中间节点 109 收集的统计数据对服务器 151 定级为在处理恶意程序代码方面是弱的。存储在中间节点 109（支持服务器 169）处的统计数据既可以通过各种用户的反馈来收集，也可以通过分析服务器的恶意程序侵害的数量来收集。其他的分析和定级服务器的统计方法也是可行的。

发送到客户端设备 151 的带有人为口令机制的信息还包括用户针对服务器 151 进行反馈的规定，将用户引导到有用的站点的链接，如何在客户端设备设置浏览器应用程序以进行后续的恶意程序防护的信息。或者，在获得人为口令的响应时，中间节点 109 将浏览器引导到一个或多个提供必须信息的站点，该信息教导用户并提供修复恶意程序的帮助。但是，如果中间节点 109 明确地确定服务器 151 发送包含恶意代码和破坏性代码的数据包，那么，中间节点 109 将阻止这种传输并做出合适的响应，例如中断后续来自服务器 151 的数据包的路由，同时可使用或者不使用上面提到的人为口令机制、信息和警告。

中间节点 109 为了执行上述的隔离处理，如果数据包是加密的则解密数



据包，并调用本地的或者远程的服务来进行解密处理。另外，中间节点 109 通过一定方式完成隔离处理没，以便不在从服务器 151 到客户端设备 153 的通信路径重复这些处理。这一无重复处理通过在隔离处理完成以后，在数据包中添加比较表版本代码 (comparision table version code) 来完成。所述比较表版本代码包含有与该数据包比较的主模板和次级模板有关的信息、与之前节点对该数据包使用的隔离服务功能有关的信息。比较表版本代码包含的信息包括模板版本、相关逻辑的版本、本地隔离服务功能版本以及应用的本地或者远程隔离服务功能。例如，如果通信路径中的任何节点包括有增强的或者最新版的模板，该节点可决定仅仅需要比较那些增强的模板。类似的约束也可应用到相关逻辑和隔离服务功能块上。

如果数据包中没有比较表版本代码，那么，执行处理的中间节点可确定之前的节点没有对该数据包进行过分析。反之，如果存在有比较表版本代码，那么，执行处理的中间节点对该比较表版本代码进行解码，以确定之前已经发生的隔离处理。接着，如果还需要进一步的隔离处理，则仅仅进行所需的隔离处理。

如果到达该中间节点的数据包是经过加密的，且表明需要进一步的分析，那么，网络节点先执行数据包的解密。虽然公钥可从服务器 151 或者客户端设备 151 获得，但是仅有客户端设备 153 知道私钥。虽然隔离处理的描述仅仅示出了一种可能的实施例，但是本发明不局限于所描述的实施例。

图 2 是图 1 所示通信架构中的中间数据包路径节点 221、终端设备 207、233 功能框图 205。具体来说，当服务器 207 (也可以是服务器群) 发送数据包 211 到因特网时，一个或者多个中间数据包路径节点 221 开始进行一系列分析 223 和处理。成功完成分析和处理 (以后简称隔离处理) 的数据包连同消息一起被发送到客户端设备 233，客户端设备 233 可以是个人计算机、手持设备或者电话。或者，在分析过程 225、227 中，通过检测到源地址发送具有恶意程序或者其他恶评内容的数据包时，隔离处理 229 引起一系列动作，例如丢弃该数据包、发送消息和隔离该服务器 207。

在中间节点 221 上对到达的数据包进行分析时，首先使用多个主模板与



数据包内容进行比较。通过这种主模板比较 225, 中间节点 221 确定服务器的源地址。出现匹配时, 中间节点 221 应用与该主模板有关的逻辑 225。接着逻辑 225 又引起次级模板比较 227, 使用选择的一组次级模板与数据包内容进行比较。接着, 应用与次级模板有关的逻辑。次级模板比较以及相关逻辑的应用过程重复执行, 直到作出关于源地址传播恶意程序或者恶评内容的结论为止。

一旦确定源地址为恶意程序或者其他恶评内容传播源, 就开始进行隔离处 229。在这里, 应用隔离服务功能处理。另外, 中间节点 221 在项目表中插入隔离状态, 所述项目表包括有主域路径地址 265、子域路径地址 275、整个服务器或者服务器群的地址、站点路径、风险因素等。通常, 这种项目表包括: (a) 表示主语路径地址的源地址; (b) 表示子域路径地址的源地址; (c) 表示单个服务器的源地址; (d) 表示具有多个地址的整个物理服务器的源地址; (e) 与源端设备的有关的通信路径; (f) 恶意程序的风险级别指示; 以及 (g) 隔离状态指示。另外, 项目表中的隔离状态是可编辑的, 可由系统管理员或者通过与可靠第三方 (例如恶意程序清除公司的雇员、警察或者其他权威人士) 进行软件交互来添加新条目。

隔离状态指示还导致一系列动作, 包括但不限于: (a) 改变或者丢弃数据包; (b) 向终端设备 207、233 发送合适的带有人为口令机制的警告、信息或者相关帮助消息; (c) 中断到服务器 207 的路由服务; (d) 提供帮助给终端设备 207、233 修复恶意程序; 以及 (e) 引导用户到提供附加信息和帮助的站点。或者, 如果中间节点 221 上的隔离服务功能不可用, 就将数据包引导到支持服务器 215, 以进行外部隔离服务功能 217 处理。也可以使用支持服务器 215 上可用的其他外部服务功能 219。终端设备 207、233 可包括有其它能够执行或者编译下载的 QFD (隔离功能下载)、CP (通信路径) 和 CA (通信应用程序) 的软件组件, 例如 BA (浏览器应用程序)。通信应用程序能够在屏幕上显示消息以及人为口令, 例如不需要浏览器的弹出窗口。

图 3 是图 1 所示的通信架构的一个实施例的示意图 305, 其中示出了终端设备、中间数据包路径节点以及服务器或服务器群的其他细节。根据本发明,

骨干网 313 内的中间交换/路由节点 307 到 310 包含恶意程序识别系统 (MIS) 315、316 以及隔离服务功能块 (QSF) 325、326。QSF 帮助检测发送恶意程序的服务器以及执行隔离处理。类似地, 其他中间接点如个人接入点 (PAP) 335、接入点 (AP) 337、339、因特网服务提供商网络 341、343 和 345 也包含有恶意程序识别系统 (MIS) 317 到 322 以及隔离服务功能块 (QSF) 327 到 332。下面将结合图 4、5 和 6 的对构成恶意程序识别系统 315 到 322 的功能模块进行详细描述。

另外, 如图所示, 支持服务器 393 通信地连接到一个或多个中间节点 309 到 310, 支持服务器 393 提供附加的外部隔离服务功能 395, 并向交换/路由节点 307 到 310 增加隔离处理能力。这些支持服务器 393 表示通信地连接到中间接点的、位于相同位置的服务器, 或者表示远程的外部提供商的服务器。

终端设备包括服务器 351、个人计算机 353 或者个人电话机 355。终端设备使用中间接点 307 到 310、335、337、339、341、343 以及 345 的网络服务来交换数据、音频或者视频数据包。这些终端设备 351、353 以及 355 还包括有下载的 QFD (隔离功能下载) 369 到 371、CP (通信路径) 361 到 363 以及 CA (通信应用程序) 365 到 367。这些软件组件帮助中间节点 307 到 310、335、337、339、341、343 和 345 进行隔离处理, 如上面结合图 1 和 2 所述。

图 4 是根据图 1 和图 3 的实施例构建的网络节点 (交换机/路由器/ISPN/AP) 407 的示意图 405。另外, 附图示出了通信路径 455, 通信路径 455 通信地连接网络节点 407 和相邻节点 467, 节点 467 具有类似的隔离处理能力。网络节点电路 407 表示任何的路由数据包的因特网节点, 网络节点电路 407 可部分地或者全部地结合到任何的网络设备中, 例如交换机、路由器、ISPN 或者接入点。网络节点电路 407 通常包括处理电路 409、本地存储器 417、管理接口 449 和网络接口 441。这些组件互相之间通过一个或多个系统总线、专用的通信路径, 或者其他直接的或者间接的通信路径通信地连接。在各种实施例中, 处理电路 409 可以是微处理器、数字信号处理器、状态机、专用集成电路、现场可编程门阵列、或者其他类型的电路。处理电路 409 通信地连接到编码/加密管 411、解码/解密管 413 以及恶意程序识别电路 415。这些硬

件组件 411、413 和 415 可以是硬布线的，以提高隔离处理和路由的速度。

本地存储器 417 可以是随机存取存储器、只读存储器、闪存、硬盘驱动器、光学驱动器，或者是其它类型的能够存储计算机指令和数据的存储器。本地存储器 417 包括服务模块管理器 (SMM) 419，通过将包头内容和负载内容与合适的模板进行比较来分析进站数据包。这些模板以及有关的逻辑包括主模板和相关逻辑 421、次级模板和相关逻辑。如果在主模板比较过程中发现了匹配，有关的逻辑 421 将数据包引导到选定的次级模板组进行进一步的分析，在次级模板比较之后，就应用与次级模板有关的逻辑。这一过程重复执行直到得出结论为止。然后，应用合适的隔离服务功能 425 或者远程隔离服务功能。通信应用程序 427 允许在屏幕上显示消息和人为口令，例如在不需要浏览器的情况下弹出窗口。

另外，网络接口 441 包括有线和无线数据包交换接口 445、有线和无线电路交换接口 447。进一步地，网络接口 441 也可以包括内置的或者独立的接口处理电路 443。网络接口 441 允许网络设备与其他的网络设备进行通信，允许处理电路 409 接收和发送数据包，该数据包可能包括恶意程序代码序列。另外，当本地上的这些功能无法使用时，网络接口 441 能够使用外部的隔离服务功能以进行分析和处理。管理接口 449 包括显示器和键盘接口，这些管理接口 449 允许进行网络交换的用户控制本发明所述的系统。

在其他的实施例中，本发明的网络节点 407 具有比附图所示的更少的或者更多的组件，以及更少的或更多的功能。换句话说，所示的网络设备仅仅是提供一种根据本发明的可能的功能和构造的实施例。图 5 和图 6 描述了网络节点的其他可能实施例。

网络节点 407 通过通信路径 455 通信地连接到外部网络设备，例如相邻节点 467 或者支持服务器（未示出）。相邻节点 467 也由本发明的组件组成，例如恶意程序识别电路 477、SMM（服务模块管理器）479、PT & AL（主模板及有关的逻辑）481、ST & AL（次级模板和有关的逻辑）487。另外，相邻节点 467 可能具有网络节点 407 的其它组件例如加密管和解密管（未示出）。

网络节点 407 通过将数据包内容与多个主模板进行比较，来开始进行分

析。节点 407 通过这种主模板比较确定数据包中的源地址是否是任何已知的发送恶意程序的服务器。出现匹配时，节点 407 应用与主模板有关的逻辑。这一操作进而引出次级模板比较，将数据包包头内容和有效载荷内容与选定的次级模板组进行比较。接着，应用与次级模板有关的逻辑。次级模板比较以及应用有关的逻辑的过程重复进行，直到得出关于源地址的结论为止。一旦确定源地址是已知的发送恶意程序的服务器，就开始隔离处理。在这里，通过使用本地上可用的隔离服务功能 425 或者将数据包引导到相邻节点 467 使用外部隔离服务功能（QSF）如 QSF 485，对该数据包应用隔离服务功能。另外，节点 407 在项目表中插入隔离状态指示，该项目表包括全部的 IP 地址或者具有多个 IP 地址的全部的物理服务器。站点路径、风险因素等。隔离状态指示包括改变或者丢弃数据包、向终端设备发送具有用户口令机制的警告、信息或者帮助相关消息，以及向终端设备提供帮助以修复恶意程序。或者，如果节点 407 上的隔离服务功能不可用，就将数据包引导到外部提供商的服务器以进行外部隔离功能处理。

图 5 是没有安装本发明的组件以与相邻节点 567 进行交互以完成隔离服务功能处理的网络节点（交换机/路由器/ISPN/AP）507 的示意图 50。网络节点 507 可以是传统老式（legacy）设备，网络节点 507 包括处理电路 509、网络接口 515 以及本地存储器 517。该节点 507 通过通信路径 595 通信地连接到相邻节点 567。相邻节点 567 包含有至少图 4 所示的本发明的一些组件。图 5 所示的相邻节点 567 包括处理电路 569、本地存储器 577、管理接口 559 和网络接口 551。相邻节点 567 的硬布线组件包括编码/加密管 571、解码/解密管 573、恶意程序识别电路 575。另外，网络接口 551 包括有线和无线数据包交换接口 555、有线和无线电路交换接口 557。网络接口 551 也可以包括内置的或者独立的接口处理电路 553。本地存储器 577 包括服务模块管理器（SMM）579、隔离服务功能块 585 和通信应用程序 587。

但是，网络节点 507 没有安装本发明的任何组件，但包括有服务模块管理器 521。当数据包到达节点 507 时，服务模块管理器 521 使用封装指令将数据包引导到相邻节点 567，以对数据包进行隔离处理并将数据包返回到节点

507。相邻节点 567 按照图 4 中关于节点 407 所述的方式对数据包进行隔离处理，并将数据包返回给节点 507。接着，节点 507 向目的端设备路由该数据包。因此，网络节点 507 通过仅仅将数据包引导到相邻节点 567 来完成数据包的隔离处理，并接收处理后的数据包。

图 6 是根据本发明的图 1 和图 3 构建的路由器 675 的示意图 605。路由器 675 可以是分组交换器或者接入点。例如，路由器电路 675 可以指图 3 所述的骨干网 313 中任何的网络节点。路由器电路 607 通常包括通用主处理卡 655、交换器 609 以及多个线卡 615 和 618。在某些实施例中，线卡 615 和 618 可以不同。

第一线卡 615 包括网络接口 625，网络接口 625 能够与有线和无线网络例如 10Mbit、1000Mbit 以太网和 5Gbit DWDM（密集波分复用）光纤网交互。第一线卡 615 也包括交换接口 645，交换接口 645 允许线卡与互连交换器 609 进行交互。此外，第一线卡 615 包括次级处理电路 635，次级处理电路 635 在互连交换器 609 路由数据包之前对数据包进行预处理。次级处理电路 635 包括转发引擎 637 和路由缓存。次级处理电路 635 除了预处理数据包之外，也包括有 PT & AL（主模板和有关的逻辑）641。进站数据包首先与主模板进行比较，并应用有关的逻辑。如果出现了匹配，就是用本地可用的隔离服务功能 639 来处理数据包。

通用主处理卡 655 还包括核心主处理电路 657，核心主处理电路 657 通信地连接到编码/加密管 659 和解码/解密管 661。通用主处理电路 655 也包括有服务模块管理器（SMM）665、SP & AL（附加模板及有关的逻辑）667 和 QSF（隔离服务功能块）669。在第一线卡 615 引导下，服务模块管理器 665 结合 SP & AL 667、QSF 669 执行次级隔离分析和处理。

服务模块管理器 665 通过比较进站数据包有效载荷和 SP & AL 667，并应用附加模板的相关逻辑所指示的合适的隔离服务功能 669，来执行源地址检测和处理功能。隔离服务功能处理涉及在检测到源地址时向对应的终端设备发送具有人为口令的消息。该消息可以是在终端设备的显示器上显示的弹出消息，例如在个人计算机、服务器或者如图 3 所述的电话机上显示。该消息包

括标题例如“恶评内容警告”、恶意程序的简要描述、发送方和接收方的 IP 地址、恶意程序类型、风险因素以及其他的一些细节。另外，SP & AL 667 和 QSF 669 可为外部提供商的模板以及隔离服务模块提供存储空间。

图 7 是根据本发明的图 1 和图 3 的实施例构建的终端设备（服务器和/或客户端）707 的示意图 705。终端设备电路 707 可以是发起或接收可能经过加密或未经加密、可能包含恶意程序或其它恶评内容的数据包的任何设备电路。终端设备电路 707 可以部分或全部地结合到图 1 和图 3 所述的任何的终端设备中。终端设备电路 707 通常包括处理电路 709、本地存储器 715、用户接口 731 以及网络接口 755。这些组件通过一个或多个系统总线、专用通信路径、或者其他直接的或者间接的通信路径通信地互相连接。在某些实施例中，处理电路 709 可以是微处理器、数字信号处理器、状态机、专用集成电路、现场可编程门阵列，或者其他处理电路。

网络接口 755 包括有线和无线数据包交换接口 759、有线和无线电路交换接口 761。网络接口 755 还包括内置的或者独立的接口处理电路 757。网络接口 755 允许终端设备与其他的终端设备通信。用户接口 731 包括显示接口和键盘接口。

本地存储器 715 可以是随机存取存储器、只读存储器、闪存、硬盘驱动器、光学驱动器，或者是其它类型的能够存储计算机指令和数据的存储器。本地存储器 715 包括有通信路径 717、通信应用程序 719 以及隔离功能下载软件 723。另外，本地存储器 715 可包含有浏览器应用程序 729 以及操作系统 725 和浏览器 727。浏览器应用程序 729 能够执行或者编译所下载的隔离功能下载软件 723，隔离功能下载软件 723 帮助用户了解恶意程序有关的内容以及修复恶意程序有关的问题。当网络节点在发起于或者目的地为终端设备电路 707 的数据包中检测到恶意程序代码片段时，网络节点可用这些下载软件 723。通信应用程序 719 允许消息和人为口令在屏幕上显示，例如不需要浏览器的弹出窗口。

在其它实施例中，本发明的终端设备电路 707 可包括更少的或者更多的组件，以及更少的或更多的功能。换句话说，所示的终端设备仅仅是提供一

种根据本发明的可能的功能和构造的实施例。

终端设备 707 通过网络 775 通信地连接到外部网络设备, 例如远程设备 781。外部网络设备 781 也包括有本发明的组件例如处理电路 783 和本地存储器 795, 本地存储器 795 包括本发明的功能模块如服务模块管理器 785 和 PT & AL 787、ST & AL 789、QSF 791 和 CA 793。服务器或客户端通常通过互相之间交换数据包来进行通信。这些数据包可能有意地或者无意地包含恶意程序代码片段。网络节点如远程设备 781 检测到源地址时, 网络节点会采用多个可能的步骤之一。这些可能的步骤包括改变或丢弃数据包, 向终端设备发送具有人为口令机制的合适的警告、信息或者帮助相关消息, 提供帮助给终端设备修复恶意程序。这些功能通过远程设备 781 的组件 785、787、789、791 和 793 结合终端设备电路 707 的组件 717、719、721、723、725、727 和 729 一起工作来实现。

图 8 是图 4、图 5 和图 6 所示网络设备处理恶意程序时的典型方法流程的流程图 805。尽管针对的是恶意程序, 该方法流程也适用于所有类型的恶评内容。具体来说, 在步骤 811 中, 网络设备通过网络接口接收路由的数据包。在下一步骤 813 中, 网络设备将该数据包与主模板进行比较, 并应用相关逻辑。该主模板包括包头模板和有效载荷模板。当数据包到达该网络设备时, 将该数据包与主模板进行比较。若该数据包与目标为恶评服务器的源地址的主模板之间存在匹配, 那么将立即触发隔离服务功能。若该来源并非恶评的, 而仅仅包含有恶评内容, 那么将在步骤 815 中将其与次级模板进行匹配。在此, 网络设备在相匹配的主模板的相关逻辑的指引下, 将该数据包与至少一个次级模板进行比较。若没有出现匹配, 继续与剩下的其它次级模板进行比较。若该数据包与至少一个次级模板之间确实存在匹配, 便可得出结论为, 该数据包与恶评内容相关。

为了对该匹配作出响应, 在下一步骤 817 中, 应用所选择的隔离服务功能处理。换句话说, 一旦该源地址被证实为发送恶意程序或与恶评内容相关的地址, 即启动该隔离处理。该步骤中, 可利用本地隔离服务功能和/或远端隔离服务功能来应用该隔离服务功能处理。



然后，在下一步骤 819 中，网络设备在项目表中插入隔离状态符，该项目表包含主域路径地址、子网域路径地址，以及整个服务器或者服务器群的地址、站点路径、风险因素等等。一般而言，该项目表可包括：(a) 代表主域路径地址的源地址；(b) 代表子域路径地址的源地址；(c) 代表单个服务器的源地址；(d) 代表具有多个地址的整个物理服务器的源地址；(e) 与源端终端设备相关的通信路径；(f) 恶意程序的风险级指示符；(g) 隔离状态指示符。该隔离状态指示符进一步通过网络设备引导一系列操作，可包括修改或丢弃数据包，发送带有人为口令机制的合适的警告、信息或帮助相关消息，中断路由服务，提供帮助给终端设备修复恶意程序，以及将用户引导到提供附加信息和协助的站点。然后，若在该隔离状态指示符中作出指示，则在步骤 821 中将该数据包向目的端终端设备路由。

上述内容提及的“与模板进行匹配”实际上是指，与该模板相关的逻辑进行匹配。例如，若该模板找到相关性，那么逻辑则指示成功匹配；或者，若该模板没有找到相关性，则指示结果相反。逻辑还可能会更加复杂，例如，需要与主模板和第一次级模板之间存在相关性，同时与第三次级模板之间没有相关性。该流程图仅为本发明可能的流程图中的一个简要示例。

图 9 是图 4、图 5 和图 6 所示网络设备在一个实施例中更为详细的功能流程图 905。该网络设备的详细功能从步骤 907 开始执行。在步骤 909 中，该网络设备通过网络接口接收路由过来的数据包，并将其引导至验证管理器单元。该验证管理器验证是否已由在源端和目的端设备之间的通信路径内参与数据包路由的在先节点执行了隔离处理。在下一判断步骤 913 中，该网络设备决定是否指示有任何进一步的分析。如果没有，该网络设备则在步骤 933 中路由该数据包，且其功能在下一步骤 935 中结束。

若在判断步骤 913 中，验证管理器决定有必要进行进一步的处理，则在下一步骤 915 中，数据包被引导至编码/加密管中。在下一判断步骤 917 中，该编码/加密管确定数据包是否经过加密，若是，则在下一步骤 919 中，网络设备接收对应的密钥并对该数据包进行解密。如果判断步骤 917 的结果是该数据包没有经过加密，网络设备则转为执行步骤 919。在下一步骤 921 中，网



络设备通过将包头内容及有效载荷内容与主模板及次级模板进行比较，从而分析该数据包，并应用相关逻辑。

在下一判断步骤 923 中，网络设备确定在主模板及次级模板的比较过程中是否存在匹配，若没有发现存在匹配，网络设备将在步骤 933 中路由该数据包，并在下一步骤 935 中结束其功能。若在步骤 923 中发现存在匹配，则在下一步骤 925 中，网络设备应用隔离服务功能，或者将该数据包引导至外部设备中进行隔离功能处理。在下一步骤 927 中，网络设备在项目表中添加隔离状态指示符。在下一步骤 929 中，网络设备根据该项目表中的隔离状态指示符发送警告消息至服务器。然后，该网络设备执行隔离状态指示，包括在下一步骤 913 中，中断路由任何来自相关 IP 地址（即，主域路径地址、子域路径地址、整个服务器或服务器群的地址）的数据包。然后，在下一步骤 933 中，若隔离状态给出指示，则网络设备路由该数据包，并在下一步骤 935 中结束其功能。

图 10 是图 4、图 5、图 6 所示网络设备在一个实施例中其恶意程序识别电路的功能实现图。该恶意程序识别电路（MIC）的功能可扩展为能够识别任何种类的恶评内容，其从步骤 1007 开始执行。在步骤 1009 中，该恶意程序识别电路从服务模块管理器（SMM）中接收数据包。在步骤 1011 中，该恶意程序识别电路识别由服务模块管理器所检测到的源地址，并将该源地址添加到项目表中。在下一步骤 1013 中，该恶意程序识别电路在该项目表中插入隔离状态指示符，该项目表的输入内容可能包括主域路径地址、子域路径地址、整个服务器或者服务器群的地址、站点路径以及其他条目之间的风险因素。

然后，在下一步骤 1015 中，该恶意程序识别电路根据该隔离状态指示符的指示，向源端设备的用户发送带有人为口令的警告消息，并接收响应。在下一步骤 1017 中，该恶意程序识别电路将该数据包发送至另一个单元进行路由。若没有指示进行进一步的路由，该恶意程序识别电路丢弃该数据包，并提供帮助给该远端设备修复恶意程序，以及中断对来自源地址的数据包的进一步路由，直至问题被解决。然后在下一步骤 1019 结束其功能。

本领域普通技术人员可知，本申请中所使用的短语“通信连接”包括有

线的和无线的、直接的连接和通过其它组件、元件或模块的间接连接。本领域普通技术人员还可知，推定连接（即推定一个部件与另一个部件连接）包括两个部件之间与“通信连接”方式相同的无线的和有线的、直接的和间接的连接。

本发明通过借助方法步骤展示了本发明的特定功能及其关系。所述方法步骤的范围和顺序是为了便于描述任意定义的。只要能够执行特定的功能和顺序，也可应用其它界限和顺序。任何所述或选的界限或顺序因此落入本发明的范围和精神实质。

本发明还借助功能模块对某些重要的功能进行了描述。所述功能模块的界限和各种功能模块的关系是为了便于描述任意定义的。只要能够执行特定的功能，也可应用其它的界限或关系。所述其它的界限或关系也因此落入本发明的范围和精神实质。

本领域普通技术人员还可知，本申请中的功能模块和其它展示性模块和组件可实现为离散组件、专用集成电路，执行恰当软件的处理器和前述的任意组合。

此外，尽管以上是通过一些实施例对本发明进行的描述，本领域技术人员知悉，本发明不局限于这些实施例，在不脱离本发明的精神和范围的情况下，可以对这些特征和实施例进行各种改变或等效替换。本发明的保护范围仅由本申请的权利要求书来限定。

本专利申请参考并引用以下专利申请：

申请日为 2006 年 5 月 5 日的美国专利申请 No. 11/429,477，名称为“PACKET ROUTING WITH PAYLOAD ANALYSIS, ENCAPSULATION AND SERVICE MODULE VECTORING” (BP5390)；

申请日为 2006 年 5 月 5 日的美国专利申请 No. 11/429,478，名称为“PACKET ROUTING AND VECTORING BASED ON PAYLOAD COMPARISON WITH SPATIALLY RELATED TEMPLATES” (BP5391)；

申请日为 2006 年 7 月 20 日的美国专利申请 No. 11/491,033，名称为“SWITCHING NETWORK EMPLOYING VIRUS DETECTION” (BP 5457)；

申请日为 2006 年 6 月 23 日的美国专利申请 No. 11/474,033, 名称为 “INTERMEDIATE NETWORK NODE SUPPORTING PACKET ANALYSIS OF ENCRYPTED PAYLOAD” (BP5458);

以及申请日为 2006 年 8 月 18 日的美国专利申请 No. 11/xxx,xxx, 名称为 “SWITCHING NETWORK EMPLOYING ADWARE QUARANTINE TECHNIQUES” (BP5524)。

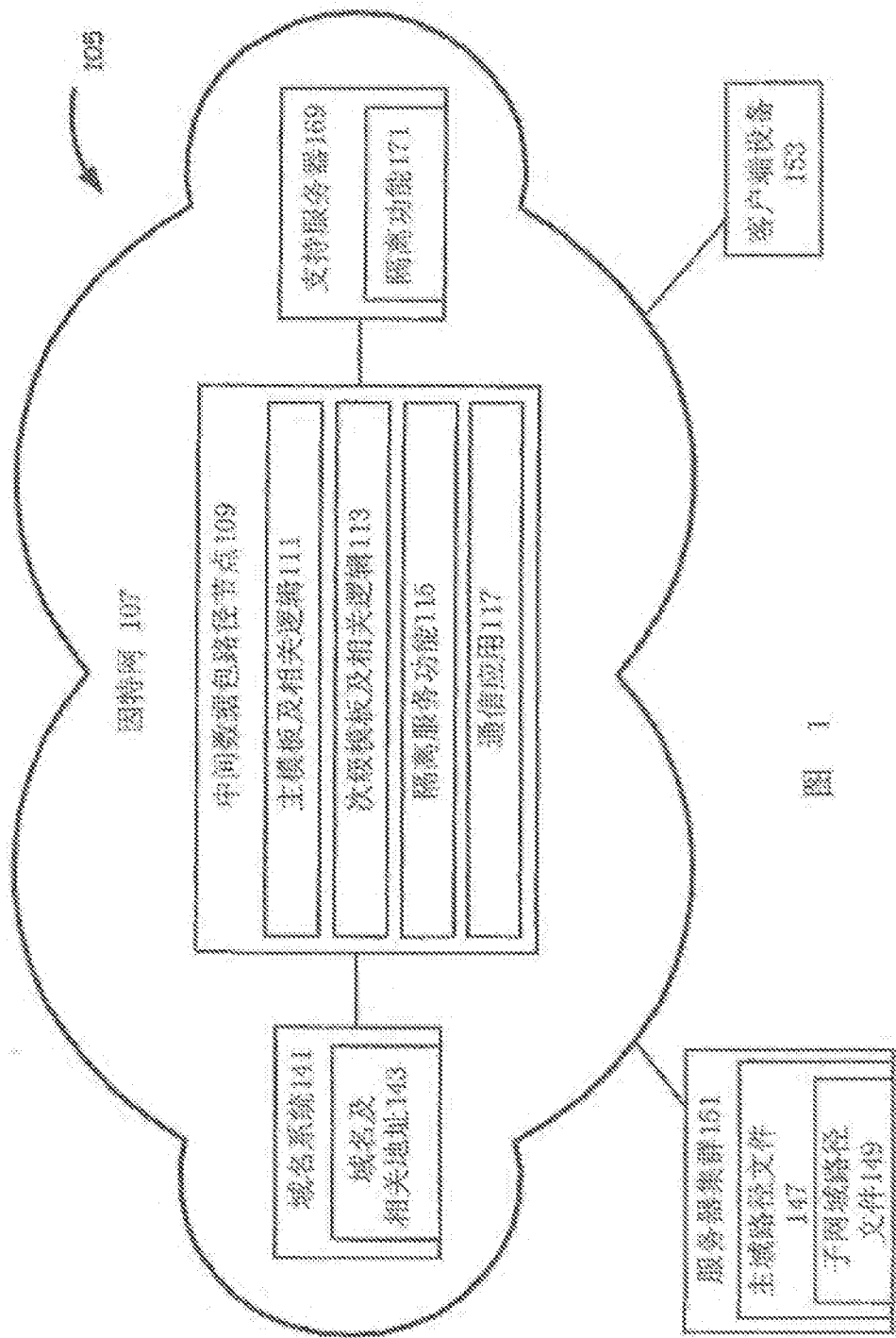


图 1

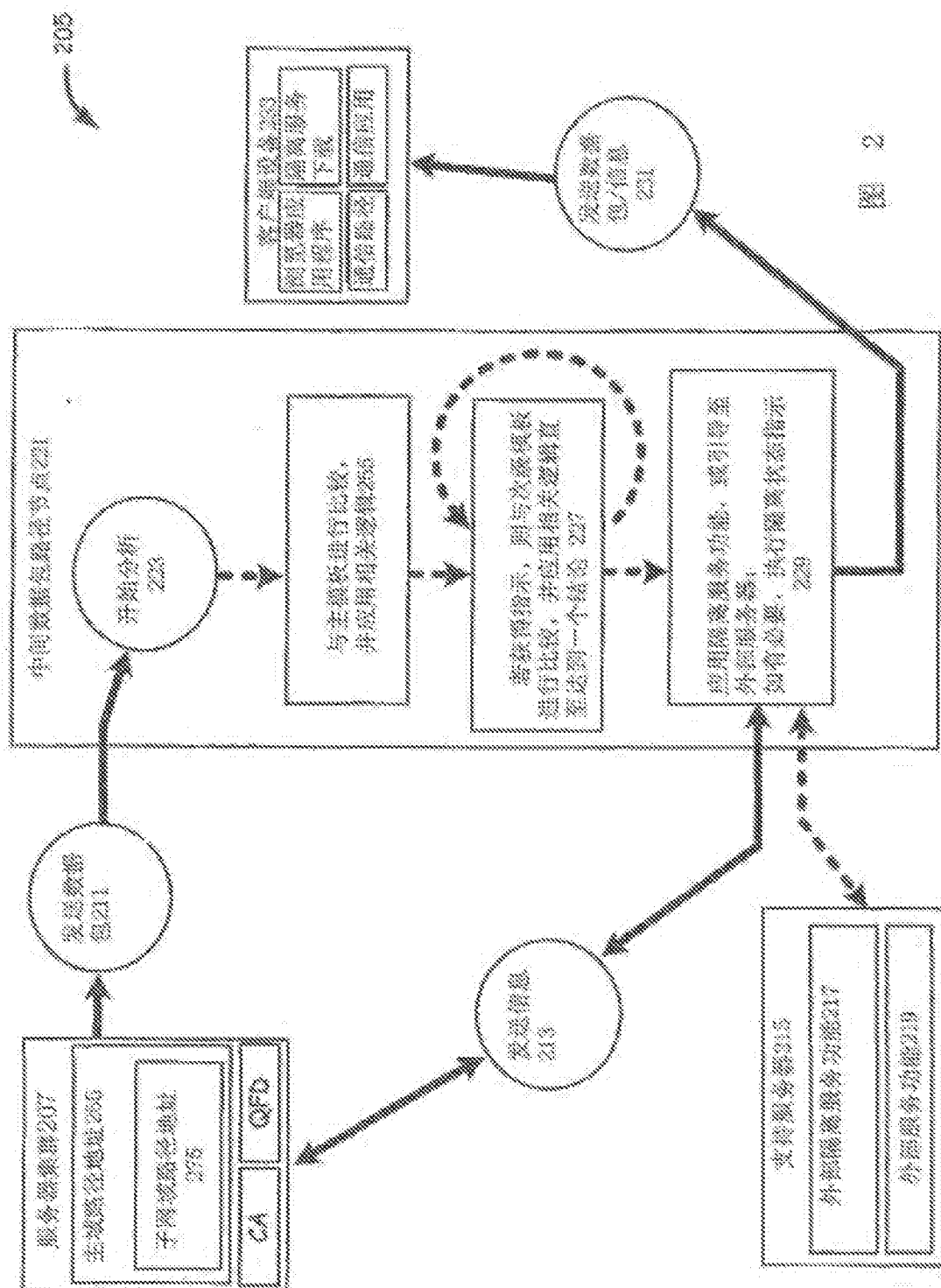


图 2

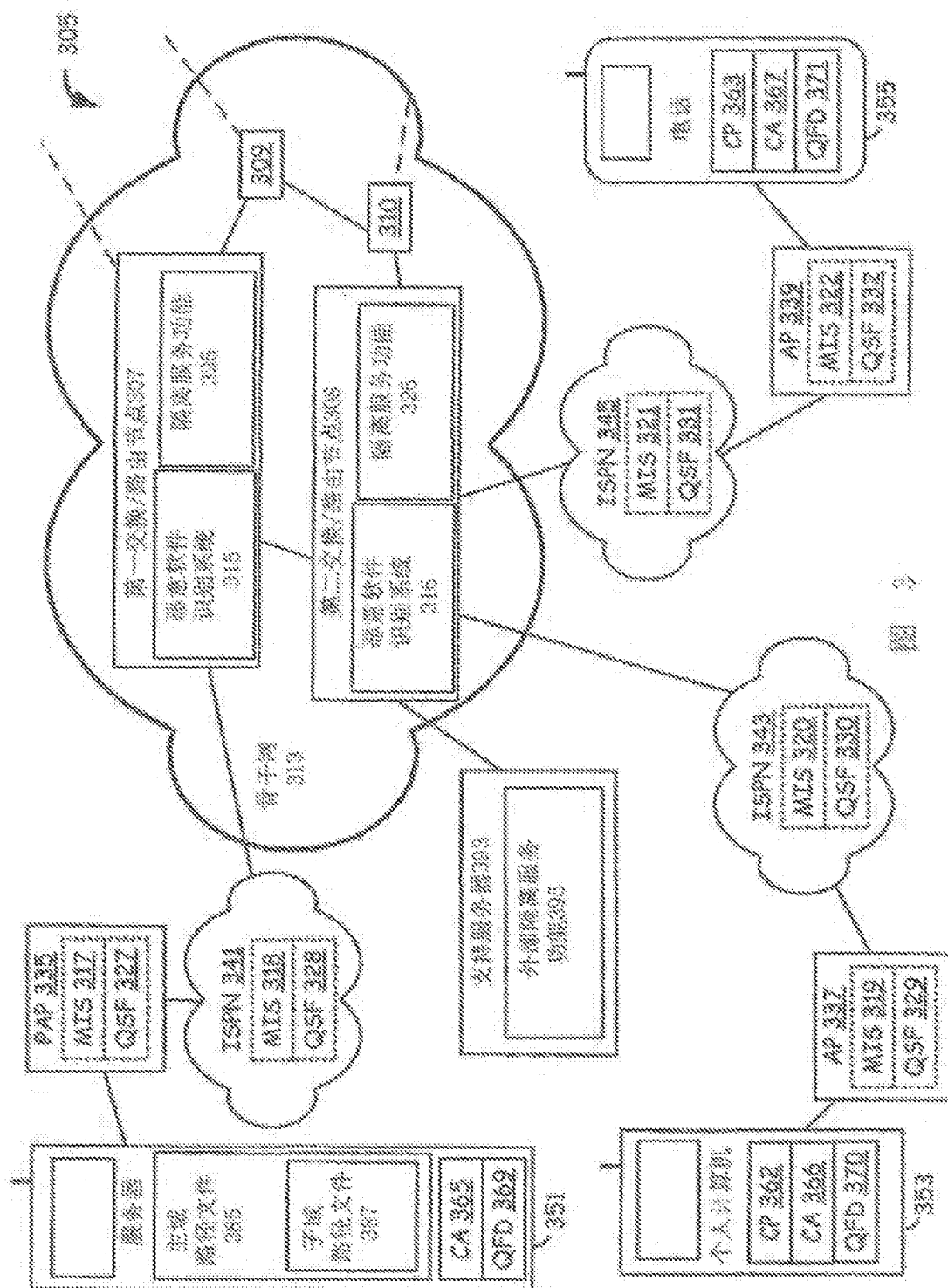


图 3

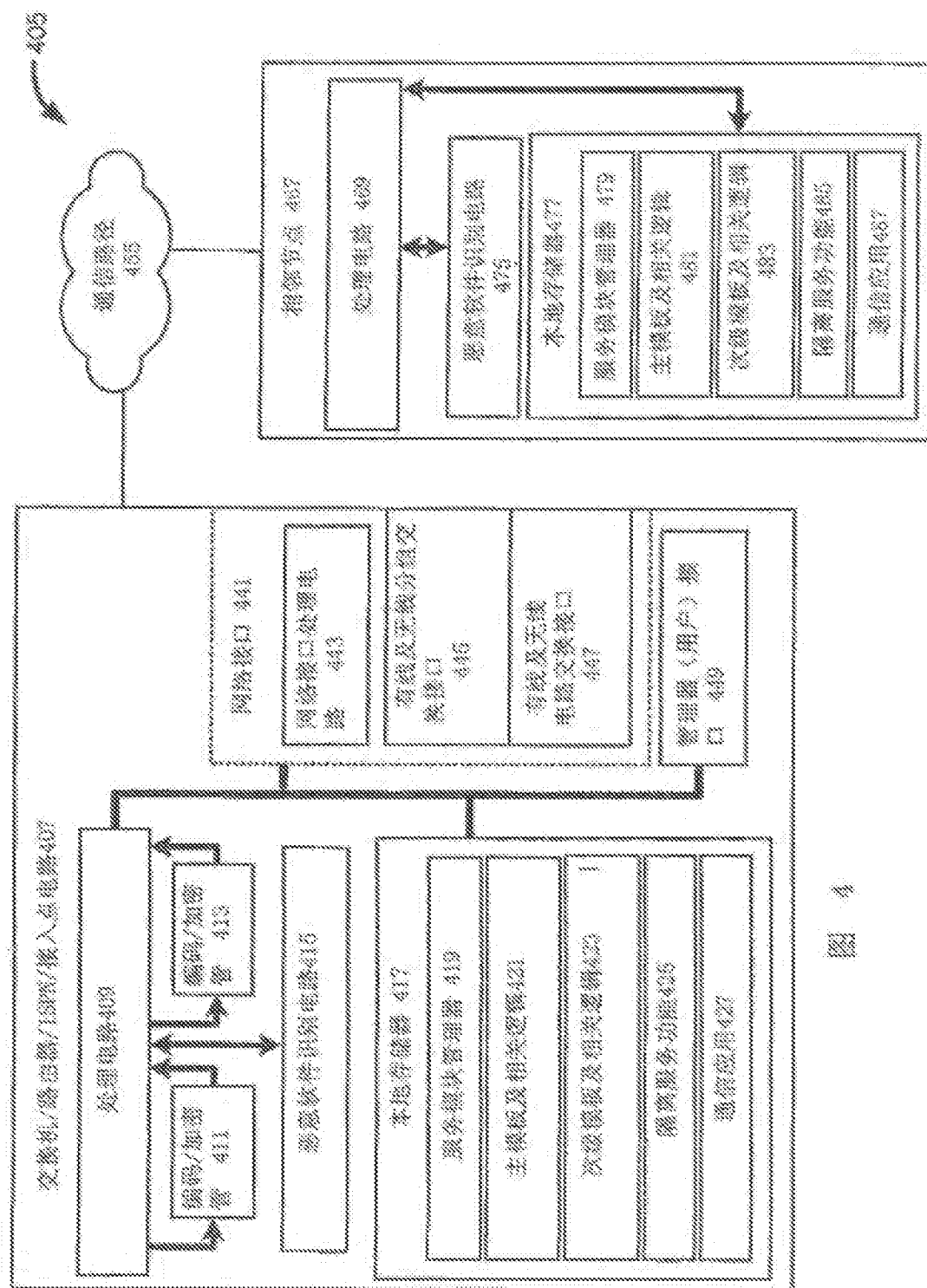


图 4

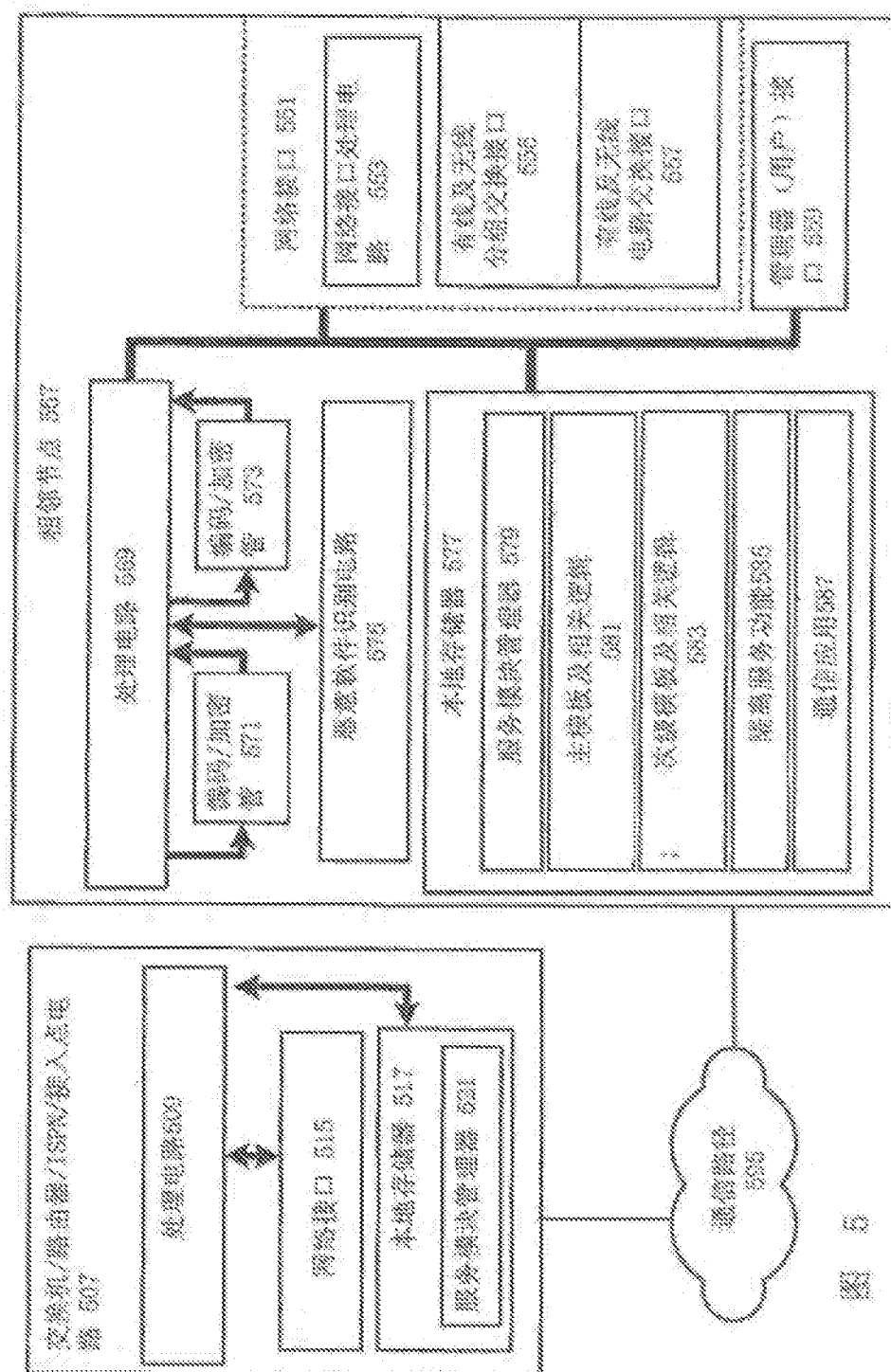


图 5



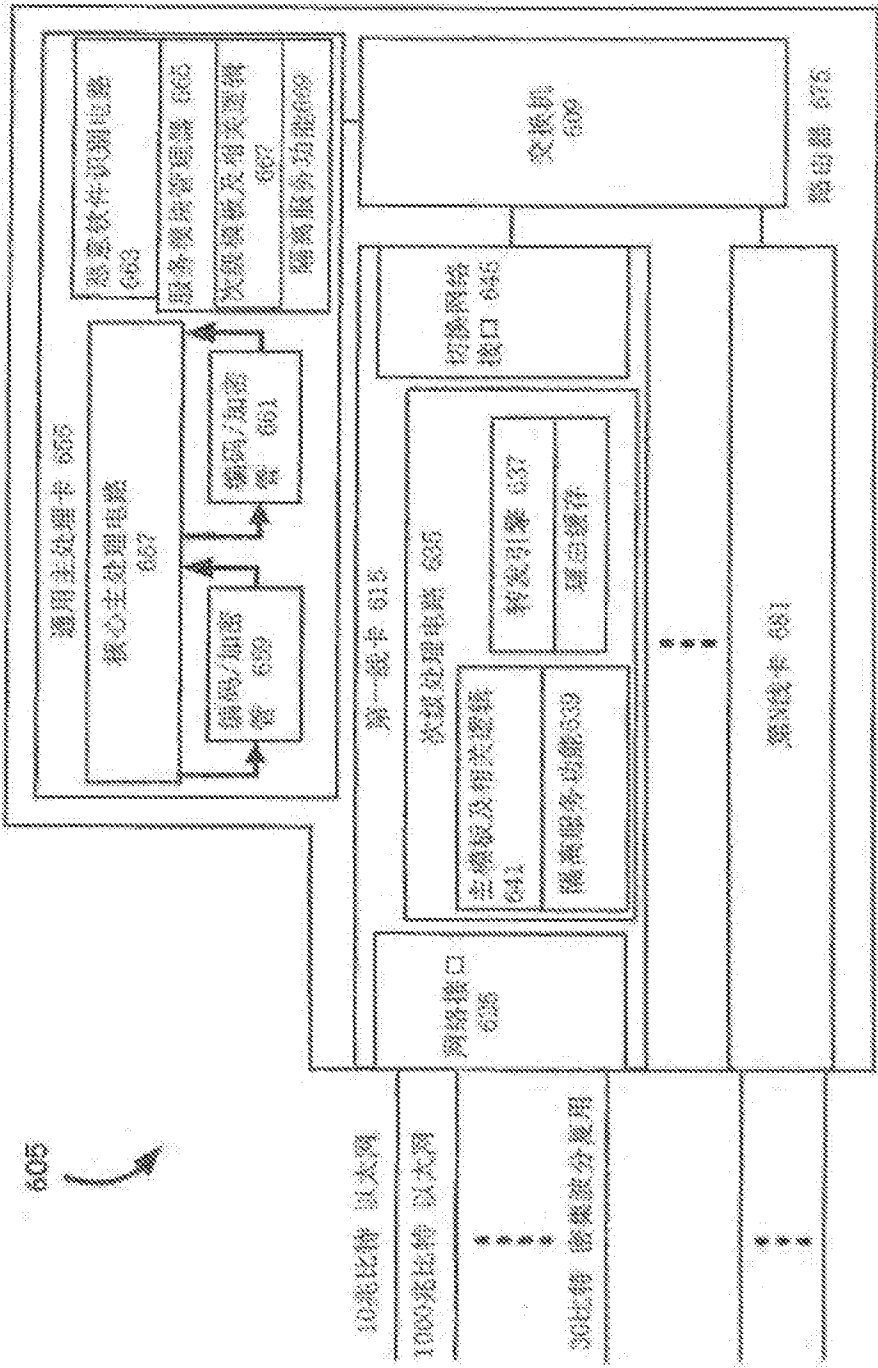


图 6

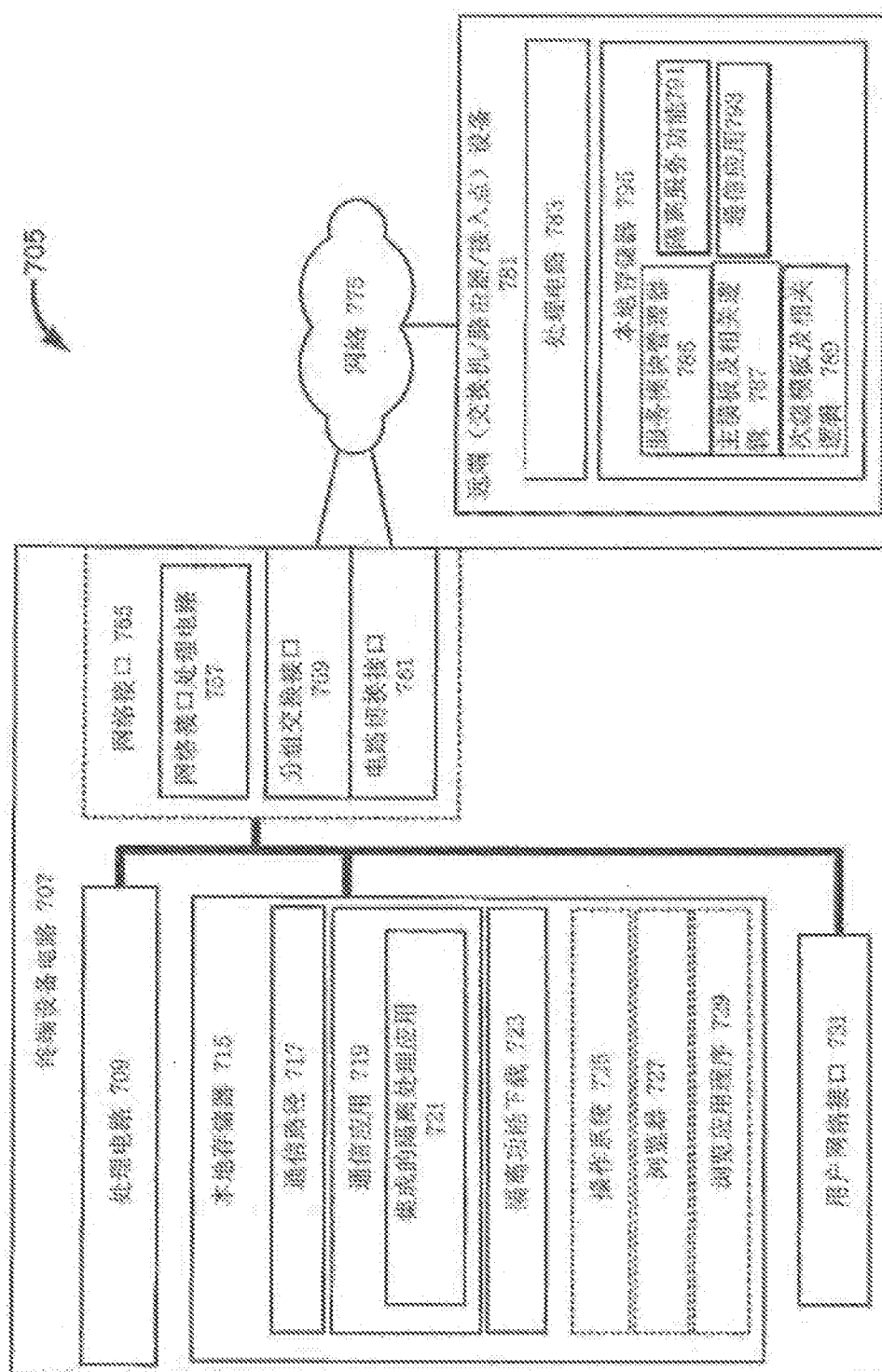


图 7

805

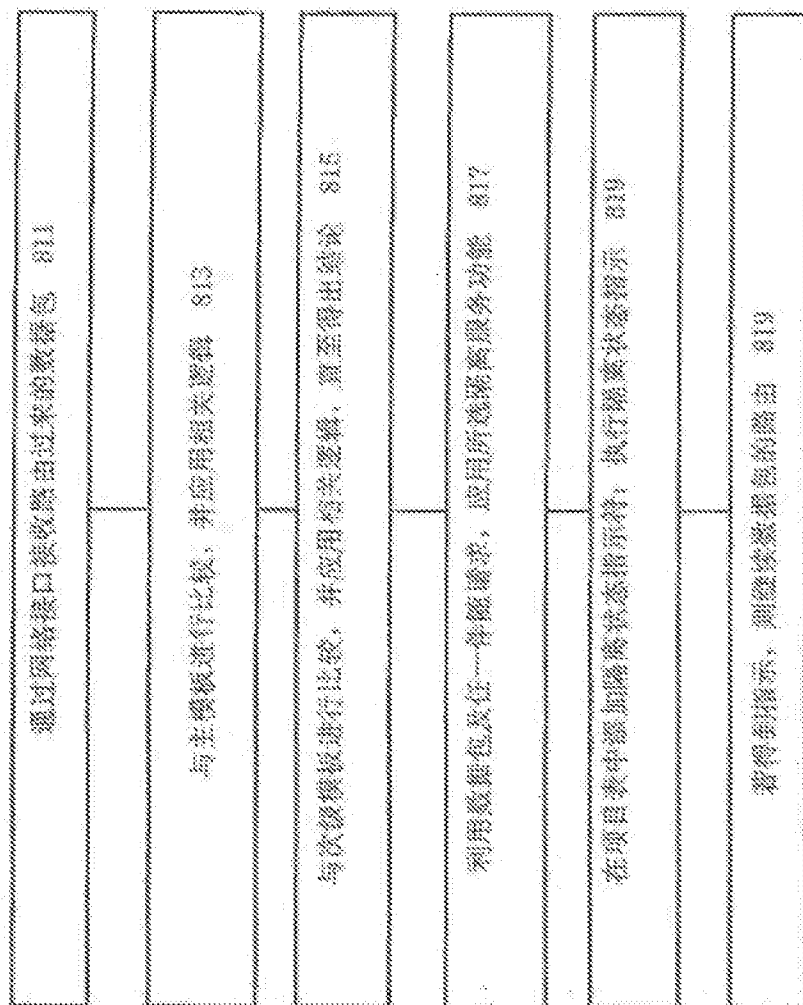


图 8

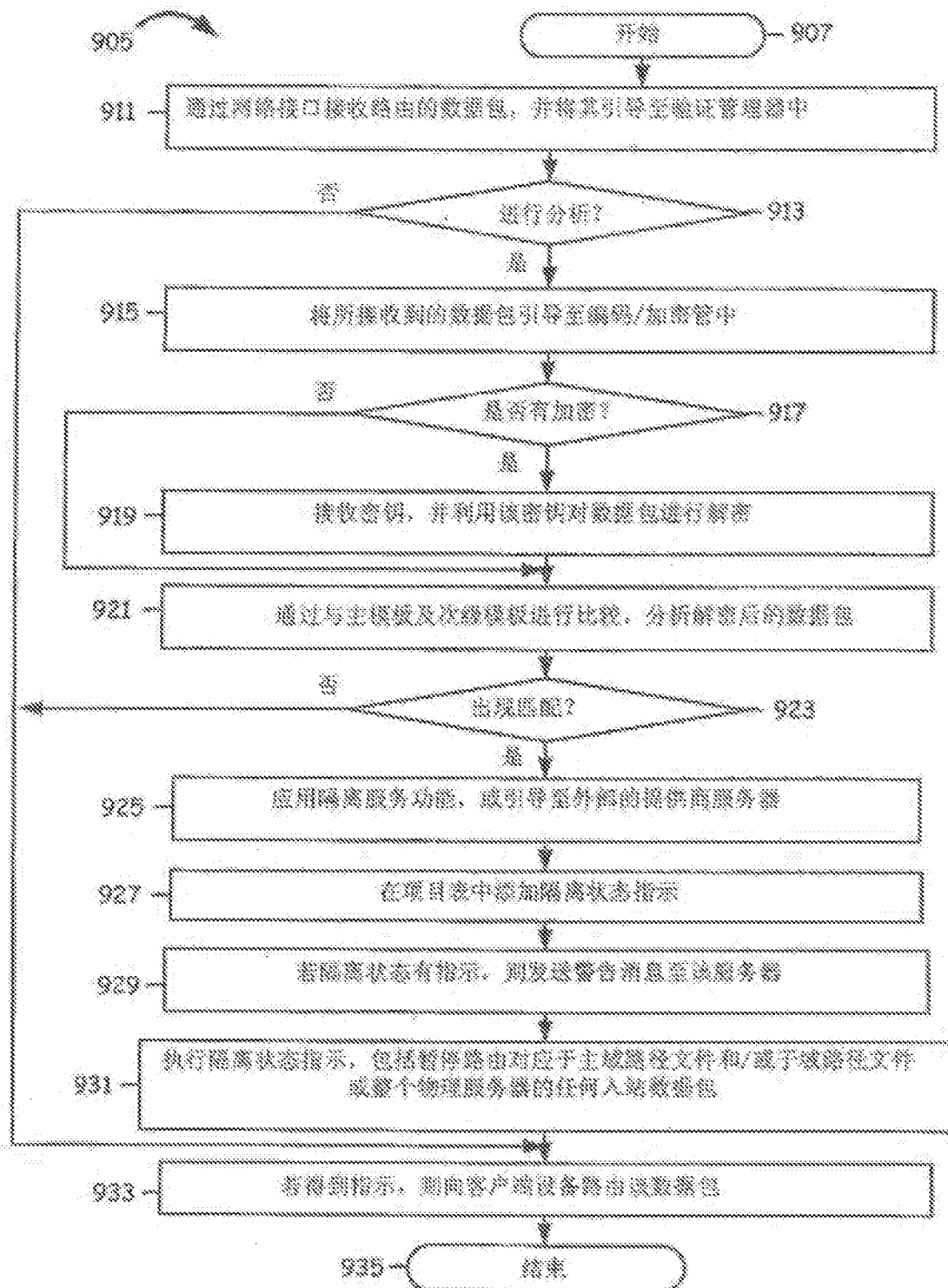
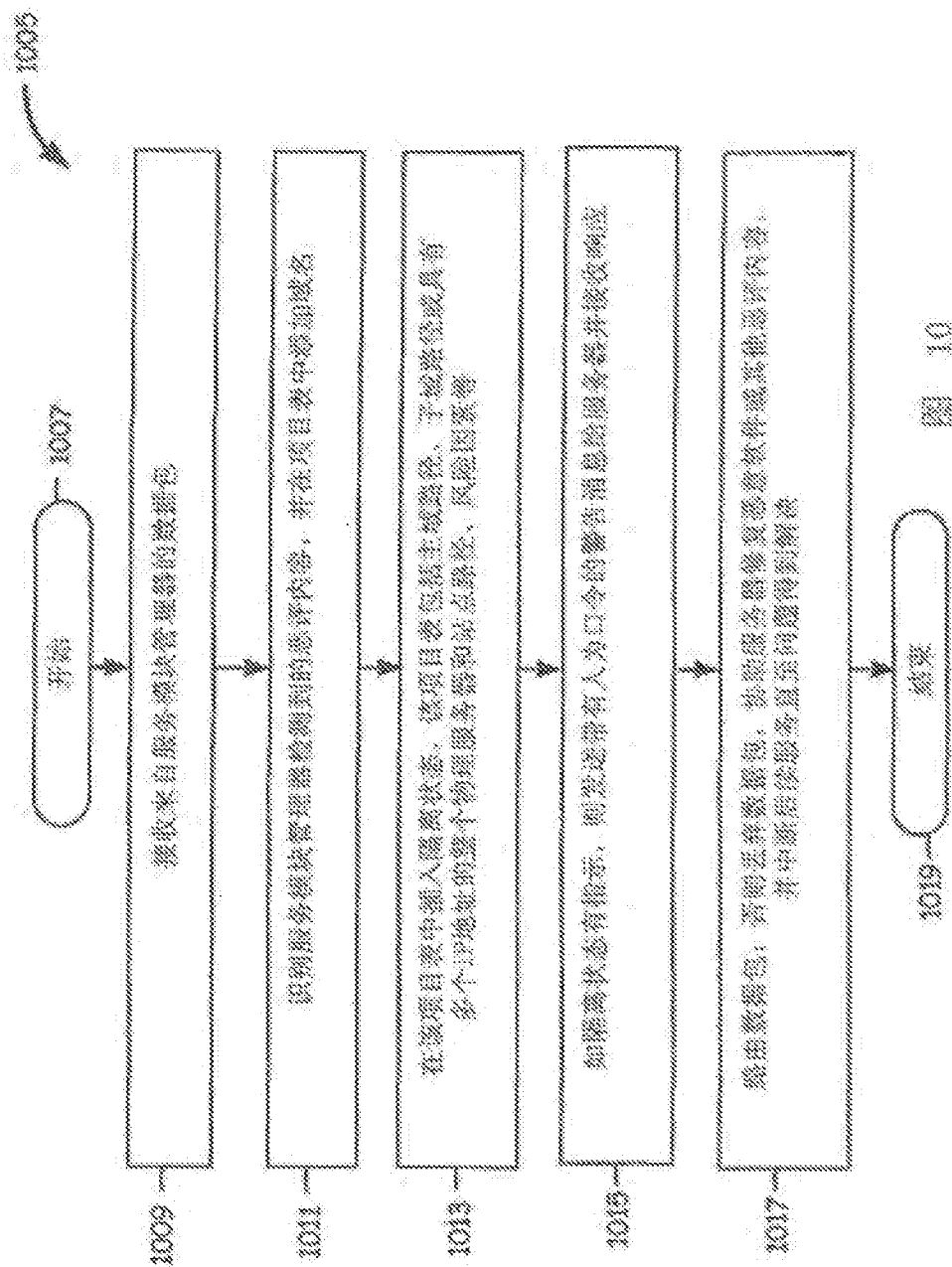


图 9





Espacenet

Bibliographic data: CN101141396 (A) — 2008-03-12

## Packet processing method and network appliance

No documents available for this priority number.

Inventor(s): ZHIWANG ZHAO [CN] ± (ZHAO ZHIWANG)

Applicant(s): HUAWEI TECH CO LTD [CN] ± (HUAWEI TECHNOLOGIES CO., LTD)

Classification: - international: H04L12/46; H04L12/56; H04L29/06  
- cooperative:

Application number: CN20071151805 20070918

Priority number(s): CN20071151805 20070918

Also published as: CN101141396 (B)

## Abstract of CN101141396 (A)

The present invention discloses a method for processing a packet. The method comprises the following steps: the trust attribute of the received DNS server response packet access port is obtained; if the port is a trust port, the response packet of the DNS server is forwarded. The present invention also provides a network equipment, which solves the problem of the DNS phishing attack through configuring the trust attribute of the port, and the security of the network equipment is improved, thereby, the security of the DNS service is enhanced.

Last updated: 15.03.2015 | Worldwide Database | 5.8.11.1.922

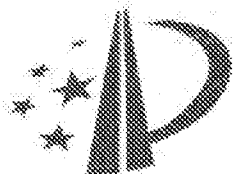
[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 29/06 (2006.01)

H04L 12/46 (2006.01)



# [12] 发明专利申请公布说明书

[21] 申请号 200710151805.6

[43] 公开日 2008 年 3 月 12 日

[11] 公开号 CN 101141396A

[22] 申请日 2007.9.18

[21] 申请号 200710151805.6

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为  
总部办公楼

[72] 发明人 赵志旺

[74] 专利代理机构 北京挺立专利事务所

代理人 梁吉甫

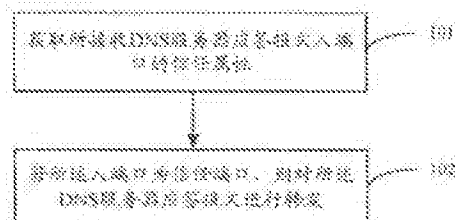
权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称

报文处理方法和网络设备

[57] 摘要

本发明公开了一种报文处理方法，包括以下步骤：获取所接收 DNS 服务器应答报文入端口的信任属性；若所述入端口为信任端口，则对所述 DNS 服务器应答报文进行转发。本发明还提供了一种网络设备，通过配置端口的信任属性，解决了 DNS 仿冒攻击的问题，提高了网络设备的安全能力，从而提升了 DNS 业务的安全性。



1. 一种报文处理方法, 其特征在于, 包括以下步骤:  
获取所接收域名系统 DNS 服务器应答报文入端口的信任属性;  
若所述入端口为信任端口, 则对所述 DNS 服务器应答报文进行转发。
2. 如权利要求 1 所述报文处理方法, 其特征在于, 在所述获取所接收 DNS 服务器应答报文入端口的信任属性之前, 还包括: 设置网络设备各端口的信任属性, 并将所述各端口的信任属性存储在所述网络设备中。
3. 如权利要求 2 所述报文处理方法, 其特征在于, 所述设置网络设备各端口的信任属性, 具体包括: 将与 DNS 服务器连接的端口设置为信任端口, 将不与 DNS 服务器连接的端口设置为非信任端口。
4. 如权利要求 1 所述报文处理方法, 其特征在于, 所述获取所接收 DNS 服务器应答报文入端口的信任属性, 具体包括: 根据所述 DNS 服务器应答报文入端口信息和网络设备存储的所述端口信任属性获取所述入端口的信任属性。
5. 一种网络设备, 其特征在于, 包括:  
端口信任属性获取单元, 用于获取所接收 DNS 服务器应答报文入端口的信任属性;  
报文转发单元, 与所述端口信任属性获取单元连接, 用于在所述端口信任属性获取单元获取到接收 DNS 服务器应答报文的入端口为信任端口之后, 转发所述 DNS 服务器应答报文。
6. 如权利要求 5 所述网络设备, 其特征在于, 还包括: 端口信任属性设置单元, 用于设置所述网络设备各端口的信任属性。
7. 如权利要求 6 所述网络设备, 其特征在于, 还包括: 端口信任属性存储单元, 与所述端口信任属性设置单元连接, 用于存储所述网络设备各端口的信任属性。
8. 如权利要求 5 所述网络设备, 其特征在于, 还包括: 报文丢弃单元, 与所述端口信任属性获取单元连接, 用于在所述端口信任属性获取单元获取到接收 DNS 服务器应答报文的入端口为非信任端口之后, 直接丢弃该 DNS



服务器的应答报文。

9、如权利要求5所述网络设备，其特征在于，还包括：报文上报单元，与所述端口信任属性获取单元连接，用于在所述端口信任属性获取单元获取到接收DNS服务器应答报文的入端口为非信任端口之后，将所述非信任端口的报文上报并输出日志。

## 报文处理方法和网络设备

### 技术领域

本发明涉及网络通信技术领域，尤其指一种报文处理方法和网络设备。

### 背景技术

在TCP/IP (Transmission Control Protocol/Internet Protocol, 传输控制协议/互联网络协议) 架构的网络环境中，例如广泛使用的Internet，DNS (Domain Name System, 域名系统) 是一个非常重要而且常用的系统。DNS的主要功能就是将用户容易记忆的域名与不容易记忆的IP (Internet Protocol, 互联网络协议) 地址进行转换，而执行DNS服务的网络主机则称之为DNS服务器。DNS服务器通常是将域名转换为IP地址，然后再使用所查找到的IP地址进行服务的连接，该过程俗称为正向解析。例如：用户终端向DNS服务器发送访问域名www.popunet.net的请求，则DNS服务器根据其保存的域名和IP地址的映射关系，查找与域名www.popunet.net相对应的IP地址，如61.186.250.41，然后向IP地址为61.186.250.41的服务提供设备发送服务请求，进行服务连接。通过DNS服务器的作用，使得用户能够通过记忆简单的域名代替难记的IP地址，方便了用户的服务查询。

随着Internet的飞速发展，组网环境日趋复杂，网络攻击、病毒攻击、网络欺骗等行为也日益频繁，对网络整体组网安全的危害性也日趋严重。DNS的安全性也日益成为人们关注的焦点，由DNS安全引发的安全问题也越来越多，例如：网络中存在部分恶意用户终端假冒DNS服务器的情况，由于该情况的存在，导致了用户终端发出的DNS申请不能被正确的DNS服务器应答，而被假冒的DNS服务器应答，从而引起用户终端不能正常进行域名转换而导致用户终端业务异常。另外，假冒DNS服务器还可能通过向用户终端发送大量的假冒DNS应答报文，占用大量资源达到对用户终端进行攻击的目的，此种攻击方式属于DOS (Denial Of Service, 拒绝服务) 攻击。

现有技术中一种解决DNS安全问题的方法是应用层过滤，即通过分析设备收发的DNS报文的协议内容，根据预先设定的规则干预DNS报文的转发流程，从而达到保护DNS安全的目的。但是该方法的重点部署是在防火墙设备上，而在其他类型的网络设备上因资源占用等一些原因导致无法很好的部署，并且该方法的配置过程繁琐，需要熟悉DNS协议的专业人员进行配置，而且需要对应用层协议信息进行分析，对设备的处理性能要求比较高。

## 发明内容

本发明实施例提供一种报文处理方法和网络设备，以解决现有技术中保护DNS安全的方法复杂、不易部署的缺陷。

为达到上述目的，本发明实施例一方面提供了一种报文处理方法，包括以下步骤：获取所接收域名系统DNS服务器应答报文入端口的信任属性；若所述入端口为信任端口，则对所述DNS服务器应答报文进行转发。

另一方面，本发明实施例还提供了一种网络设备，包括：端口信任属性获取单元，用于获取所接收DNS服务器应答报文入端口的信任属性；报文转发单元，与所述端口信任属性获取单元连接，用于在所述端口信任属性获取单元获取到接收DNS服务器应答报文的入端口为信任端口之后，转发所述DNS服务器应答报文。

与现有技术相比，本发明实施例在网络设备上设置端口的信任属性，通过简单易用的配置解决了DNS仿冒攻击的问题，提高了网络设备的安全能力，从而提升了DNS业务的安全性。

## 附图说明

图1是本发明实施例一种报文处理方法的流程图；

图2是本发明实施例一的报文处理示意图；

图3是本发明实施例二的报文处理示意图；

图4是本发明实施例一种网络设备的结构示意图。

## 具体实施方式

下面结合附图和具体实施例进行详细说明。

如图1所示，图1是本发明实施例一种报文处理方法的流程图，主要包括以下步骤：

步骤101，获取所接收DNS服务器应答报文入端口的信任属性。

网络设备接收外界的DNS服务器应答报文，并根据该DNS服务器应答报文获取报文的入端口信息，然后查找该网络设备中与该入端口相对应的信任属性，从而获取到所接收DNS服务器应答报文入端口的信任属性。其中网络设备各端口的信任属性是在组网的时候设置在该网络设备上的，在组网的时候能够确定网络设备中连接DNS服务器的端口，将连接DNS服务器的端口设置为信任端口，将不连接DNS服务器的端口设置为非信任端口。如果需要对网络结构进行重组，而改变了原来的组网结构，则需对重组后的网络结构中网络设备各端口的信任属性重新进行设置，但还是同样将连接DNS服务器的端口设置为信任端口，将不连接DNS服务器的端口设置为非信任端口。如果系统中包含主用DNS服务器和备用DNS服务器，则将连接主备用DNS服务器的端口均设为信任端口，且主备用DNS服务器具有相同的优先级。

其中，DNS服务器应答报文为一种DNS报文，所谓DNS报文包括：DNS请求报文和DNS服务器应答报文，DNS请求报文是指用户终端向DNS服务器发送的域名解析请求报文，DNS服务器应答报文是指DNS服务器向用户终端返回的域名解析应答报文。

步骤102，若所述入端口为信任端口，则对所述DNS服务器应答报文进行转发。

网络设备根据获取到该DNS服务器应答报文入端口的信任属性，对该应答报文进行相应的处理。如果该应答报文的入端口为信任端口，则网络设备将该应答报文进行转发；如果该应答报文的入端口为非信任端口，则网络设备对该应答报文不做转发，而是采取其他处理方式，有多种处理方式，例如可以将其直接丢弃，对非信任端口的报文进行上报并输出日志等。因为在组网的时候已经确定了该网络设备中与DNS服务器相连接的端口为信任端口，

也即DNS服务器应答报文只能从该信任端口被网络设备所接收，网络设备不会从其他非信任端口上接收到正常的DNS服务器应答报文。如果网络设备从其他非信任端口接收到DNS服务器应答报文，则说明该DNS服务器应答报文为非正常的DNS服务器应答报文，有可能为仿冒DNS服务器发出的应答报文。因此，设置了端口信任属性，也就确定了安全的DNS服务器应答报文的来源，网络设备只对信任端口上接收到的DNS服务器应答报文进行转发，对非信任端口上接收到的DNS服务器应答报文不做转发，而是采取其他处理方式，有多种处理方式，例如可以将其直接丢弃、对非信任端口的报文进行上报并输出日志等。

需要指出的是，上述本发明实施例中的网络设备包括路由器、交换机、防火墙设备等等，并且该网络设备可以是与DNS服务器直接相连接的PE（Provider Edge，提供商边缘）设备，也可以是与DNS服务器间接相连接的CE（Customer Edge，用户边缘）设备。无论是PE设备，还是CE设备，在组网的时候都能够确定出该些网络设备中直接或间接与DNS服务器相连接的端口，也即无论是直接与DNS服务器相连接的PE设备，还是通过其他上游网络设备与DNS服务器间接连接的CE设备，该DNS服务器向该PE或CE设备发送应答报文时，该PE或CE设备必然通过其直接或间接连接DNS服务器的端口进行接收。

下面结合图2所示本发明实施例一的报文处理示意图进一步详细说明。如图2所示，PE设备包括3个端口，其中端口3与真实的DNS服务器相连接，端口1、端口2分别连接用户终端，则在组网时可确定该PE设备各端口的连接状况，根据该连接状况对该PE设备各端口的信任属性进行设置，设置端口3为信任端口，端口1和端口2为非信任端口，PE设备对设置的各端口信任属性进行存储。正常工作时，PE设备对到达该设备的DNS报文进行监听，当监听到有DNS服务器应答报文时，根据该应答报文的入端口信息，获取PE设备中存储的该入端口对应的信任属性。若PE设备监听到该DNS服务器应答报文的入端口为端口3，则可根据该PE设备中存储的各端口和信任属性的映射关系获取到端口3为信任端口，该PE设备根据该应答报文中携带的目的信息对该应答报文进行

转发；若PE设备监听到该DNS服务器应答报文的入端口为端口2，则可根据该PE设备中存储的各端口和信任属性的映射关系获取到端口2为非信任端口，该PE设备在端口2不转发该应答报文，而是采取其他处理方式，有多种处理方式，例如：可以将其直接丢弃，对非信任端口的报文进行上报并输出日志等。

假如有攻击者仿冒DNS服务器通过该PE设备向用户终端发送仿冒的DNS服务器应答报文，PE设备通过端口2进行接收，由于端口2为非信任端口，则PE设备直接在端口2上将接收的应答报文丢弃，因此攻击者仿冒DNS服务器发送的应答报文也就无法最终到达用户终端，从而有效避免了该攻击者的攻击行为。

在上述本发明实施例中，组网的时候已经确定了PE设备中只有端口3连接DNS服务器，可知DNS服务器向该PE设备发送应答报文时，该PE设备通过端口3进行接收，而该PE设备的端口1、端口2分别连接用户终端，则可推断该PE设备不会从端口1、端口2接收到DNS服务器应答报文。因此该PE设备对到达该设备DNS报文进行监听，并且只对端口3上接收到的DNS服务器应答报文进行转发；如果监听到端口1或端口2接收的DNS服务器应答报文，则将该应答报文归类为非正常的DNS服务器应答报文，直接在端口1或端口2上将该应答报文丢弃。由此可知，本发明实施例对网络设备各端口的信任属性进行设置，只是对DNS服务器应答报文进行了安全域的划分，也即对安全的DNS服务器应答报文的来源进行了限定，只有在信任端口上接收到的DNS服务器应答报文才为安全的DNS服务器应答报文。

上述本发明实施例是通过设置网络设备物理端口的信任属性对DNS服务器应答报文进行安全域的划分，本发明实施例二还可通过设置网络设备逻辑端口，也即VLAN（Virtual Local Area Network，虚拟局域网）的信任属性对DNS服务器应答报文进行安全域的划分。如图3所示，PE设备分别连接不同的VLAN：VLAN1、VLAN2和VLAN3，其中真实的DNS服务器在VLAN3中，则组网的时候设置VLAN3为信任VLAN，设置VLAN1和VLAN2为非信任VLAN，PE设备对设置的各VLAN的信任属性进行存储。正常工作时，PE设备对到达该设备的DNS报文进行监听，当监听到有DNS服务器应答报文时，根据该应

答报文中携带的入VLAN信息，获取PE设备中存储的对应VLAN的信任属性。若该DNS服务器应答报文携带的入VLAN信息为VLAN3，则可根据该PE设备中存储的各VLAN和信任属性的映射关系获取到VLAN3为信任VLAN，该PE设备根据该应答报文中携带的目的信息对该应答报文进行转发；若该DNS服务器应答报文的入VLAN为VLAN2，则可根据该PE设备中存储的各VLAN和信任属性的映射关系获取到VLAN2为非信任VLAN，该PE设备在VLAN2上不转发该应答报文，而是采取其他处理方式，有多种处理方式，例如：可以将其直接丢弃、对非信任端口的报文进行上报并输出日志等。

假如有攻击者假冒DNS服务器通过该PE设备向用户终端发送仿冒的DNS服务器应答报文，PE设备获取到该应答报文的入VLAN为VLAN2，由于VLAN2为非信任VLAN，PE设备不转发接收到的应答报文，而是采取其他处理方式，有多种处理方式，例如：可以将其直接丢弃、对非信任端口的报文进行上报并输出日志等，从而有效避免了该攻击者的攻击行为。

本发明实施例还提供了一种网络设备，如图4所示，包括：端口信任属性获取单元1和报文转发单元2。端口信任属性获取单元1，用于获取所接收DNS服务器应答报文入端口的信任属性。报文处理单元2，与端口信任属性获取单元1连接，用于在端口信任属性获取单元1到接收的DNS服务器应答报文的入端口为信任端口之后，转发该DNS服务器应答报文。

本发明另一实施例的网络设备在上述基础上还包括：端口信任属性设置单元3和端口信任属性存储单元4。端口信任属性设置单元3，用于设置该网络设备各端口的信任属性。端口信任属性存储单元4，与端口信任属性设置单元3和端口信任属性获取单元1连接，用于对端口信任属性设置单元3所设置的各端口信任属性进行存储，以供端口信任属性获取单元1根据网络设备所接收DNS服务器应答报文的入端口信息获取对应的端口信任属性。

本发明另一实施例的网络设备在上述基础上还包括：报文丢弃单元5，与端口信任属性获取单元1连接，用于在端口信任属性获取单元1获取到接收的DNS服务器应答报文的入端口为非信任端口之后，不转发该DNS服务器应答报文，而是将其直接丢弃。报文上报单元6，与端口信任属性获取单元1连接，

用于在端口信任属性获取单元1获取到接收的DNS服务器应答报文的入端口为非信任端口之后，不转发该DNS服务器应答报文，而是对非信任端口的报文进行上报并输出日志。

综上所述，本发明实施例提供的一种报文处理方法和网络设备，通过设置网络设备各端口的信任属性，将连接DNS服务器的端口设置为信任端口，将不连接DNS服务器的端口设置为非信任端口，从而实现了对DNS服务器应答报文的安全域划分，并且网络设备只对安全域发来的DNS服务器应答报文进行转发处理，对非安全域发来的DNS服务器应答报文不做转发，而是采取其他处理方式，有多种处理方式，例如：可以将其直接丢弃，对非信任端口的报文进行上报并输出日志等，使得攻击者仿冒DNS服务器发送的应答报文无法最终到达用户终端，从而有效避免了攻击者的攻击行为，保证了DNS业务的安全。

另外，现有的仿冒DNS服务器发起DNS应答报文的DOS攻击，也是由攻击者通过向用户终端发送大量的仿冒DNS服务器应答报文，占用大量资源进行攻击的手段。由于本发明实施例在网络设备的非信任端口上直接将DNS应答报文丢弃，使得攻击者发送的大量DNS服务器应答报文无法到达用户终端，从而也就自然解决了仿冒DNS服务器发起应答报文的DOS攻击问题，确保了网络设备的安全，也避免了非法流量在网络上的传播，提升了网络资源的利用率。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等等）执行本发明各个实施例所述的方法。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润



饰, 这些改进和润饰也应视为本发明的保护范围。

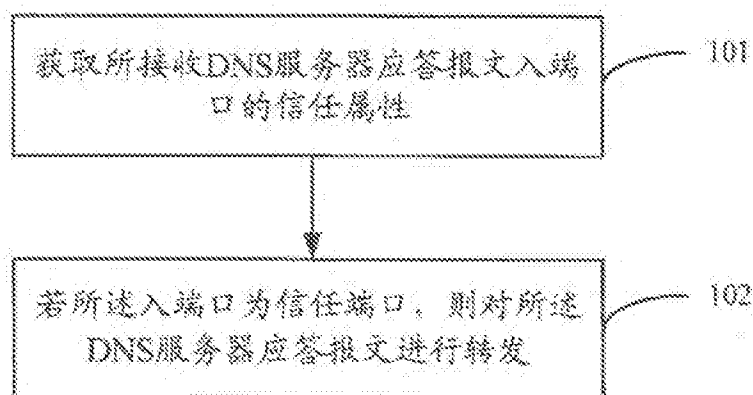


图 1

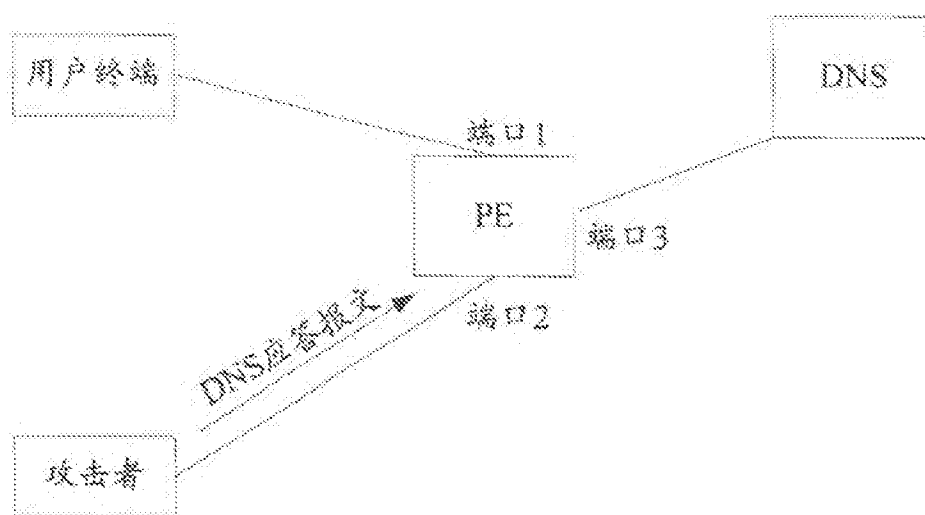


图 2

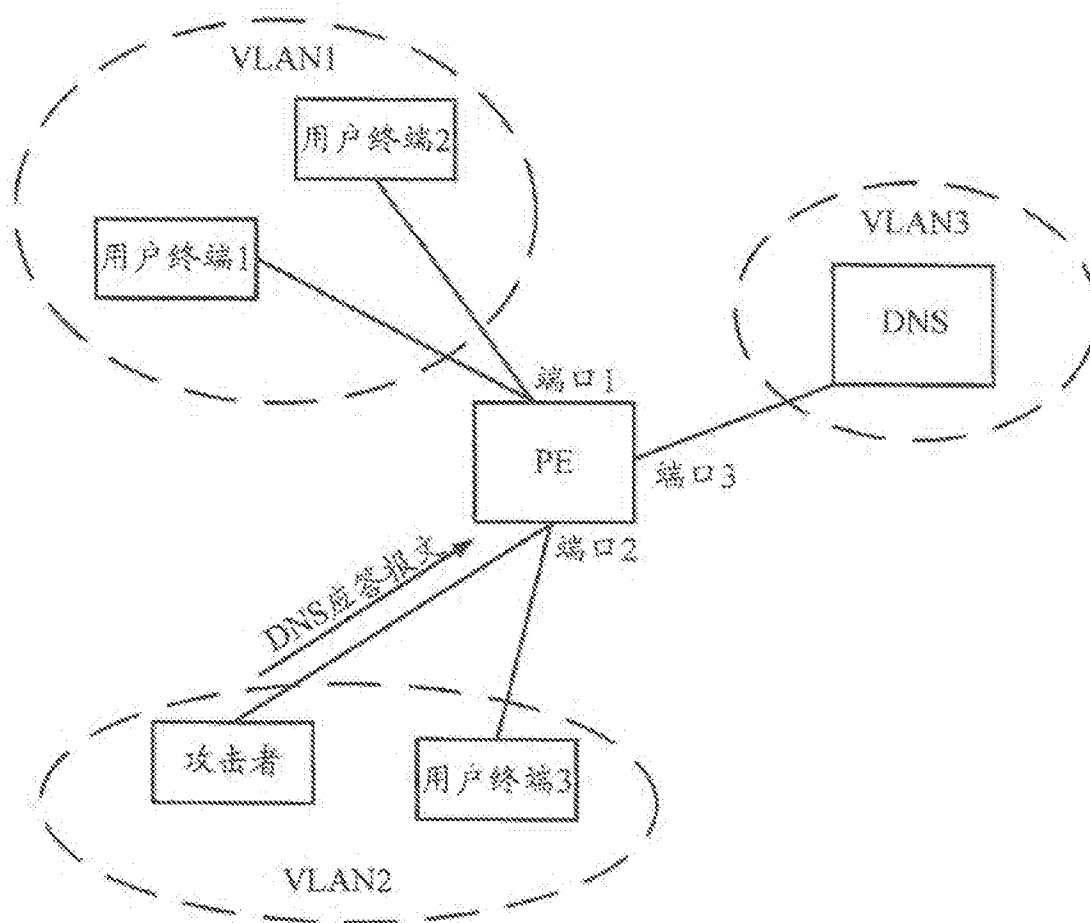


图 3

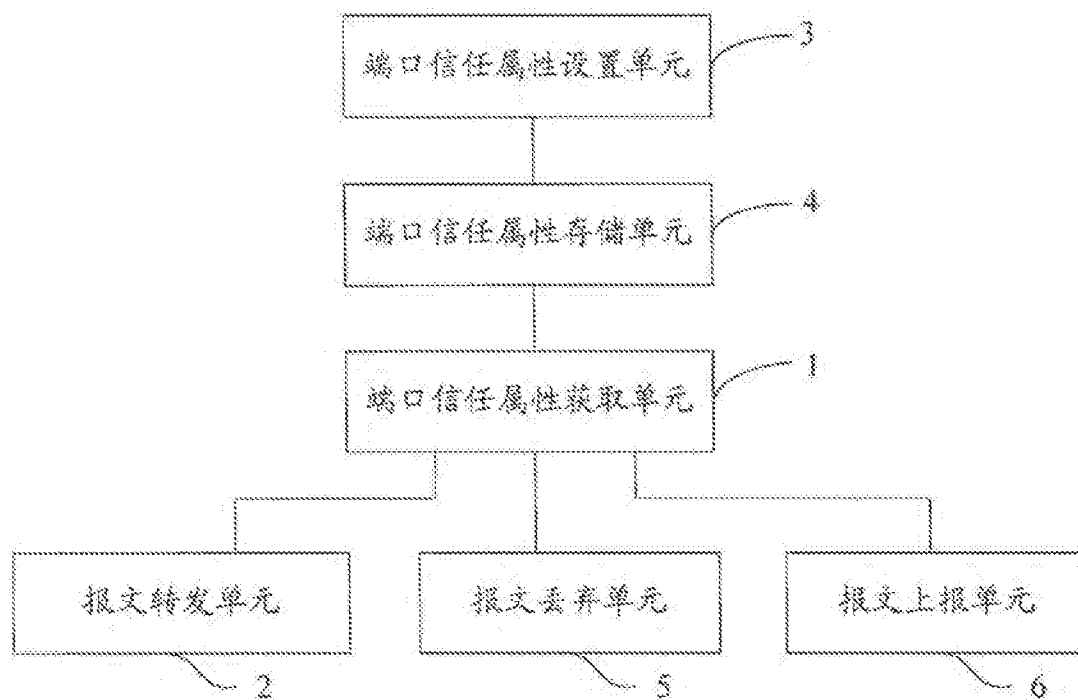


图 4



Espacenet

Bibliographic data: CN101945053 (A) — 2011-01-12

## Method and device for transmitting message

No documents available for this priority number.

Inventor(s): BIN WANG; TAO LIN ± (WANG BIN ; LIN TAO)

Applicant(s): H3C TECHNOLOGIES CO LTD ± (H3C TECHNOLOGIES CO., LIMITED ; HANGZHOU H3C TECHNOLOGIES CO., LTD)

Classification: - international: H04L12/56; H04L29/06; H04L29/12  
- cooperative:

Application number: CN20101502935 20101012

Priority number (s): CN20101502935 20101012

Also published as: CN101945053 (B)

## Abstract of CN101945053 (A)

The invention discloses a method and a device for transmitting a message. The method comprises the following steps that: NAS equipment monitors a process that user equipment acquires a DNS server address, sets a DNS access rule for the user equipment according to the DNS server address, and allows the message sent to the DNS server by the user equipment according to the DNS access rule. In the invention, the problem that a free IP address needs to be reconfigured by an administrator when the IP address of the DNS server is changed can be avoided, and the network configuration is simplified.

Espacenet, 12-01-2013 Worldwide Database 1/1 (W)



The stated NAT separates according to said DNS server address in the DNS access rule is user equipment, also includes the following:  
when the DNS server address receiving status changed, the user equipment is obtaining said DNS server address;

The stated NAT separates according to the user device to implement the re-configuration process of the DNS server address, and is accordance with changes of the DNS server address meet new NAT access rules.

The stated NAT separates according to said DNS server address in the DNS access rule is user equipment, also includes the following:

If the user equipment in the preset time has not passed the authentication of the authentication server, the NAT rules device is delete for access rules.

The stated NAT separates when the user equipment sends the message to the authentication server, comprising:

when receiving from the user equipment said the network access message, the stated NAT separates according to the authentication server; the address of the network access message on the authentication server, and by the authentication server passed to the user authentication device.

The authentication server portal to the user authentication device, also includes the following:

when the user equipment when authentication through the portal, the stated NAT, also allows the message to the network access of the user equipment.

The meaning of the DNS server address message comprises:

In DNS network, the user equipment from the DHCP server to obtain the address of the server in the process of DNS; said DHCP NAT separates through the server to the user of the equipment sends message ACK; or,

In DNS network, the user equipment from the first DNS server to obtain the address of the server in the course of, the stated DHCP NAT separates through the server to the user of the equipment sends message Reply; or,

In DNS network, the user equipment from the router is obtained in the process of DNS server address, the router through the stated NAT equipment of the device to send to the user the message RA.

The present invention provides a apparatus NAT including the NAT separates applied to, a user equipment, the authentication server, DNS server address allocation server and in the authentication system, the user equipment through the before authentication of the authentication server, the NAT separates when the user equipment to the authentication server sends the message sent to the user device and the address allocation message of the server, and includes the user message of user equipment, the NAT separates includes:

Setting module, used for user equipment through that authentication takes the address allocation server to obtain the process of DNS server address, and when the equipment to the address allocation server sends to the user equipment of the DNS server address of the message, according to said DNS server address to the NAT access rule is user equipment;

Processing module, according to said NAT access rules allow the user device sends the message to the DNS server;

The included in the DNS access rule the IP address of user equipment and the DNS server address;

The processing module, and is also used for the IP address of NAT permission source when rule of user equipment is the IP address;

destination IP address to the NAT access rule DNS server address in the message;

The purpose for the IP address allows status the authentication of the message the address of the server;

The IP address allows the purpose of the address allocation of the message the address of the server.

The setting module, when the DNS is also used to change the address of the server, the user equipment re-obtaining the address of the DNS server, the user device to implement the re-configuration process of the DNS server address, and is accordance with changes of the DNS server address meet new NAT access rules.

The processing module, is also used for the preset time has not passed the user equipment in the authentication of the authentication server, the DNS access rule is deleted.

The processing module, is also used for when receiving from the user equipment said the network access message, according to the authentication server the address of the network access message on the authentication server, and by the authentication server passed to the user authentication device.

The processing module, and is also used for authentication when the user equipment through portal, allowing the message to the network access of the user equipment.

The meaning of the DNS server address message comprises:

In DNS network, the user equipment from the DHCP server to obtain the address of the server in the process of DNS; said DHCP NAT separates through the server to the user of the equipment sends message ACK; or,

In DNS network, the user equipment from the first DNS server to obtain the address of the server in the course of, the stated DHCP NAT separates through the server to the user of the equipment sends message Reply; or,

In DNS network, the user equipment from the router is obtained in the process of DNS server address, the router through the stated NAT equipment of the device to send to the user the message RA.

Consistent with the prior art, the present invention at least has the following advantages:

In the user device to obtain in the process of DNS server address, NAT NAT that the address of the server apparatus dynamically, manual configuration does not need to be a fixed IP address to allow a user device to access the DNS server, the DNS server address and could the need to re-configuration of the change, the network configuration is simplified, and it is convenient to NAT equipment maintenance and use.

Description of drawings

Figure 1 is sending method flowchart of the present invention provides a kind of message;

Figure 2 is a schematic diagram of the processing procedure in the invention first DNS access rule application scene;

Figure 3 is a schematic diagram of the processing procedure in the invention third DNS access rule application scene;

Figure 4 is flow of the invention in equipment NAT;

Principle of operation

In the prior art, there are the following individual the needs of the users of the static DNS network obtaining IP address, then discuss the fixed IP address, DNS server and the need for more new IP address using the solution of re-configuration, known NAT port directly allow the safety problem caused by the message of the illegal user mentions addresses DNS server is also the attack.

Against the above-mentioned problem, the present invention provides a method and apparatus for the sending of the message, user equipment device NAT by means to the process of obtaining the DNS server address, the server address of NAT is dynamically discovered, and is accordance with the DNS server address setting DNS access rule, the access rule according to DNS and from the user device to determine whether the domain name resolution message is sent to the NAT server.

In this invention, the address of the server DNS through the dynamic discovery, manual configuration does not need to be a fixed IP address of the free way to allow a user device to access the DNS server. NAT access rule by setting, can be only the destination address of the DNS server address on the domain name resolution message is sent to the DNS server, the DNS-known port directly allow the safety problem caused by the message. Through the DNS access rules in determining whether the domain name from the user device to assign the message given to the NAT server, the DNS access rule only meet the substrate, equipment of the NAT server can only be added, to avoid unauthorized user in maliciously attack, problem of the DNS server.

Combining the figure below detailed description of the invention.

As shown in Figure 1, in the invention presents a method of sending of the message, the method is applied to include NAS equipment, the user equipment, the authentication server, DNS server address allocation server and in the authentication system, wherein the authentication server is used for portal device for each user authentication, the address allocation server for each user equipment and DNS server address, in practical application, the address allocation server may include, but is not limited to the DHCP server and router. In this invention, the user equipment perform the authentication of the authentication server, NAS apparatus may send the user to an authentication server apparatus sends the message (used for the authentication server registration portal authentication page in portal authentication, that is, allow the destination IP address to the authentication server address message), and sent to the user equipment of the message directly allocation server (for first the address allocation server obtain the corresponding IP address and the DNS server address, that is, allow the destination IP address to address allocation server address message), and to other message of the user equipment, for example, network access message (used for access to the network, such as web site visited by the message www.baidu.com), and the like. Based on the above-mentioned situation, the method comprises the following steps:

Step 101, NAS apparatus intercepting the user equipment through the address allocation server DNS for process of obtaining the address of the server, and upon the interception to the address allocation server to the user equipment through the NAS equipment sent by the DNS server address of the message, the address of the server DNS, NAS of the apparatus, according to the user equipment DNS access rule set. In the practical application, in order to access to the network, the user equipment needs to obtain the DNS server address, at this time, user equipment NAS apparatus needs to intercept the process of obtaining the address of the server DNS.

In DNS network, when the user equipment from the DHCP server (address allocation server) obtain to their own IP address, DHCP server needs to be distributed in the user equipment (DHCP address) IP address, DNS server address, gateway, and other network configuration parameters through NAS device sends information to the user equipment.

Specific, user equipment through NAS device to the DHCP server sends DHCP REQUEST (request) message, when receiving the DHCP message after REPLY (DHCP server for the user equipment IP address allocation, DHCPACK message provides the IP address, the DNS server address NAS device sends information to the user equipment).

NAS apparatus through the interception the above-mentioned process, message reply when detects heard, it indicates that the device receives the NAS NAS device to the user equipment sends the DHCP server address of the message (the message Reply).

In DNS network, when the user equipment from the DHCP server (address allocation server) obtain to their own IP address is obtained, DHCP server needs to be distributed in the user equipment (DHCP address) IP address, DNS server address, gateway, and other network configuration parameters through NAS device sends information to the user equipment.

Specific, to the user equipment through NAS DHCP server sends message REQUEST, when receiving the message after REPLY, DHCP server address for the user equipment IP address, the IP address of the message Reply, through DNS server address NAS device sends information to the user equipment.

NAS apparatus through the interception the above-mentioned process, message reply when detects heard, it indicates that the device receives the NAS NAS device to the user equipment sends the DNS server address of the message (the message Reply).

In DNS network, when the user equipment from the router (address allocation server) when obtaining routing table information, through router sends RA (advertisement router, router advertisement) message to the local link configuration information (for example, network prefix, such as DNS server address) through NAS apparatus (router) to the user equipment.

NAS apparatus through the interception the above-mentioned process, message RA when detects heard, it indicates that the device receives the NAS NAS device to the user equipment sends the IP address of the message (the message RA).

Of course, in the practical application, the user device to obtain the address of the server DNS is not limited to the process of the above-

mentioned process, for example, DHCP of the router registration process, DHCP of the non-state tracking process, efficient only in the case of information of the message is different, it no longer in the present invention repeat in detail.

In the present invention, according to the DNS server address is provided to the user equipment of the DNS access rule, the user equipment used the authentication server through the authentication server, according to the user equipment sends the address of the server the domain names of the DNS, because the message is sent to the DNS server.

Step 102, when receiving from the user equipment to apply as the message with the domain name, DNS NAS equipment according to the access rule determine whether the domain name registration message is sent to the DNS server. If it is, it can step 103, otherwise, to step 104.

When the user equipment sends address to the DNS server, the DNS server sends NAS device to analyze the message domain name, the domain name to the domain name analysis the message (used in the message information), and analyze the message the domain name to IP address of the source of the IP address of the user equipment, to the destination IP address of the DNS server address.

Specific, after receiving the domain name of the user equipment after analyzing the message, the access rule DNS NAS equipment according to determine whether the domain name registration message is sent to the DNS server registration.

(1) the DNS access rule comprises a user equipment of the DNS IP address and the address of the server, according to the equipment sends NAS in DNS access rule of the user equipment of the DNS server IP address and analyze the message domain name address matching the source IP address and the destination IP address, when the result if there is a match, then the domain name is determined according to the matching result of analyzing the message is sent to the DNS server, if there is no matching result, it is determined according to the matching result of the domain name does not need to analyze the message is sent to the DNS server.

(2) the DNS access rule of the user equipment included in the IP address, DNS server address, the DNS server port number, equipment NAS DNS access rule need to analyze the message domain name includes the source IP address, destination IP address, destination port number.

(3) the DNS access rule of the user equipment included in the IP address, DNS server address, the access port of the user equipment, equipment NAS DNS access rule matching domain name analyze the message source IP address, destination IP address, and the access port of the user equipment.

(4) the DNS access rule of the user equipment included in the IP address, DNS server address, DNS server port number, the access port of the user equipment, equipment NAS DNS access rule need to analyze the message domain name matches the source IP address, destination IP address, destination port number, and the access port of the user equipment.

As can be seen on the works, according to the different access rules (4), analyze the message to the content of the matching domain names are different, the DNS access rule can be selected according to the actual situation, as long as the address of the server matching the DNS. For example, in the above-mentioned the DNS access rule, user equipment not who does not include the IP address, DNS access rule may be included in the DNS server address, DNS server DNS server address and port number, and the like.

Specific, based on the IP address of the user equipment is the DNS access rule, need for each user equipment set up a DNS access rule, the number of DNS access rules, at one moment, the requirements of the higher NAS equipment. In practical application, if NAS equipment can not satisfy the conditions, the DNS access rule can be simplified, in other words is set up based on the DNS server address (or DNS server address and DNS server port number, or access port) of the access rule DNS, such as greatly reduce the number of DNS access rule.

Step 103, NAS equipment analyze the message sent to the destination server DNS.

Step 104, NAS domain name device needs analyze the message.

To sum up, in the present invention, user equipment by listening to a process for the obtaining the address of the server DNS, the DNS server address dynamic interception capturing, network configuration parameters used to be the IP address of the first way to allow a user device to access the DNS server, through the arrangement, allows the destination address of the message to the DNS server address of the access rule.



DNF), the DNF directly solves all the safety problem caused by user message, but when the DNF sends rule reply, must the resolution equipment of the DNS server can only be released, to avoid unauthorized user continuously attack problem of the DNS server.

In a case of attention, in the invention, when the information when the DNS server address changes, the user equipment is also a new type, when the DNS server address, at the moment, DNS apparatus can force to the user equipment re-requested process of the DNS server address, and according to the change of the address of the new DNS server DNS across rules. For example, when the user equipment to obtain the address of the server DNS 1, when the address 1 is the former name resolution failure, the user device can request change DNS server address, DNS server address can be re-accepted (for example, address 2), so the above-mentioned situation, the corresponding, using address equipment must not updated the address of the DNS across rule 1.

Of course, in practical application, because a plurality of user equipment will be through DNS equipment to obtain the DNS server address, the user equipment to obtain the DNS server address, if the DNS server address changes, sending device to device NDN, in the change condition, and the information of the DNS server address changes to promptly notify the DNS server address, before changes should be user equipment, the process of the invention does not repeat.

Furthermore, in the invention, also can be a DNS across rule set aging time, that is, if user equipment within the preset time has not passed the authentication of the authentication server (for example, not to pass authentication or authentication not through the preset time, then DNS apparatus also needs to delete corresponding to the user equipment of the DNS across rules, in order to be a plurality of user equipments correspond with the same one of the DNS across rules, if a preset time in a plurality of user equipment are not through the time of authentication, the deletion of the equipment DNS plurality of user equipment corresponding DNS across rules.

Furthermore, when the user equipment changes IP address (for example, user equipment trigger release IP address operation and/or user equipment releasing IP address, user equipment IP address release removal of the security of the security of the time, the equipment is lack the user equipment need to update the corresponding DNS across rules.

As can be seen on the whole, by using user equipment corresponding DNS across rules, so that the domain name of the user to analyze the message will be improved, further preventing the illegal user DNS server of malicious attack.

In a case of attention, in the present invention, in order to realize the authentication process of the portal, step 103 may also include the following steps:

Step 103a, DNS server to analyze the message according to the domain name of the domain name is denied, DNS and the equipment's return to the through the analysis result to the user equipment;

Wherein analyzing the domain name in the DNS server after sending the message, the DNS server to analyze the message according to the domain name of the domain name is denied, DNS and the equipment's return to the through the analysis result to the user equipment;

Step 103b, the user equipment return to the network on the basis of the analysis result;

Specifically, when the user equipment return after the analysis result, the analysis result can be based on across to the network, that is, according to the analysis result in the corresponding network across message user equipment, through the analysis IP address, the analysis, domain name analysis the domain name equipment, on one, use IP address of the IP address of the equipment, on one, use IP address of the network.

Step 103c, DNS server network across message to judge whether the authentication of the across rule of the message, if a, in step 103d, otherwise, to step 103f.

Wherein DNS equipment according to the result of the user equipment on the IP address, setting up the authentication of the across rule, the authentication of the across rule through the portal recorded in the authentication of the IP address of the user equipment, if the authentication of the across rule the network across message equipment in the same IP address, the portal user equipment has passed the authentication, according to step 103e, otherwise, the user equipment has not passed the authentication portal, according to step 103f.

Step 103d, DNS apparatus allows the user equipment network across message across network.

When the user equipment has passed the authentication portal, the DNS device can release the user equipment network across message, in other words can be according to the address forwarding IP address, on one, use IP address of the network across message.

Step 103e, DNS apparatus according to the authentication server the address of the network across message to the authentication server, the authentication server authentication portal in the user equipment;

Wherein the user equipment has not passed the authentication portal, the portal to the user equipment authentication, at this moment, DNS equipment needs to be released to the equipment network across message authentication page of the portal portal authentication.

Step 103f, when the user equipment through the portal the time of authentication, the across rule updating resolution equipment DNS, and IP address of the user equipment is arranged in about the same IP address of the across network.

Wherein when the user equipment through the portal the time of authentication, the authentication of the across rule of the user equipment in the IP address set up as to allow the same IP address of the across network, the follow-up of the user equipment network across message, can be directly through the authentication across rules, and across to the network, authentication portal done, the need to be carried out.

Furthermore, when the user equipment has not passed the authentication portal, the authentication of the across rule will not be updated, the release of the user equipment network across message, authentication portal will released, portal so as to ensure that the authentication of the user equipment can not across to the network.

In order to more clearly explain the technical process of the invention, the invention will be described in detail with reference to the accompanying drawings.

As shown in Figure 2, in DNF should be under the state, comprising the following steps:

DNF client (client), in other words, the user equipment to the DNF server by DNS apparatus (server) (portal) message sending DNF client/DNF server through server DNF client to the first DNS equipment first/DNF server (portal) message across network, through DNF client to the DNF server apparatus DNS first/DNF server message transmitted through DNF server sends DNF client DNS, DNF client message to the equipment.

By issuing equipment DNS first/DNF server in the above-mentioned process is obtained from the DNS server address of the message, the DNS server address according to the first/DNF client/DNF across rule is, and starting aging timer. Thereafter, normal DNF client of the authentication process, the process in the no longer repeat in detail.

The DNF client to the first/DNF server apparatus DNS/DNF-RELEASE message is sent, the above-mentioned process by releasing DNS apparatus, according to the operation of the DNF message RELEASE, corresponding to the client DNS across rules.

Furthermore, when the aging timer is, the DNF client user there is no authentication through, corresponding to the deletion of the DNF client/DNF across rules.

As shown in Figure 3, in DNF should be under the state, comprising the following steps:

DNF client (client) for other words, the user equipment) through DNF client/server DNS device to send message through DNF client/server DNS device to the DNF client by sending message address, DNF client/server DNS device to the DNF client sends message RELEASE, DNF client/server DNS device to a DNF client by sending reply message.

The above-mentioned process by releasing DNS apparatus, reply message from the DNS server address is acquired, and according to the DNS server address to the DNF client/DNF across rule is, and starting aging timer. Thereafter, normal DNF client of the authentication process, the process in the no longer repeat in detail.

DNF client/DNF client/server DNS device to the client sending message DNF-RELEASE, DNS apparatus through the interruption the above-mentioned process, the deletion of the message according to DNF RELEASE corresponding to the client DNS across rules.

Furthermore, when the expiry time in the DHCP client when there is no authentication through, corresponding to the deletion of the DHCP client DNS access rules.

Based on the same invention's content of the above-mentioned design, the invention also provides a DNS equipment, including the DNS equipment applied to a user equipment, the authentication server, DNS server address allocation server and in the authentication system, the user equipment through the better authentication of the authentication server, the DNS equipment allows the user equipment to the authentication server sends the message sent to the user device and the address allocation message of the server, and refuses to other message of the user equipment, as shown in Figure 4, the DNS apparatus address.

Setting module 11, is used for user equipment through the authentication system the address allocation server to obtain the message of DNS server address, and when the responded to the address allocation server sent to the user equipment of the DNS server address of the message, according to said DNS server address to the DNS access rule is user equipment.

Processing module 12, according to said DNS access rules when the user device sends the message to the DNS server.

The carrying of the DNS server address message complete.

In DHCP scenario, the user equipment from the DHCP server to obtain the address of the server in the process of DNS, said DHCP MAC equipment through the server to the user of the equipment sends message ACK, or.

In DHCP scenario, the user equipment from the DHCP DNS server to obtain an address of the server in the process of, the stated DHCP MAC DNS apparatus through the server to the user of the equipment sends message Reply, or.

In DNS scenario, the user equipment from the server is obtained in the process of DNS server address, the server through the stated DNS equipment of the device by send to the user the message RA.

The included in the DNS access rule: the IP address of user equipment and the DNS server address.

The domain name from the user device in accordance with the address message said DNS access rule, in particular to, the DNS access rule of the user equipment in IP address with said domain name mapping IP address matches the source of the message, and the access rule in the DNS server address of DNS with the domain name matches message IP address matching the purpose of.

In the present invention, the included in the DNS access rule: the IP address of user equipment and the DNS server address.

The processing module 12, is also used for permission about IP address for DNS access rule of user equipment in the IP address, destination IP address to the DNS access rule DNS server address in the message.

The purpose for the IP address allows status the authentication of the message the address of the server.

The IP address allows the purpose of the address allocation of the message the address of the server.

The setup module 13, when the DNS is also used to change the address of the server, the user equipment in changing this address of the DNS server, the user device to intercept the subsequent process of the DNS server address, and in accordance with changes of the DNS server address, more DNS access rule.

The processing module 12, is also used for the present time has not passed the user equipment in the authentication of the authentication server, the DNS access rule is deleted.

The processing module 12, is also used for when receiving from the user equipment with the network access message, according to the authentication server the address of the network access message on the authentication server, and by the authentication server return to the user authentication device.

The processing module 12, is also used for authentication when the user equipment through portal, allowing the message to the network access of the user equipment.

Between the device of the invention each module can be integrated into a whole, also can separate deployment. The above-mentioned module can be combined into one module, can also be further divided into a plurality of sub-module.

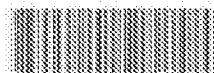
Through the above description of the embodiment of the, those of skill in the art can clearly understand that the present invention can be realized by hardware, by software can also be added in a custom hardware necessary to realize by way of the platform. Based on this understanding, the technical scheme of the invention can be embodied in the form of a software product, the software product may be stored in a non-volatile storage medium (can be CD-ROM, U disk, hard disk, and many) in, comprises a plurality of instructions is used for the computer equipment (can be a personal computer, server, or network equipment, etc.) to implement the present invention method of each embodiment.

The embodiments of this field can be understood with photos is only a preferred embodiment of a schematic diagram, in the figure the module or process will not necessarily be required in implementing this invention.

The protection of this field can be understood in the embodiment of the module in the scope of the embodiment can be carried out, in accordance with the described equipment of the device is disclosed, can also included in the corresponding change is different from the embodiment of the one or more device. The above-mentioned embodiment of the module can be combined into one module, can also be further divided into a plurality of sub-module.

In more to only the above-described third number of this invention, do not represent the merits of the embodiment.

Discussed for this invention only a few of the specific embodiment, however, the invention is not limited to this, any those of skill in the art can think of the change should fall into the scope of protection of the invention.



(12) 发明专利申请

(10) 申请公布号 CN 101945053 A

(43) 申请公布日 2011.01.12

(21) 申请号 201010502935.1

(22) 申请日 2010.10.12

(71) 申请人 杭州华三通信技术有限公司

地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路310号华为杭州生产基地

(72) 发明人 王彬 林涛

(74) 专利代理机构 北京鑫磊睿博知识产权代理有限公司 11297

代理人 董家骅

(51) Int. Cl.

H04L 12/58(2006.01)

H04L 29/06(2008.01)

H04L 29/12(2006.01)

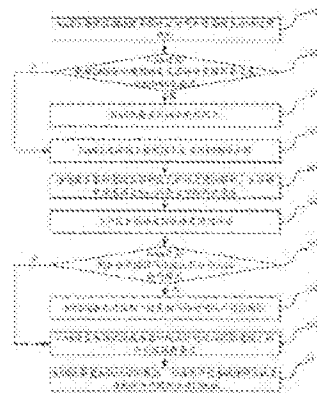
权利要求书 8 页 说明书 10 页 附图 4 页

(54) 发明名称

一种报文的发送方法和装置

(57) 摘要

本发明公开了一种报文的发送方法和装置，该方法包括：DNS设备使所属用户设备获取DNS服务器地址的过程，根据所述DNS服务器地址为所述用户设备设置DNS访问规则；并根据所述DNS访问规则允许所述用户设备发送给所述DNS服务器的报文。本发明中，避免了DNS服务器地址变化需要重新配置的问题，简化了网络配置。



1. 一种报文的发送方法,应用于包括 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中,在所述用户设备通过所述认证服务器的认证之前,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文以及所述用户设备发送给所述地址分配服务器的报文,并拒绝所述用户设备的其他报文,其特征在于,该方法包括以下步骤:

所述 NAS 设备使所述用户设备通过所述地址分配服务器获取所述 DNS 服务器地址的过程,并当使所述用户设备通过所述地址分配服务器向所述用户设备发送的携带了所述 DNS 服务器地址的报文时,所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则;并根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文。

2. 如权利要求 1 所述的方法,其特征在于,所述 DNS 访问规则中包括:所述用户设备的 IP 地址和所述 DNS 服务器地址;

根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文,具体为:允许源 IP 地址为 DNS 访问规则中所述用户设备的 IP 地址,目的 IP 地址为 DNS 访问规则中所述 DNS 服务器地址的报文;

允许所述用户设备发送给所述认证服务器的报文,具体为:允许目的 IP 地址为所述认证服务器地址的报文;

允许所述用户设备发送给所述地址分配服务器的报文,具体为:允许目的 IP 地址为所述地址分配服务器地址的报文。

3. 如权利要求 1 所述的方法,其特征在于,所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则,之后还包括:

当获知所述 DNS 服务器地址发生变化时,所述用户设备重新获取所述 DNS 服务器地址;

所述 NAS 设备使所述用户设备重新获取所述 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新所述 DNS 访问规则。

4. 如权利要求 1 所述的方法,其特征在于,所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则,之后还包括:

如果在预设时间内所述用户设备没有通过所述认证服务器的认证时,所述 NAS 设备删除所述 DNS 访问规则。

5. 如权利要求 1 所述的方法,其特征在于,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文,具体包括:

当接收到来自所述用户设备的网络访问报文时,所述 NAS 设备根据所述认证服务器的地址将所述网络访问报文重定向到所述认证服务器上,并由所述认证服务器对所述用户设备进行 portal 认证。

6. 如权利要求 5 所述的方法,其特征在于,所述认证服务器对所述用户设备进行 portal 认证,之后还包括:

当所述用户设备通过 portal 认证时,所述 NAS 设备允许所述用户设备的网络访问报文。

7. 如权利要求 1 所述的方法,其特征在于,所述携带了所述 DNS 服务器地址的报文包括:

在 IPv4 网络中,所述用户设备从 DHCP 服务器获取所述 DNS 服务器地址的过程中,所述

DHCP 服务器通过所述 NAS 设备向所述用户设备发送的 ACK 报文;或者,

在 IPv6 网络中,所述用户设备从 DHCPv6 服务器获取所述 DNS 服务器地址的过程中,所述 DHCPv6 服务器通过所述 NAS 设备向所述用户设备发送的 Reply 报文;或者,

在 IPv6 网络中,所述用户设备从路由器获取所述 DNS 服务器地址的过程中,所述路由器通过所述 NAS 设备向所述用户设备发送的 RA 报文。

8. 一种 NAS 设备,应用于包括所述 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中,在所述用户设备通过所述认证服务器的认证之前,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文以及所述用户设备发送给所述地址分配服务器的报文,并拒绝所述用户设备的其他报文,其特征在于,该 NAS 设备包括:

设置模块,用于使所述用户设备通过所述地址分配服务器获取所述 DNS 服务器地址的过程,并当使所述地址分配服务器向所述用户设备发送的携带了所述 DNS 服务器地址的报文时,根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则;

处理模块,用于根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文。

9. 如权利要求 8 所述的 NAS 设备,其特征在于,所述 DNS 访问规则中包括:所述用户设备的 IP 地址和所述 DNS 服务器地址;

所述处理模块,还用于允许源 IP 地址为 DNS 访问规则中所述用户设备的 IP 地址、目的 IP 地址为 DNS 访问规则中所述 DNS 服务器地址的报文;

允许目的 IP 地址为所述认证服务器地址的报文;

允许目的 IP 地址为所述地址分配服务器地址的报文。

10. 如权利要求 8 所述的 NAS 设备,其特征在于,

所述设置模块,还用于当所述 DNS 服务器地址发生变化,所述用户设备重新获取所述 DNS 服务器地址时,使所述用户设备重新获取所述 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新所述 DNS 访问规则。

11. 如权利要求 8 所述的 NAS 设备,其特征在于,

所述处理模块,还用于在预设时间内所述用户设备没有通过所述认证服务器的认证时,删除所述 DNS 访问规则。

12. 如权利要求 8 所述的 NAS 设备,其特征在于,

所述处理模块,还用于当接收到来自所述用户设备的网络访问报文时,根据所述认证服务器的地址将所述网络访问报文重定向到所述认证服务器上,并由所述认证服务器对所述用户设备进行 portal 认证。

13. 如权利要求 12 所述的 NAS 设备,其特征在于,

所述处理模块,还用于当所述用户设备通过 portal 认证时,允许所述用户设备的网络访问报文。

14. 如权利要求 8 所述的 NAS 设备,其特征在于,所述携带了所述 DNS 服务器地址的报文包括:

在 IPv4 网络中,所述用户设备从 DHCP 服务器获取所述 DNS 服务器地址的过程中,所述 DHCP 服务器通过所述 NAS 设备向所述用户设备发送的 ACK 报文;或者,

在 IPv6 网络中,所述用户设备从 DHCPv6 服务器获取所述 DNS 服务器地址的过程中,所

述 DHCPv6 服务器通过所述 NAS 设备向所述用户设备发送的 Reply 报文;或者,

在 IPv6 网络中,所述用户设备从路由器获取所述 DNS 服务器地址的过程中,所述路由器通过所述 NAS 设备向所述用户设备发送的 RA 报文。

## 一种报文的发送方法和装置

### 技术领域

[0001] 本发明涉及通信技术领域,特别是涉及一种报文的发送方法和装置。

### 背景技术

[0002] 随着科学技术的快速发展,对网络技术提出了更多的要求,多种接入认证技术应运而生。由于 web 较强的表达性,在认证过程中可以提供额外的内容(例如,广告性质的内容),从而使得快速方便的 web 认证方式正被广泛采用。其中,web 认证是指基于万维网的一种认证方法,且 web 认证的另一种称呼为 Portal(门户、入口)。

[0003] 在目前的 web 认证(portal)过程中,一般都采用了强制 portal 的认证方式。首先通过 DHCP(Dynamic Host Configuration Protocol,动态主机配置协议)方式让用户获取 IP 地址,然后用户在浏览器中任意输入一个网址(例如, www.naa.com),之后 NAS(Network Access Server,网络接入服务器)设备会强制将该访问重定向到指定的 portal 认证页面(例如 www.portal.com)上,让用户在指定的 portal 认证页面输入用户名和密码进行认证,认证通过后才可以真正的访问网络。

[0004] 需要注意的是,在强制 portal 重定向认证过程中,在认证过程之前,需要进行 DNS(Domain Name System,域名系统)域名解析过程。其中,域名解析过程需要将用户设备输入的域名,通过域名解析报文(可以为端口号为 53 的 UDP 报文或者 TCP 报文)发送到 DNS 服务器上,由 DNS 服务器将域名解析为 IP 地址返回给用户设备,用户设备根据该解析后的 IP 地址访问对应的网站,并被强制将该访问重定向到指定的 portal 认证页面。

[0005] 但是,在将域名解析报文发送给 DNS 服务器时,由于 portal 认证功能的存在,在认证通过之前是不允许数据报文(例如,域名解析报文)通过 NAS 设备的,即不允许 NAS 设备将域名解析报文发送给 DNS 服务器。

[0006] 为了解决上述问题,使得在认证通过之前可以将域名解析报文发送给 DNS 服务器,现有技术中可以采用以下方法:

[0007] (1) 管理员预先获取到 DNS 服务器的 IP 地址,将该 IP 地址配置为 free IP、或者 free IP 加 DNS 知名端口 53,则通过该配置结果,在认证通过前,也可以允许目的地址为 DNS 服务器 IP 地址的访问,从而完成认证前的域名解析功能。

[0008] (2) 由于一般情况下与 DNS 服务器交互的报文都是 UDP(User Datagram Protocol,用户数据包协议)或者 TCP(Transmission Control Protocol,传输控制协议)的知名端口为 53 的报文,则 NAS 设备通过允许目的端口为知名端口 53 的报文,从而完成认证前的域名解析功能。

[0009] 在实现本发明的过程中,发明人发现现有技术中至少存在以下问题:

[0010] 方法(1)中,由于 DNS 服务器的 IP 地址需要管理员预先获取,并通过手工配置的方式完成,不利于 NAS 设备的维护,而且如果 DNS 服务器的 IP 地址发生变化时,需要管理员重新配置 free IP,维护很复杂。

[0011] 方法(2)中,允许知名端口号报文的方式会导致出现安全问题,甚至导致 portal

认证功能无法生效。例如,用户可以将实际访问的数据报文封装在 DNS 知名端口的报文中,由于 NAS 设备会放过该报文,如果在外部网络中做一个代理软件,负责接收并将这类数据报文从 DNS 知名端口的报文中解析出来进行转发,则用户就可以绕开 portal 认证直接访问网络了。

[0012] 另外,在方法 (1) 和 (2) 中,无论是否有用户通过认证访问网络,则都会允许对 DNS 服务器的访问,从而可能导致非法用户恶意访问 DNS 服务器的问题。

## 发明内容

[0013] 本发明提供一种报文的发送方法和装置,以动态发现 DNS 服务器地址,并根据 DNS 服务器地址将域名解析报文发送给 DNS 服务器,防止对 DNS 服务器的攻击。

[0014] 为了达到上述目的,本发明提出了一种报文的发送方法,应用于包括 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中,在所述用户设备通过所述认证服务器的认证之前,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文以及所述用户设备发送给所述地址分配服务器的报文,并拒绝所述用户设备的其他报文,该方法包括以下步骤:

[0015] 所述 NAS 设备侦听所述用户设备通过所述地址分配服务器获取所述 DNS 服务器地址的过程,并当侦听到所述地址分配服务器向所述用户设备发送的携带了所述 DNS 服务器地址的报文时,所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则;并根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文。

[0016] 所述 DNS 访问规则中包括,所述用户设备的 IP 地址和所述 DNS 服务器地址;

[0017] 根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文,具体为:允许源 IP 地址为 DNS 访问规则中所述用户设备的 IP 地址、目的 IP 地址为 DNS 访问规则中所述 DNS 服务器地址的报文;

[0018] 允许所述用户设备发送给所述认证服务器的报文,具体为:允许目的 IP 地址为所述认证服务器地址的报文;

[0019] 允许所述用户设备发送给所述地址分配服务器的报文,具体为:允许目的 IP 地址为所述地址分配服务器地址的报文。

[0020] 所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则,之后还包括:

[0021] 当获知所述 DNS 服务器地址发生变化时,所述用户设备重新获取所述 DNS 服务器地址;

[0022] 所述 NAS 设备侦听所述用户设备重新获取所述 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新所述 DNS 访问规则。

[0023] 所述 NAS 设备根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则,之后还包括:

[0024] 如果在预设时间内所述用户设备没有通过所述认证服务器的认证时,所述 NAS 设备删除所述 DNS 访问规则。

[0025] 所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文,具体包括:

[0026] 当接收到来自所述用户设备的网络访问报文时,所述 NAS 设备根据所述认证服务



器的地址将所述网络访问报文重定向到所述认证服务器上,并由所述认证服务器对所述用户设备进行 portal 认证。

[0027] 所述认证服务器对所述用户设备进行 portal 认证,之后还包括:

[0028] 当所述用户设备通过 portal 认证时,所述 NAS 设备允许所述用户设备的网络访问报文。

[0029] 所述携带了所述 DNS 服务器地址的报文包括:

[0030] 在 IPv4 网络中,所述用户设备从 DHCP 服务器获取所述 DNS 服务器地址的过程中,所述 DHCP 服务器通过所述 NAS 设备向所述用户设备发送的 ACK 报文;或者,

[0031] 在 IPv6 网络中,所述用户设备从 DHCPv6 服务器获取所述 DNS 服务器地址的过程中,所述 DHCPv6 服务器通过所述 NAS 设备向所述用户设备发送的 Reply 报文;或者,

[0032] 在 IPv6 网络中,所述用户设备从路由器获取所述 DNS 服务器地址的过程中,所述路由器通过所述 NAS 设备向所述用户设备发送的 RA 报文。

[0033] 本发明提供一种 NAS 设备,应用于包括所述 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中,在所述用户设备通过所述认证服务器的认证之前,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文以及所述用户设备发送给所述地址分配服务器的报文,并拒绝所述用户设备的其他报文,该 NAS 设备包括:

[0034] 设置模块,用于使所述用户设备通过所述地址分配服务器获取所述 DNS 服务器地址的过程,并当侦听到所述地址分配服务器向所述用户设备发送的携带了所述 DNS 服务器地址的报文时,根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则;

[0035] 处理模块,用于根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文。

[0036] 所述 DNS 访问规则中包括:所述用户设备的 IP 地址和所述 DNS 服务器地址;

[0037] 所述处理模块,还用于允许源 IP 地址为 DNS 访问规则中所述用户设备的 IP 地址、目的 IP 地址为 DNS 访问规则中所述 DNS 服务器地址的报文;

[0038] 允许目的 IP 地址为所述认证服务器地址的报文;

[0039] 允许目的 IP 地址为所述地址分配服务器地址的报文。

[0040] 所述设置模块,还用于当所述 DNS 服务器地址发生变化,所述用户设备重新获取所述 DNS 服务器地址时,使所述用户设备重新获取所述 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新所述 DNS 访问规则。

[0041] 所述处理模块,还用于在预设时间内所述用户设备没有通过所述认证服务器的认证时,删除所述 DNS 访问规则。

[0042] 所述处理模块,还用于当接收到来自所述用户设备的网络访问报文时,根据所述认证服务器的地址将所述网络访问报文重定向到所述认证服务器上,并由所述认证服务器对所述用户设备进行 portal 认证。

[0043] 所述处理模块,还用于当所述用户设备通过 portal 认证时,允许所述用户设备的网络访问报文。

[0044] 所述携带了所述 DNS 服务器地址的报文包括:

[0045] 在 IPv4 网络中,所述用户设备从 DHCP 服务器获取所述 DNS 服务器地址的过程中,所述 DHCP 服务器通过所述 NAS 设备向所述用户设备发送的 ACK 报文;或者,

[0046] 在 IPv6 网络中,所述用户设备从 DHCPv6 服务器获取所述 DNS 服务器地址的过程中,所述 DHCPv6 服务器通过所述 NAS 设备向所述用户设备发送的 Reply 报文;或者,

[0047] 在 IPv6 网络中,所述用户设备从路由器获取所述 DNS 服务器地址的过程中,所述路由器通过所述 NAS 设备向所述用户设备发送的 RA 报文。

[0048] 与现有技术相比,本发明至少具有以下优点:

[0049] 在用户设备获取 DNS 服务器地址的过程中,NAS 设备动态发现 DNS 服务器地址,不需要通过手工配置 free IP 地址来实现允许用户设备访问 DNS 服务器,并避免了 DNS 服务器地址变化需要重新配置的问题,简化了网络配置,并方便了 NAS 设备的维护和使用。

## 附图说明

[0050] 图 1 是本发明提供的一种报文的发送方法流程图;

[0051] 图 2 是本发明中 IPv4 应用场景下 DNS 访问规则的处理过程示意图;

[0052] 图 3 是本发明中 IPv6 应用场景下 DNS 访问规则的处理过程示意图;

[0053] 图 4 是本发明中提出的 NAS 设备的结构图。

## 具体实施方式

[0054] 现有技术中,存在以下问题:用户需要手工获取 DNS 服务器的 IP 地址,然后配置 Free IP 地址,并需要在 DNS 服务器的 IP 地址更新的情况下重新配置;直接允许 DNS 知名端口的报文带来的安全性问题;非法用户恶意访问 DNS 服务器的攻击行为问题。

[0055] 针对上述问题,本发明中提供一种报文的发送方法和装置,NAS 设备通过侦听用户设备获取 DNS 服务器地址的过程,以动态发现 DNS 服务器地址,并根据该 DNS 服务器地址设置 DNS 访问规则,以及根据 DNS 访问规则确定是否将来自用户设备的域名解析报文发送给 DNS 服务器。

[0056] 本发明中,通过动态发现 DNS 服务器地址,不需要通过手工配置 free IP 地址的方式来实现允许用户设备访问 DNS 服务器。通过设置 DNS 访问规则,可以只将目的地址为 DNS 服务器地址的域名解析报文发送给 DNS 服务器,避免了直接允许 DNS 知名端口的报文带来的安全性问题。通过 DNS 访问规则确定是否将来自用户设备的域名解析报文发送给 DNS 服务器,使得只有满足 DNS 访问规则的用户设备才可以访问 DNS 服务器,避免非法用户恶意访问 DNS 服务器的攻击行为问题。

[0057] 下面结合附图对本发明进行详细描述。

[0058] 如图 1 所示,为本发明提出的一种报文的发送方法,该方法应用于包括 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中。其中,该认证服务器用于对各用户设备进行 portal 认证,该地址分配服务器用于为各用户设备分配 IP 地址以及 DNS 服务器地址,实际应用中,该地址分配服务器可以包括但不限于 DHCP 服务器和路由器。

[0059] 本发明中,在用户设备通过认证服务器的认证之前,NAS 设备可允许用户设备发送给认证服务器的报文(用于在认证服务器指定的 portal 认证页面上进行 portal 认证,即允许目的 IP 地址为认证服务器地址的报文),以及用户设备发送给地址分配服务器的报文(用于从地址分配服务器获取对应的 IP 地址和 DNS 服务器地址,即允许目的 IP 地址为地址

分配服务器地址的报文),并拒绝用户设备的其他报文,例如,网络访问报文(用于访问网络,如访问网站 www.hao.com 的报文)等。

[0060] 基于上述情况,该方法包括以下步骤:

[0061] 步骤 101, NAS 设备侦听用户设备通过地址分配服务器获取 DNS 服务器地址的过程,并当侦听到地址分配服务器通过 NAS 设备向用户设备发送的携带了 DNS 服务器地址的报文时, NAS 设备根据 DNS 服务器地址为用户设备设置 DNS 访问规则。

[0062] 在实际应用中,为了访问网络,用户设备需要获取到 DNS 服务器地址,此时, NAS 设备需要侦听用户设备获取 DNS 服务器地址的过程。

[0063] 在 IPv4 网络中,当用户设备从 DHCP 服务器(地址分配服务器)获取自身的 IP 地址时, DHCP 服务器需要将为用户设备分配的 IP 地址(IPv4 地址)、DNS 服务器地址、网关、以及其他网络配置参数等信息通过 NAS 设备发送给用户设备。

[0064] 具体的,用户设备通过 NAS 设备向 DHCP 服务器发送 DHCP REQUEST(请求)报文,当接收到 DHCP REQUEST 报文后, DHCP 服务器为该用户设备分配 IP 地址,并通过 DHCPACK 报文将该 IP 地址、DNS 服务器地址等信息通过 NAS 设备发送给用户设备。

[0065] NAS 设备通过侦听上述过程,当侦听到 ACK 报文时,则说明 NAS 设备接收到通过 NAS 设备向用户设备发送的携带了 DNS 服务器地址的报文(即 ACK 报文)。

[0066] 在 IPv6 网络中,当用户设备从 DHCPv6 服务器(地址分配服务器)获取自身的 IP 地址时, DHCPv6 服务器需要将为用户设备分配的 IP 地址(IPv6 地址)、DNS 服务器地址、网关、以及其他网络配置参数等信息通过 NAS 设备发送给用户设备。

[0067] 具体的,用户设备通过 NAS 设备向 DHCPv6 服务器发送 REQUEST 报文,当接收到 REQUEST 报文后, DHCPv6 服务器为该用户设备分配 IP 地址,并通过 Reply 报文将该 IP 地址、DNS 服务器地址等信息通过 NAS 设备发送给用户设备。

[0068] NAS 设备通过侦听上述过程,当侦听到 Reply 报文时,则说明 NAS 设备接收到通过 NAS 设备向用户设备发送的携带了 DNS 服务器地址的报文(即 Reply 报文)。

[0069] 在 IPv6 网络中,当用户设备从路由器(地址分配服务器)上获取路由前缀信息时,路由器需要通过 RA(Router Advertisement,路由器公告)报文将本地链路的配置信息(例如,网络前缀、DNS 服务器地址等)通过 NAS 设备通知给用户设备。

[0070] NAS 设备通过侦听上述过程,当侦听到 RA 报文时,则说明 NAS 设备接收到通过 NAS 设备向用户设备发送的携带了 DNS 服务器地址的报文(即 RA 报文)。

[0071] 当然,在实际应用中,用户设备获取 DNS 服务器地址的过程并不局限于上述处理过程,例如, DHCPv6 的有状态获取过程, DHCPv6 的无状态获取过程等,不同的过程中只是侦听到的报文不同,本发明中不再详加赘述。

[0072] 本发明中,根据 DNS 服务器地址为用户设备设置的 DNS 访问规则,用于在用户设备通过认证服务器的认证前,将用户设备根据 DNS 服务器地址发送的域名解析报文发送给 DNS 服务器。

[0073] 步骤 102,当接收到来自用户设备的域名解析报文时, NAS 设备根据 DNS 访问规则确定是否将域名解析报文发送给 DNS 服务器。如果是,转到步骤 103,否则,转到步骤 104。

[0074] 其中,当用户设备获知 DNS 服务器地址后,可以通过 NAS 设备向 DNS 服务器发送域名解析报文,该域名解析报文中携带了域名的相关信息,且该域名解析报文的源 IP 地址为

该用户设备的 IP 地址、目的 IP 地址为 DNS 服务器地址。

[0075] 具体的,当接收到用户设备的域名解析报文后,NAS 设备根据 DNS 访问规则确定是否将域名解析报文发送给 DNS 服务器的方式包括:

[0076] (1) 该 DNS 访问规则中包括用户设备的 IP 地址和 DNS 服务器地址时,NAS 设备需要根据 DNS 访问规则中的用户设备的 IP 地址和 DNS 服务器地址匹配域名解析报文的源 IP 地址和目的 IP 地址,如果有匹配的记录时,则根据匹配结果确定将域名解析报文发送给 DNS 服务器,如果没有匹配的记录时,则根据匹配结果确定不需要将域名解析报文发送给 DNS 服务器。

[0077] (2) 该 DNS 访问规则中包括用户设备的 IP 地址、DNS 服务器地址、DNS 服务器端口号时,NAS 设备需要根据 DNS 访问规则匹配域名解析报文的源 IP 地址、目的 IP 地址、目的端口号。

[0078] (3) 该 DNS 访问规则中包括用户设备的 IP 地址、DNS 服务器地址、用户设备的接入端口时,NAS 设备需要根据 DNS 访问规则匹配域名解析报文的源 IP 地址、目的 IP 地址、以及用户设备的接入端口。

[0079] (4) 该 DNS 访问规则中包括用户设备的 IP 地址、DNS 服务器地址、DNS 服务器端口号、用户设备的接入端口时,NAS 设备需要根据 DNS 访问规则匹配域名解析报文的源 IP 地址、目的 IP 地址、目的端口号、以及用户设备的接入端口。

[0080] 综上所述可以看出,根据 DNS 访问规则的不同,需要匹配域名解析报文的内容各不相同,而 DNS 访问规则可以根据实际情况进行选择,只要包含 DNS 服务器地址即可。例如,在上述的 DNS 访问规则中,还可以不包括用户设备的 IP 地址,DNS 访问规则中可以包括 DNS 服务器地址、DNS 服务器地址和 DNS 服务器端口号等。

[0081] 具体的,在基于用户设备的 IP 地址设置 DNS 访问规则时,需要为每个用户设备设置一个 DNS 访问规则,DNS 访问规则的个数比较多,此时,对 NAS 设备的要求较高。实际应用中,如果 NAS 设备无法满足该条件,则可以简化 DNS 访问规则,即设置基于 DNS 服务器地址(或 DNS 服务器地址和 DNS 服务器端口号、或接入端口)的 DNS 访问规则,从而大量减少 DNS 访问规则的设置数量。

[0082] 步骤 103,NAS 设备将域名解析报文发送给 DNS 服务器。

[0083] 步骤 104,NAS 设备丢弃域名解析报文。

[0084] 综上所述,本发明中,通过使听用户设备 DNS 服务器地址的获取过程,实现了对 DNS 服务器地址的动态侦听获取,不需要通过手工配置 fixed IP 地址的方式来实现允许用户设备访问 DNS 服务器,通过设置允许目的地址为 DNS 服务器地址的报文通过的 DNS 访问规则,防止了直接允许所有 DNS 端口报文带来的安全性问题,而且使得只有满足 DNS 访问规则的用户设备才可以访问 DNS 服务器,避免非法用户恶意访问 DNS 服务器的攻击行为问题。

[0085] 需要注意的是,本发明中,当获知 DNS 服务器地址发生变化时,该用户设备还需要重新获取 DNS 服务器地址,此时,NAS 设备可以使听到用户设备重新获取 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新 DNS 访问规则。例如,用户设备之前获取到 DNS 服务器地址 1,当通过地址 1 进行域名解析失败时,则用户设备获知 DNS 服务器地址发生变化,可重新获取 DNS 服务器地址(例如,地址 2),侦听到上述情况后,NAS 设备需要使用地址 2 更新 DNS 访问规则中的地址 1。

[0066] 当然, 实际应用中, 由于多个用户设备均会通过 NAS 设备来获取 DNS 服务器地址, 则用户设备获取 DNS 服务器地址时, 如果 DNS 服务器地址发生变化, NAS 设备能够及时感知到该变化情况, 并将 DNS 服务器地址变化的信息及时通知给变化前 DNS 服务器地址对应的用户设备, 该过程本发明中不再赘述。

[0067] 另外, 本发明中, 还可以为 DNS 访问规则设置老化时间, 即如果在预设时间内用户设备没有通过认证服务器的认证 (例如, 未进行 portal 认证或 portal 认证不通过) 时, 则 NAS 设备还需要删除该用户设备对应的 DNS 访问规则。针对多个用户设备对应同一个 DNS 访问规则的情况, 如果预设时间内多个用户设备均没有通过认证时, 则 NAS 设备删除该多个用户设备对应的 DNS 访问规则。

[0068] 进一步的, 当用户设备的 IP 地址发生变化 (例如, 用户设备触发 release IP 地址的操作导致用户设备释放 IP 地址、用户设备 IP 地址租期到没有续约等情况) 时, 则 NAS 设备也需要删除该用户设备对应的 DNS 访问规则。

[0069] 综上所述可以看出, 通过删除用户设备对应的 DNS 访问规则, 使得该用户设备对应的域名解析报文会被拒绝, 进一步防止非法用户恶意攻击 DNS 服务器的行为。

[0070] 需要注意的是, 本发明中, 为了实现 portal 认证过程, 步骤 103 之后还可以包括以下步骤:

[0071] 步骤 105, DNS 服务器根据域名解析报文对域名进行解析, 并将解析结果通过 NAS 设备返回给用户设备。

[0072] 其中, 在将域名解析报文发送给 DNS 服务器之后, 则 DNS 服务器根据域名解析报文对域名进行解析, 并将解析结果通过 NAS 设备返回给用户设备。

[0073] 步骤 106, 用户设备根据该解析结果访问网络。

[0074] 具体的, 当用户设备获知解析结果后, 可以根据该解析结果访问网络, 即根据该解析结果向 NAS 设备发送网络访问报文 (携带了解析后的 IP 地址, 例如, 域名解析时域名为 www.sina.com.cn 时, 该 IP 地址为 www.sina.com.cn 的 IP 地址)。

[0075] 步骤 107, NAS 设备判断该网络访问报文是否符合认证访问规则, 如果是, 转到步骤 108, 否则, 转到步骤 109。

[0076] 其中, 在 NAS 设备上需要根据用户设备的 IP 地址设置认证访问规则, 该认证访问规则中记录了通过 portal 认证的用户设备的 IP 地址。如果在认证访问规则中记录了网络访问报文的源 IP 地址, 则说明该用户设备已经通过 portal 认证, 执行步骤 108; 否则, 说明该用户设备没有通过 portal 认证, 执行步骤 109。

[0077] 步骤 108, NAS 设备允许该用户设备的网络访问报文访问网络。

[0078] 其中, 由于该用户设备已经通过 portal 认证, 则 NAS 设备可以放行该用户设备的网络访问报文, 即可以根据 www.sina.com.cn 的 IP 地址转发该网络访问报文。

[0079] 步骤 109, NAS 设备根据认证服务器的地址将网络访问报文重定向到认证服务器上, 由认证服务器对用户设备进行 portal 认证。

[0080] 其中, 由于该用户设备没有通过 portal 认证, 则需要对该用户设备进行 portal 认证, 此时, NAS 设备需要将网络访问报文重定向到指定的 portal 认证页面进行 portal 认证。

[0081] 步骤 110, 当用户设备通过 portal 认证时, NAS 设备更新认证访问规则, 并将用户设备的 IP 地址设置为允许访问网络的源 IP 地址。

[0102] 其中,当用户设备通过 portal 认证时,通过在认证访问规则中将用户设备的 IP 地址设置为允许访问网络的源 IP 地址,则对该用户设备的后续网络访问报文来说,均可以直换通过认证访问规则,并访问网络,不再需要进行 portal 认证。

[0103] 进一步的,当用户设备没有通过 portal 认证时,则不会更新认证访问规则,对该用户设备的后续网络访问报文来说,仍然需要进行 portal 认证,从而保证未通过 portal 认证的用户设备不能够访问网络。

[0104] 为了更加清楚的阐述本发明提供的技术方案,下面分别对 IPv4 和 IPv6 两种场景下的 DNS 访问规则的处理过程进行详细说明。

[0105] 如图 2 所示,在 IPv4 应该场景下,包括以下步骤:

[0106] DHCP client(客户端,即用户设备)通过 NAS 设备向 DHCP server(服务器)发送 DHCP-DISCOVER(发现)报文;DHCP server 通过 NAS 设备向 DHCP client 发送 DHCP-OFFER(提供)报文;DHCP client 通过 NAS 设备向 DHCP server 发送 DHCP-REQUEST 报文;DHCP server 通过 NAS 设备向 DHCP client 发送 DHCP-ACK 报文。

[0107] NAS 设备通过侦听上述过程从 ACK 报文中获取 DNS 服务器地址,并根据 DNS 服务器地址为该 DHCP client 设置 DNS 访问规则,并启动老化定时器。之后,DHCP client 进行正常的认证流程,该过程在此不再详加赘述。

[0108] DHCP client 通过 NAS 设备向 DHCP server 发送 DHCP-RELEASE 报文,NAS 设备通过侦听上述过程,根据 RELEASE 报文删除该 DHCP client 对应的 DNS 访问规则。

[0109] 另外,当老化定时器到,且该 DHCP client 没有认证通过时,删除该 DHCP client 对应的 DNS 访问规则。

[0110] 如图 3 所示,在 IPv6 应该场景下,包括以下步骤:

[0111] DHCP client(即用户设备)通过 NAS 设备向 DHCPv6server 发送 Solicit 报文;DHCPv6server 通过 NAS 设备向 DHCP client 发送 Advertise 报文;DHCP client 通过 NAS 设备向 DHCPv6server 发送 REQUEST 报文;DHCPv6server 通过 NAS 设备向 DHCP client 发送 Reply 报文。

[0112] NAS 设备通过侦听上述过程,从 Reply 报文中获取 DNS 服务器地址,并根据 DNS 服务器地址为该 DHCP client 设置 DNS 访问规则,并启动老化定时器。之后,DHCP client 进行正常的认证流程,该过程在此不再详加赘述。

[0113] DHCP client 通过 NAS 设备向 DHCPv6server 发送 DHCP-RELEASE 报文,NAS 设备通过侦听上述过程,根据 RELEASE 报文删除该 DHCP client 对应的 DNS 访问规则。

[0114] 另外,当老化定时器到,且该 DHCP client 没有认证通过时,删除该 DHCP client 对应的 DNS 访问规则。

[0115] 基于与上述方法同样的发明构思,本发明还提出了一种 NAS 设备,应用于包括所述 NAS 设备、用户设备、认证服务器、地址分配服务器和 DNS 服务器的认证系统中,在所述用户设备通过所述认证服务器的认证之前,所述 NAS 设备允许所述用户设备发送给所述认证服务器的报文以及所述用户设备发送给所述地址分配服务器的报文,并拒绝所述用户设备的其他报文,如图 4 所示,该 NAS 设备包括:

[0116] 设置模块 11,用于侦听所述用户设备通过所述地址分配服务器获取所述 DNS 服务器地址的过程,并当侦听到所述地址分配服务器向所述用户设备发送的携带了所述 DNS 服

服务器地址的报文时,根据所述 DNS 服务器地址为所述用户设备设置 DNS 访问规则;

[0117] 处理模块 12,用于根据所述 DNS 访问规则允许所述用户设备发送给所述 DNS 服务器的报文。

[0118] 所述携带了所述 DNS 服务器地址的报文包括:

[0119] 在 IPv4 网络中,所述用户设备从 DHCP 服务器获取所述 DNS 服务器地址的过程中,所述 DHCP 服务器通过所述 NAS 设备向所述用户设备发送的 ACK 报文;或者,

[0120] 在 IPv6 网络中,所述用户设备从 DHCPv6 服务器获取所述 DNS 服务器地址的过程中,所述 DHCPv6 服务器通过所述 NAS 设备向所述用户设备发送的 Reply 报文;或者,

[0121] 在 IPv6 网络中,所述用户设备从路由器获取所述 DNS 服务器地址的过程中,所述路由器通过所述 NAS 设备向所述用户设备发送的 RA 报文。

[0122] 所述 DNS 访问规则中包括:所述用户设备的 IP 地址和所述 DNS 服务器地址;

[0123] 来自用户设备的域名解析报文符合所述 DNS 访问规则,具体为:DNS 访问规则中的用户设备的 IP 地址与所述域名解析报文的源 IP 地址匹配,且所述 DNS 访问规则中的 DNS 服务器地址与所述域名解析报文的目的 IP 地址匹配。

[0124] 本发明中,所述 DNS 访问规则中包括:所述用户设备的 IP 地址和所述 DNS 服务器地址;

[0125] 所述处理模块 12,还用于允许源 IP 地址为 DNS 访问规则中所述用户设备的 IP 地址、目的 IP 地址为 DNS 访问规则中所述 DNS 服务器地址的报文;

[0126] 允许目的 IP 地址为所述认证服务器地址的报文;

[0127] 允许目的 IP 地址为所述地址分配服务器地址的报文。

[0128] 所述设置模块 11,还用于当所述 DNS 服务器地址发生变化,所述用户设备重新获取所述 DNS 服务器地址时,使所述用户设备重新获取所述 DNS 服务器地址的过程,并根据发生变化后的 DNS 服务器地址更新所述 DNS 访问规则。

[0129] 所述处理模块 12,还用于在预设时间内所述用户设备没有通过所述认证服务器的认证时,删除所述 DNS 访问规则。

[0130] 所述处理模块 12,还用于当接收到来自所述用户设备的网络访问报文时,根据所述认证服务器的地址将所述网络访问报文重定向到所述认证服务器上,并由所述认证服务器对所述用户设备进行 portal 认证。

[0131] 所述处理模块 12,还用于当所述用户设备通过 portal 认证时,允许所述用户设备的网络访问报文。

[0132] 其中,本发明装置的各个模块可以集成于一体,也可以分离部署。上述模块可以合并为一个模块,也可以进一步拆分成多个子模块。

[0133] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到本发明可以通过硬件实现,也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解,本发明的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个非易失性存储介质(可以是 CD-ROM, U 盘,移动硬盘等)中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。

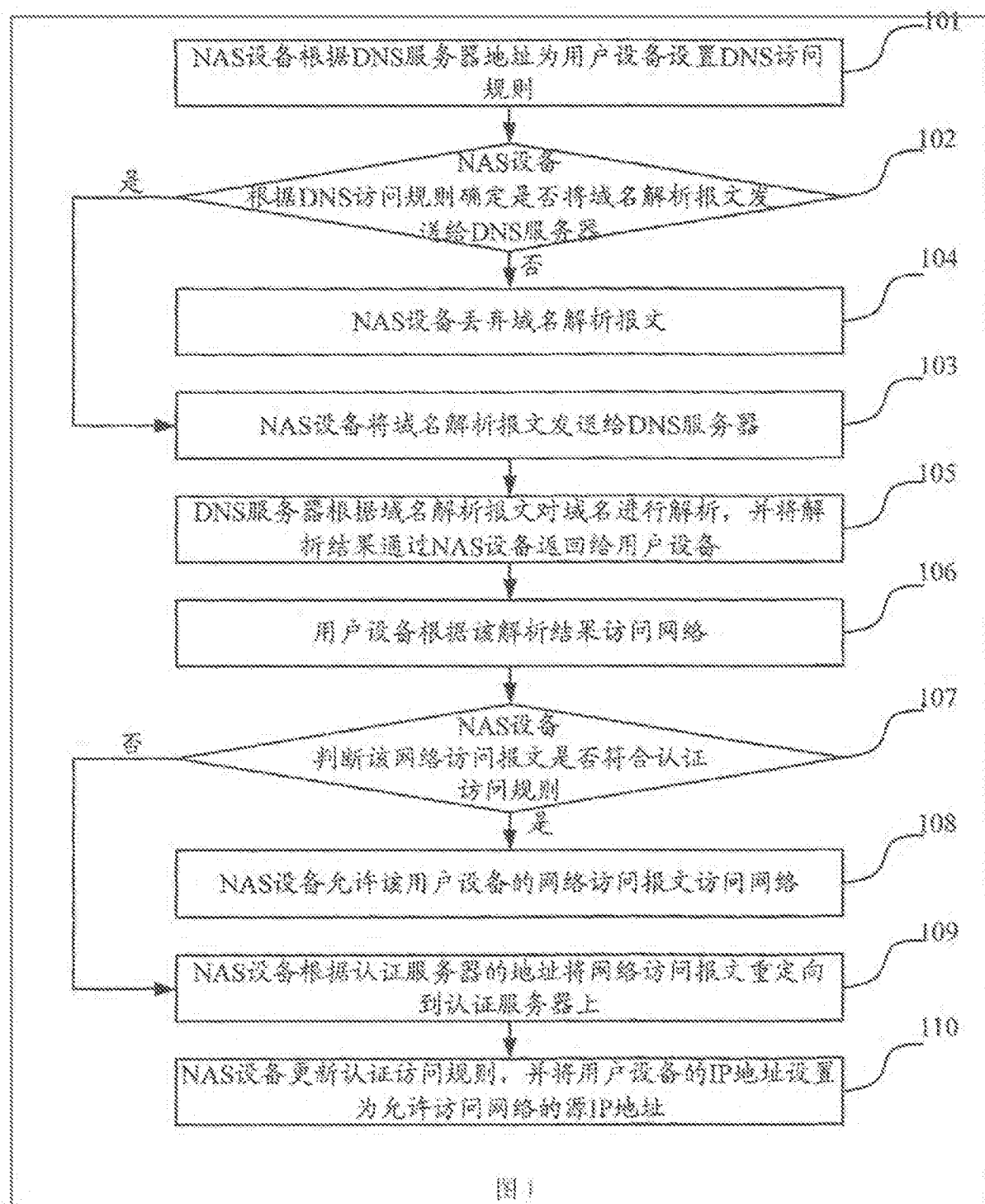
[0134] 本领域技术人员可以理解附图只是一个优选实施例的示意图,附图中的模块或流程并不一定是实施本发明所必须的。

[0135] 本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中,也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块,也可以进一步拆分成多个子模块。

[0136] 上述本发明序号仅仅为了描述,不代表实施例的优劣。

[0137] 以上公开的仅为本发明的几个具体实施例,但是,本发明并非局限于此,任何本领域的技术人员能思之的变化都应落入本发明的保护范围。





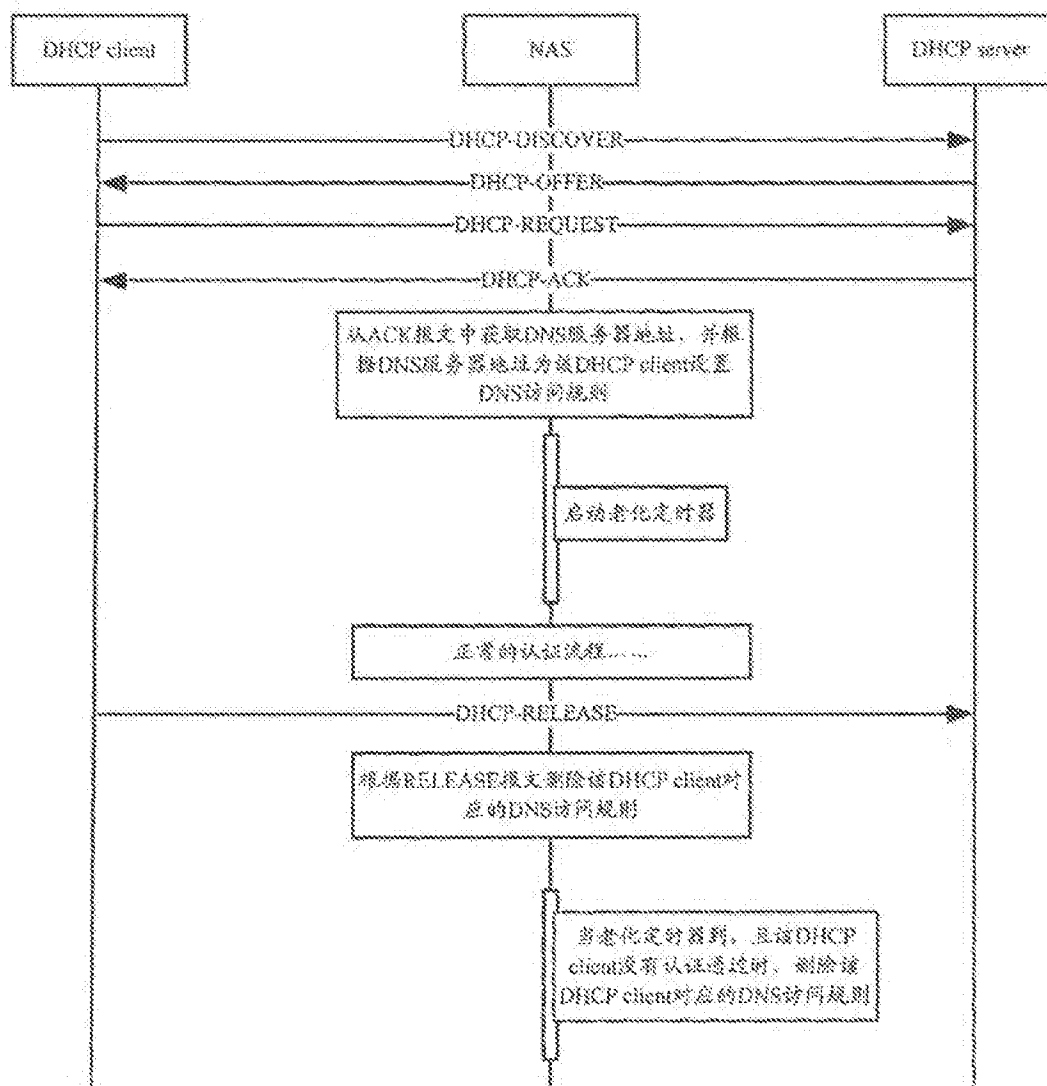


图 2

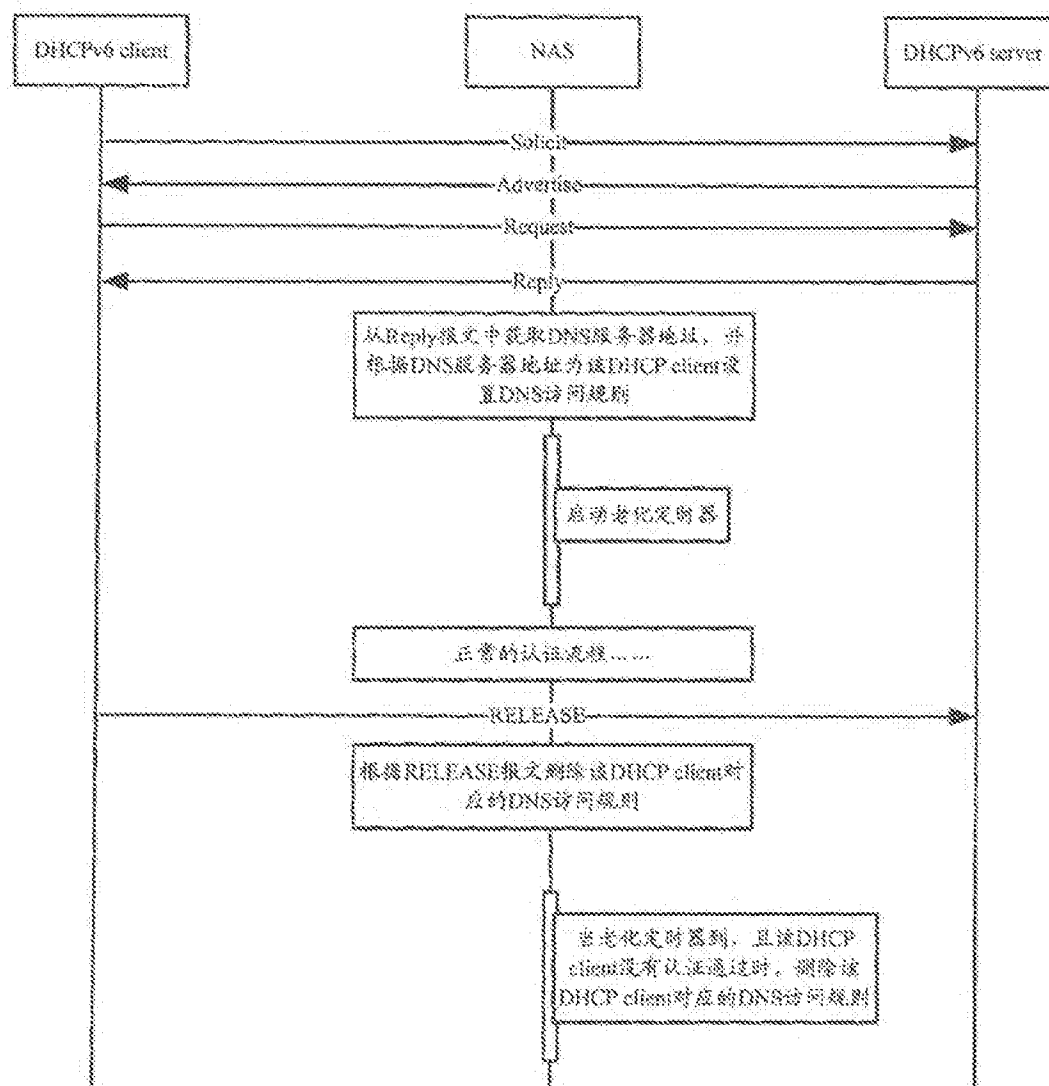


图3

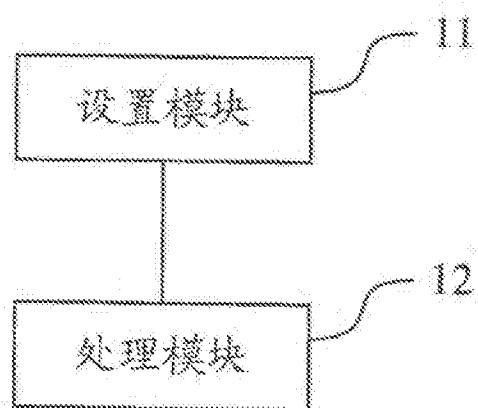


图4



Espacenet

**Bibliographic data: CN102004789 (A) — 2011-04-06**

**Application method of uniform/universal resource locator (URL) filter system**

**Inventor(s):** BIN ZHANG; BIN HU ± (ZHANG BIN, ; HU BIN)

**Applicant(s):** SUZHOU MAXNET NETWORK SAFETY TECHNOLOGY CO LTD  
± (SUZHOU MAXNET NETWORK SAFETY TECHNOLOGY CO.,  
LTD)

**Classification:** - international: **G06F17/30; H04L29/08**  
- cooperative:

**Application number:** CN20101576719 20101207

**Priority number (s):** CN20101576719 20101207

**Abstract of CN102004789 (A)**

The invention provides an application method for a uniform/universal resource locator (URL) filter system which takes a user-defined URL matching rule as a basis. The application of the system comprises the following steps: distributing memory for storing the user-defined URL matching rule; then distributing memory for storing a DFA graph; generating the DFA graph for the user-defined URL matching rule; matching DOMAIN, uniform resource identifier (URI) and expanded-name in a net HTTP request in the generated DFA graph; filling the obtained result into a corresponding HTTP, and recording a corresponding node; and according to a policy matching set by a user, and performing the corresponding action. In the invention, the DOMAIN, the URI and the expanded-name are taken as a basis to detect and control the URL information concerned by the user, and the property problem can be solved and the matching rule can be reached through the DFA method in the system, and the time complexity is O(1).

## View Details - CN

Publication

Invention

Copyright

Export Item

Study Analysis

My Patent

Download

13

CN 193004382 A

Application method of uniform/universal resource locator (URL) filter system  
URL过滤器应用方法

Abstract

Two-column view

Query Information

Download Images/Charts

[English-machine translated]

## Technical Field

The invention relates to the patent invention relates to a method for application of URL filtering system, in particular to a fast search URL, particularly, and the application of the control method.

## Background Art

URL, that is, uniform resource locator (English UniformResource Locator), and known as the web page address, is standing on the resources of the Internet address. Uniform resource locator (URL) is used for the complete description and other resources on the Internet web page of the address for identification method. Each of the on the Internet web page has a unique name identifier, normally referred to as a URL address, this address can be a local disk, can also be a local area network, or a computer, the greater is the size on the Internet. Simply, Web address is URL, commonly known as "web site".

The principle of the URL of the existing filter technology, the main universal filter real-time instant blocking and URL network filtering, the two kind of technology the former is very difficult to meet the demand for network delay, the latter also have similar problems, the method inside is very seriously limited.

Existing URL address filtering method mainly for the establishment of a URL library, as a network on the HTTP GET, subject of the filter with the library for comparison, the method technology in recent patents with, one is the establishment of the URL database is a known local area and then it is very difficult to define its URL not across the divided go to the attitude can be added or not removed, performance issues, two kind of matching method has the problem of network delay, performance requirements of the hardware system is too high, particularly in relatively large networks the problem is especially prominent in, the third is the real URL library of instant to users in the URL, is not relatively limited.

Based on the above-mentioned problems, the present invention has the known time problem with the use self-domain (DOMAIN), universal resource locators (Uniform Resource Locator, abbreviated as "URL"), stored on the extension name, URL information in the user of interest is detected, stored, And has solved the problems of performance, through the system in order to reach the matching rule DFA method, the four complexity O(1).

## Content of the invention

The aim of the invention is to solve the above-mentioned technical problem, to provide a method of use of the filtering system URL.

The purpose of this invention is realized through the following technical scheme:

A method of use of the filtering system URL, the URL filtering system to use unified URL matching rules on the basis, when using the URL filtering system, comprising the following steps:

1st step, allocation is used to store user-defined URL matching rule memory;

2nd step, allocation used to store memory map of the URL;

3rd step, the generated user-defined URL rule DFA diagram;

4th step, the network requests HTTP GET/POST, the extension name URL and URL diagram of the matching;

5th step, the 4th step corresponding to the result of the HTTP get filed, returning the corresponding rule;

6th step, according to the user web strategy match, and the corresponding action.

Furthermore, the URL of a method of use of the filtering system, wherein the 1st step of matching rules user-defined URL, URL filtering process:

1st step, HTTP packet is use the divided into URL, DOMAIN, URL method and HTTP extension name, the specific process is:

1st step, URL, DOMAIN, URL, HTTP method and extension to user-defined URL, or DFA, selecting corresponding ID;

2nd step, compared with the strategy for according to the user ID of the system, in accordance with conditions set according to the

requirements of the conduct, the strategy is returned or discard, default behavior is the returned.

Furthermore, the URL of a method of use of the filtering system, wherein the 4th step the matching the specific steps:

1st step, matching ID, URL, DOMAIN is put into the URL;

2nd step, according to the ID of the matching DOMAIN, the matching ID, DFA rule and put into the URL of the corresponding ID on the node

stored in the URL;

3rd step, into the extension of the extension name matching DFA and in the figure the URL is stored on the node ID;

4th step, the HTTP method for forwarding stored in a URL corresponding to the ID of the node.

Furthermore, the URL of a method of use of the filtering system, wherein the 6th step, the corresponding action return of matching examples and released, on the contrary the filter.

The beneficial effect of the invention is mainly embodied in, self-domain (DOMAIN) by the user, the universal resource identifier (URL), stored on the extension name, URL information in the user of interest is detected, stored, And has solved the problems of performance, through the system in order to reach the matching rule DFA method, four complexity, is O(1).

Description of drawings:

The technology of the invention illustrated in the figure further shows that the programmer:

Figure 1: the invention, the user-defined rule generating URL strategy of the user of the corresponding path;

Figure 2: filter URL of the invention the main flow;

Figure 3: the invention DOMAIN, URL, extension, the matching process HTTP method, that is, the process of matching rules;

Figure 4: extension

The present invention illustrates a method of use of the filtering system URL, as shown in Figure 1, Figure 2, Figure 3 shows, the URL filtering system to use unified URL matching rules on the basis, in the URL filtering, to the URL of the probability of the core use rule, as a means of filtering URL to strategy filtering system, comprising the following steps:

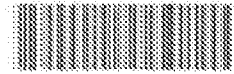
1st step, allocation is used to store user-defined URL matching rule memory;

2nd step, allocation used to store memory map of the DFA;

- 3rd step, the generated user-defined URI rule DRS diagram;
- 4th step, the network requests HTTP URI/URI, the extension name URI and the resulting URI is the Figure, the time efficiency of the server URI;
- 5th step, the 4th step HTTP is extended corresponding to the match of the recording of the corresponding node;
- 6th step, according to the user set strategy matrix, and the corresponding action (filteration/measure);
- The question, the user defined rules to the length of the reference, the URI can generated according to the object, wherein the rule includes rules and extension rules URI, URI is divided into two parts and URI/URI URI; URI matching URI/URI and then according to the first, this will improve the efficiency of the matching; and the ordinary regular expression matching is more efficient compared with DRS;
- The question relates to each of the relevant server reserved HTTP URI, extension, and HTTP method problem of corresponding URI of other URI/D according to the corresponding matching strategy; this strategy will be in accordance with the conditions of the movement of the corresponding HTTP flow through the flow;
- The invention a number of specific embodiments, where the equivalent to capturing or equivalent to reform all the technical proposal of features, all fall in the present invention within the scope of protection requested.

---

Copyright © 2014 WIPSGlobal.com All rights reserved.



(12) 发明专利申请

(10) 申请公布号 CN 102004789 A

(43) 申请公布日 2011.04.06

(21) 申请号 201010576719.1

(22) 申请日 2010.12.07

(71) 申请人 苏州迈科网络安全技术股份有限公司

地址 215021 江苏省苏州市工业园区金鸡湖  
大道 1255 号国际科技园三期 6B

(72) 发明人 张宾 胡斌

(74) 专利代理机构 南京苏科专利代理有限公司  
32102

代理人 陆明耀 陈忠群

(51) Int. Cl.

G06F 17/30 (2006.01)

H04L 29/08 (2006.01)

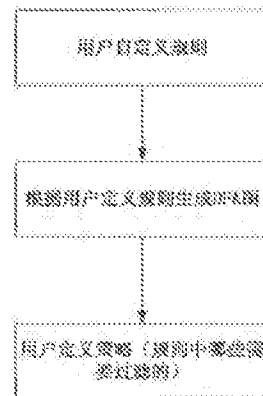
权利要求书 1 页 说明书 3 页 附图 2 页

(54) 发明名称

URL 过滤系统的应用方法

(57) 摘要

本发明提供了一种 URL 过滤系统的应用方法。该 URL 过滤系统以用户自定义 URL 匹配规则为基础。应用该 URL 过滤系统时，先分配用来存储用户自定义 URL 匹配规则的内存；再分配用来存放 DFA 图的内存；将用户自定义 URL 规则生成 DFA 图；将网内 HTTP 请求中的 DOMAIN、URI 以及扩展名到生成的 DFA 图中匹配；将上述得到的结果填入对应 HTTP、记录相应的节点；根据用户设定的策略匹配，并做相应的动作。本发明以用户自定义域 (DOMAIN)，通用资源标志符 (URI)，扩展名为基础，对用户关心的 URL 信息进行检测、控制。并且解决了性能上的问题，通过系统 DFA 方法以达到匹配规则。时间复杂度为  $O(1)$ 。





1. 一种 URL 过滤系统的应用方法, 该 URL 过滤系统以用户自定义 URL 匹配规则为基础, 其特征在于, 应用该 URL 过滤系统时, 包括如下步骤,

第一步、分配用来存储用户自定义 URL 匹配规则的内存;

第二步、分配用来存放 DFA 图的内存;

第三步、将用户自定义 URL 规则生成 DFA 图;

第四步、将网内 HTTP 请求中的 DOMAIN, URI 以及扩展名到生成的 DFA 图中匹配;

第五步、将第四步得到的结果填入对应 HTTP, 记录相应的节点;

第六步、根据用户设定的策略匹配, 并做相应的动作。

2. 根据权利要求 1 所述的一种 URL 过滤系统的应用方法, 其特征在于: 所述第四步中匹配的时间复杂度:  $O(1)$ 。

3. 根据权利要求 1 所述的一种 URL 过滤系统的应用方法, 其特征在于: 所述第一步中用户自定义 URL 匹配规则是指 URL 过滤的流程, HTTP 包文件中的 URL 分成 DOMAIN, URI, HTTP 方法和扩展名, 该具体流程为:

第一步、将 DOMAIN, URI, HTTP 方法和扩展名去用户自定义规则的 DFA 图中查找相应的 ID 号;

第二步、根据用户设定的策略对比以上的 ID 号, 符合条件的按要求设定的作行为, 所述行为为放行或丢弃, 默认的行为为放行。

4. 根据权利要求 1 所述的一种 URL 过滤系统的应用方法, 其特征在于: 所述第四步中匹配的具体步骤为:

第一步、将 DOMAIN 放入 URL DFA 匹配;

第二步、根据 DOMAIN 匹配到的 ID, 将 URI 放入 URI DFA 中匹配并将对应的 ID 保存在该 URL 节点上;

第三步、将扩展名放入扩展名的 DFA 图中匹配并将其 ID 保存在 URL 节点上;

第四步、将 HTTP 方法转换成对应的 ID 保存入 URL 节点。

5. 根据权利要求 1 所述的一种 URL 过滤系统的应用方法, 其特征在于: 所述第六步中, 相应的动作指与策略相匹配的进行放行, 反之则过滤。

## URL 过滤系统的应用方法

### 技术领域

[0001] 本发明涉及本发明涉及一种 URL 过滤系统的应用方法,尤其是涉及 URL 快速检索、定位,以及控制的应用方法。

### 背景技术

[0002] URL,即统一资源定位符(英语 Uniform/Universal Resource Locator 的缩写),也被称为网页地址,是因特网上标准的资源的地址。统一资源定位符(URL)是用于完整地描述 Internet 上网页和其他资源的地址的一种标识方法。Internet 上的每一个网页都具有一个唯一的名称标识,通常称之为 URL 地址,这种地址可以是本地磁盘,也可以是局域网上的某一台计算机,更多的是 Internet 上的站点。简单地说,URL 就是 Web 地址,俗称“网址”。

[0003] 现有的主流的 URL 过滤技术,主要技术分为实时内容过滤以及 URL 地址过滤,这两种技术前一种非常难满足网络延时需求,后一种同样也有类似的问题,可行方法一般选择后一种方式;

[0004] 现有 URL 地址过滤方法主要为建立 URL 库,把所有网络上 HTTP 流量的 URL 地址与该库进行比对,该方法技术上存以几个问题,一是 URL 库的建立是一个导常烦琐并且也很难定义其 URL 的应属于可访问或是不可访问的属性;二是性能问题,该种匹配方法存在网络延时问题对硬件系统性能要求过高,特别是在比较大的网络中该问题尤为突出;三是 URL 库中用户真正关心的 URL 还是相对有限的;

[0005] 基于以上问题该发明解决了以上三个问题即以用户自定义域(DOMAIN),通用资源标志符(Uniform Resource Identifier,简称“URI”),扩展名为基础,对用户关心的 URL 信息进行检测,控制。并且解决了性能上的问题,通过系统 DFA 方法以达到匹配规则,时间复杂度:O(1)。

### 发明内容

[0006] 本发明的目的在于解决上述的技术问题,提供一种 URL 过滤系统的应用方法。

[0007] 本发明的目的通过以下技术方案来实现:

[0008] 一种 URL 过滤系统的应用方法,该 URL 过滤系统以用户自定义 URL 匹配规则为基础,应用该 URL 过滤系统时,包括如下步骤,

[0009] 第一步、分配用来存储用户自定义 URL 匹配规则的内存;

[0010] 第二步、分配用来存放 DFA 图的内存;

[0011] 第三步、将用户自定义 URL 规则生成 DFA 图;

[0012] 第四步、将网内 HTTP 请求中的 DOMAIN,URI 以及扩展名到生成的 DFA 图中匹配;

[0013] 第五步,将第四步得到的结果填入对应 HTTP,记录相应的节点;

[0014] 第六步、根据用户设定的策略匹配,并做相应的动作。

[0015] 进一步地,所述的一种 URL 过滤系统的应用方法,其中所述第四步中匹配的时间

复杂度： $O(1)$ 。

[0016] 进一步地，所述的一种 URL 过滤系统的应用方法，其中所述第一步中用户自定义 URL 匹配规则是指 URL 过滤的流程，HTTP 包文件中的 URL 分成 DOMAIN, URI, HTTP 方法和扩展名，该具体流程为：

[0017] 第一步，将 DOMAIN, URI, HTTP 方法和扩展名去用户自定义规则的 DFA 图中查找相应的 ID 号；

[0018] 第二步，根据用户设定的策略对比以上的 ID 号，符合条件的按要求设定的作行为，所述行为为放行或丢弃，默认的行为为放行。

[0019] 进一步地，所述的一种 URL 过滤系统的应用方法，其中所述第四步中匹配的具体步骤为：

[0020] 第一步，将 DOMAIN 放入 URL DFA 匹配；

[0021] 第二步，根据 DOMAIN 匹配到的 ID，将 URI 放入 URL DFA 中匹配并将对应的 ID 保存在该 URL 节点上；

[0022] 第三步，将扩展名放入扩展名的 DFA 图中匹配并将其 ID 保存在 URL 节点上；

[0023] 第四步，将 HTTP 方法转换成对应的 ID 保存入 URL 节点。

[0024] 进一步地，所述的一种 URL 过滤系统的应用方法，其中所述第六步中，相应的动作指与策略相匹配的进行放行，反之则过滤。

[0025] 本发明的有益效果主要体现在，以用户自定义域 (DOMAIN)，通用资源标志符 (URI)，扩展名为基础，对用户关心的 URL 信息进行检测，控制。并且解决了性能上的问题，通过系统 DFA 方法以达到匹配规则，时间复杂度为  $O(1)$ 。

#### 附图说明

[0026] 下面结合附图对本发明技术方案作进一步说明：

[0027] 图 1：本发明用户自定义规则生成 DFA 图并且对应规则的策略。

[0028] 图 2：本发明 URL 过滤的主要流程。

[0029] 图 3：本发明 DOMAIN, URI, 扩展名, HTTP 方法匹配过程，即规则的匹配过程。

#### 具体实施方式

[0030] 本发明揭示了一种 URL 过滤系统的应用方法，如图 1、图 2、图 3 所示，该 URL 过滤系统以用户自定义 URL 匹配规则为基础，以 DFA 快速定位 URL 属于那条规则为核心，以策略为手段实现 URL 过滤系统，包括以下步骤：

[0031] 第一步、分配用来存储用户自定义 URL 匹配规则的内存；

[0032] 第二步、分配用来存放 DFA 图的内存；

[0033] 第三步，将用户自定义 URL 规则生成 DFA 图；

[0034] 第四步，将网内 HTTP 请求中的 DOMAIN, URI 以及扩展名到生成的 DFA 图中匹配，其时间复杂度： $O(1)$ ；

[0035] 第五步，将第四步得到的结果填入对应 http 记录相应的结点；

[0036] 第六步、根据用户设定的策略匹配，并做相应的动作（过滤 / 放行）；

[0037] 本发明用户自定义规则以对象为基准，后根据对象生成 DFA 图，其中规则包括 URL

规则和扩展名规则；URL 分成两个部分 DOMAIN 和 URI；先匹配 DOMAIN 再根据 URI，这样会增加匹配的效率；与普通正则表达式匹配相比较使用 DFA 更有效率；

[0039] 本发明为每一个 HTTP 会话保留相关 URL，扩展名，以及 HTTP 方法保存其相应的 ID；之后根据相应的 ID 在策略中进行匹配；并将符合策略条件的 HTTP 流量作相应的动作（通过 / 阻止）；

[0039] 本发明尚有多种具体的实施方式，凡采用等同替换或者等效变换而形成的所有技术方案，均落在本发明要求保护的范围之内。

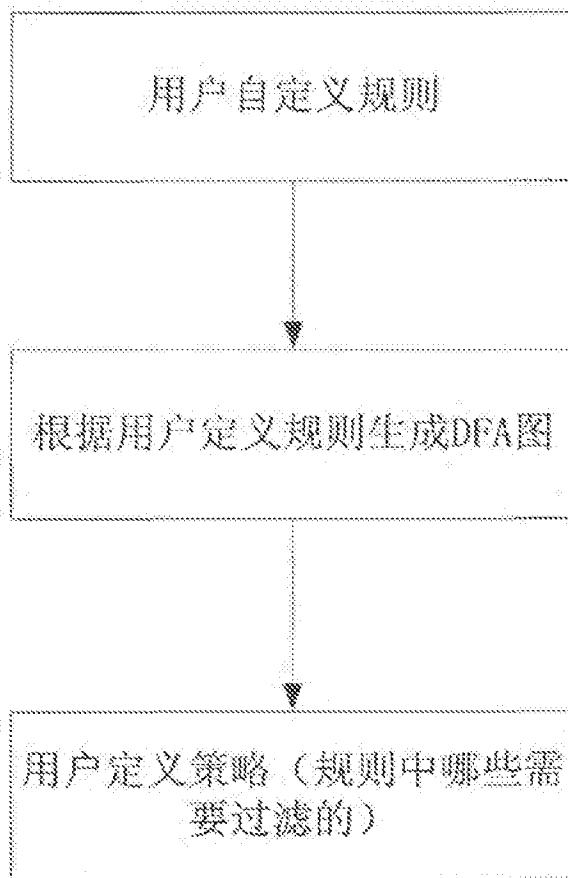


图 1

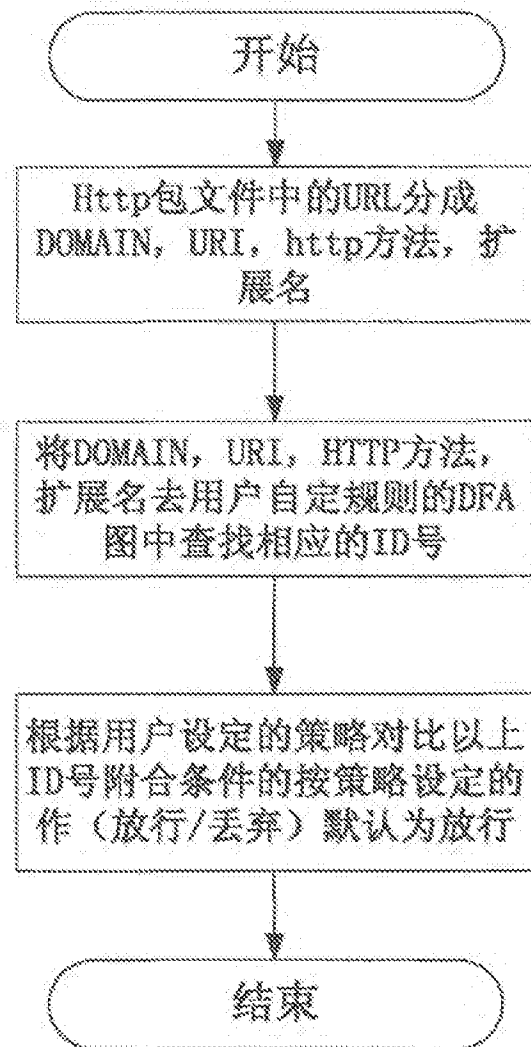


图 2

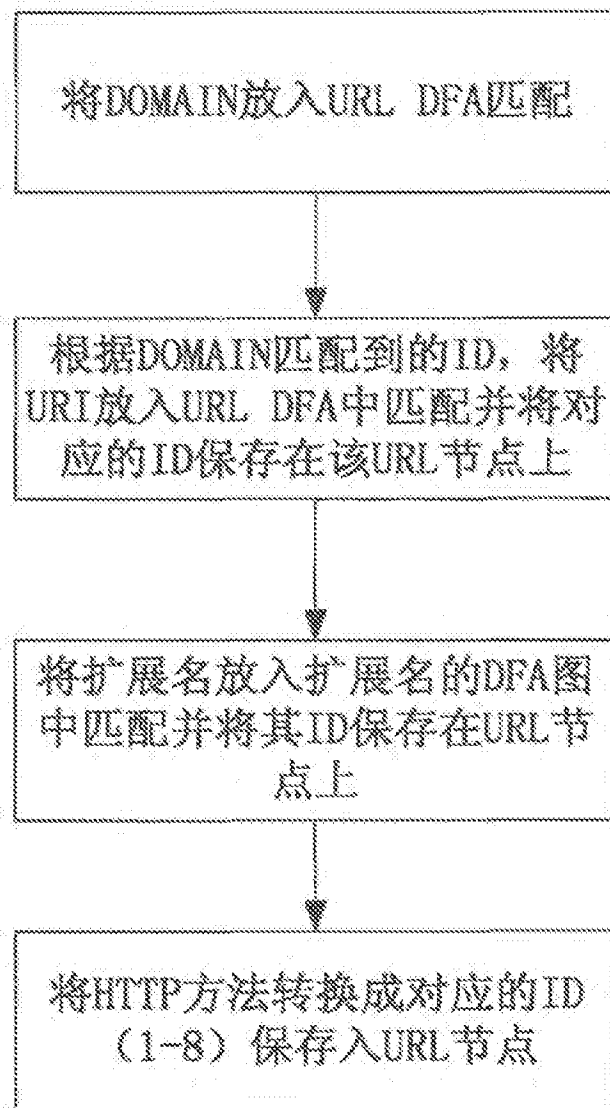


图3

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	22309818
<b>Application Number:</b>	14572514
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	2255
<b>Title of Invention:</b>	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM
<b>First Named Inventor/Applicant Name:</b>	Jiancheng GUO
<b>Customer Number:</b>	77399
<b>Filer:</b>	John B. Conklin/Brad Bares
<b>Filer Authorized By:</b>	John B. Conklin
<b>Attorney Docket Number:</b>	HW719388
<b>Receipt Date:</b>	11-MAY-2015
<b>Filing Date:</b>	18-DEC-2014
<b>Time Stamp:</b>	16:01:32
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / .zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB05)	1449Form_1.pdf	93154 <small>004020396948210080493951215500007 of 22652</small>	no	1

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

2	Transmittal Letter	IDS_1.pdf	157434	no	4
			USPTO Case File Number: 157434-001		

Warnings:

Information:

3	Foreign Reference	CN101068253A.pdf	7038258	no	40
			USPTO Case File Number: 7038258-001		

Warnings:

Information:

4	Foreign Reference	CN101141396A.pdf	13533417	no	15
			USPTO Case File Number: 13533417-001		

Warnings:

Information:

5	Foreign Reference	CN101945053A.pdf	21460312	no	24
			USPTO Case File Number: 21460312-001		

Warnings:

Information:

6	Foreign Reference	CN102004789A.pdf	5831157	no	10
			USPTO Case File Number: 5831157-001		

Warnings:

Information:

Total Files Size (in bytes):			48113762		
------------------------------	--	--	----------	--	--

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

#### New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

#### National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

#### New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.





# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address CORRESPONDENCE FOR PATENTS  
P.O. Box 1480  
Alexandria, Virginia 22313-1480  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/572,514	12/16/2014	Jiancheng GUO	HW719388

CONFIRMATION NO. 2255

77399

Leydig, Voit & Mayer, Ltd  
(for Huawei Technologies Co., Ltd)  
Two Prudential Plaza Suite 4900  
180 North Stetson Avenue  
Chicago, IL 60601

## PUBLICATION NOTICE



0000000074643369

**Title:** PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM

**Publication No.** US-2015-0103688-A1

**Publication Date:** 04/16/2015

## NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at [www.uspto.gov](http://www.uspto.gov). The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at [www.uspto.gov](http://www.uspto.gov) using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application No. 14/572,514

Confirmation No. 2255

Applicant: Huawei Technologies Co., Ltd.

Filed: December 16, 2014

TC/AU: TBA

Examiner: TBA

Docket No. HW719388 (Client Reference No. 83465722US05 )

Customer No. 77399

**PRELIMINARY AMENDMENT**

Prior to the examination of the above-identified patent application, please enter the following amendments and consider the following remarks.

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 6 of this paper.

*AMENDMENTS TO THE CLAIMS*

This listing of claims replaces all prior versions, and listings, of claims in the application.

1. (Currently Amended) A packet receiving method, comprising:
  - receiving a service request packet sent by a terminal device, wherein the service request packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request packet sent by the terminal device;
  - resolving the received server domain name to obtain a service server Internet protocol (IP) address; and
  - discarding the service request packet if the resolved service server IP address does not belong to a preset service server IP address corresponding to the received terminal domain name in a preset list.
2. (Currently Amended) The method according to claim 1, wherein, before the discarding the service request packet if the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list, the method further-comprising comprises:
  - receiving a domain name system (DNS) packet sent by the terminal device, wherein the DNS packet carries the terminal domain name and a true domain name of at least one accessible service server corresponding to the terminal domain name;
  - resolving the received true domain name to obtain at least one accessible service server IP address; and
  - taking the resolved at least one accessible service server IP address as the preset service server IP address, and setting[[,]] a corresponding relation between the terminal domain name and the preset service server IP address in the preset list.
3. (Currently Amended) The method according to claim 2, wherein, before the receiving the domain name system (DNS) packet sent by the terminal device, the method further-comprising comprises:
  - sending a DNS query request to the terminal device, ~~so that to enable~~ the terminal device to send ~~the~~ DNS packet.

4. (Currently Amended) The method according to claim 1, wherein, after the resolving the received server domain name to obtain the service server Internet protocol (IP) address, the method further comprising comprises:

if the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in the ~~the~~ [[a]] preset list, establishing a connection between the terminal device and the service server corresponding to the service server IP address, ~~so that to enable~~ the service server to provide ~~provides~~ a service corresponding to the service request of the terminal device to the terminal device.

5. (Currently Amended) The method according to claim 1, wherein, after the resolving the received server domain name to obtain the service server Internet protocol (IP) address, the method further comprising comprises:

if the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in the ~~the~~ [[a]] preset list, determining a service type of the service request according to the terminal domain name of the terminal device.

6. (Currently Amended) A deep packet inspection (DPI) device, comprising:

a receiving unit, configured to receive a service request packet sent by a terminal device, wherein the service request packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request packet sent by the terminal device;

a resolving unit, configured to resolve the server domain name received by the receiving unit to obtain a service server Internet protocol (IP) address; and

a processing unit, configured to discard the packet if the service server IP address resolved by the resolving unit does not belong to a preset service server IP address corresponding to the received terminal domain name in a preset list.

7. (Currently Amended) The DPI device according to claim 6, wherein,

the receiving unit is further configured to receive a domain name system (DNS) packet sent by the terminal device, wherein the DNS packet carries the terminal domain name and a true domain name of at least one accessible service server corresponding to the terminal domain name;

the resolving unit is further configured to resolve the true domain name received by the receiving unit to obtain at least one accessible service server IP address; and

the processing unit is further configured to take the at least one accessible service server IP address resolved by the resolving unit as the preset service server IP address, and set[[.]]a corresponding relation between the terminal domain name and the preset service server IP address in the preset list.

8. (Currently Amended) The DPI device according to claim 7, further comprising:  
a sending unit, configured to send a DNS query request to the terminal device, ~~so that~~  
to enable the terminal device to send the DNS packet.

9. (Currently Amended) The DPI device according to claim 6, wherein,  
the processing unit is further configured to: if the service server IP address resolved by the resolving unit belongs to the preset service server IP address corresponding to the received terminal domain name in the [[a]] preset list which is received by the receiving unit, establish a connection between the terminal device and the service server corresponding to the service server IP address, ~~so that to enable the service server to provide~~ provides a service corresponding to the service request of the terminal device to the terminal device.

10. (Currently Amended) The DPI device according to claim 6, wherein,  
the processing unit is further configured to: if the service server IP address resolved by the resolving unit belongs to the preset service server IP address corresponding to the received terminal domain name in the [[a]] preset list which is received by the receiving unit, determine a service type of the service request according to the terminal domain name of the terminal device.

11. (Currently Amended) A system, comprising:  
a deep packet inspection (DPI) ~~DPI device according to claim 6;~~ and  
a terminal device, configured to send a service request packet to the DPI device,  
wherein the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device;

the DPI device having;

a receiving unit, configured to receive the service request packet sent by the terminal device;

a resolving unit, configured to resolve the server domain name received by the receiving unit to obtain a service server Internet protocol (IP) address; and

a processing unit, configured to discard the packet if the service server IP address resolved by the resolving unit does not belong to a preset service server IP address corresponding to the received terminal domain name in a preset list.

*REMARKS/ARGUMENTS*

Claims 1-11 were pending. Claims 1-11 are amended herein. The foregoing amendments are made to clarify the claim language. No new matter is added hereby.

Applicants respectfully request entry of the amendments prior to examination of the above-identified patent application.

If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



/Gerald T. Gray/

Gerald T. Gray, Reg. No. 41,797

Telephone: 925-482-0100

Facsimile: 312-616-5700

Date: January 29, 2015

## Electronic Acknowledgement Receipt

EFS ID:	21350044
Application Number:	14572514
International Application Number:	
Confirmation Number:	2255
Title of Invention:	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Jiancheng GUO
Customer Number:	77399
Filer:	Gerald Todd Gray./Emily Mann
Filer Authorized By:	Gerald Todd Gray.
Attorney Docket Number:	HW719388
Receipt Date:	29-JAN-2015
Filing Date:	18-DEC-2014
Time Stamp:	18:17:28
Application Type:	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	PreliminaryAmendment_Transmittal.pdf	70376 <a href="http://www.uspto.gov/patents/publications/efs/efs.html">http://www.uspto.gov/patents/publications/efs/efs.html</a>	no	1

Warnings:

Information:



2	Preliminary Amendment	Amendment_Preliminary_719388.pdf	115847	no	6
Warnings:					
Information:					
Total Files Size (in bytes):				186223	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u>          If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u>          If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u>          If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

In re Application of: Huawei Technologies Co., Ltd.  
 Application No. 14/572,514  
 Confirmation No. 2255  
 Filing or 371(c) Date: December 16, 2014

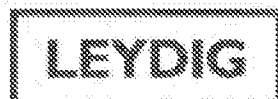
Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, VA 22313-1450

Transmitted herewith is a **Preliminary Amendment** in the subject application.

- ☐ Small entity status is claimed for this application under 37 CFR 1.27.
- ☒ Petition for an extension of time for the period noted below, as well as for any additional period necessary to render the present submission timely. Please charge Deposit Account No. 12-1216 for the appropriate petition fee.
- ☐ Other:
- ☒ Please charge Deposit Account No. 12-1216 in the total amount indicated below.

					SMALL ENTITY		OTHER THAN A SMALL ENTITY		
TIME EXTENSION PETITION FEE			none		\$ 0.00		\$ 0.00		
subtract time extension fee previously paid			none		(\$ 0.00)		(\$ 0.00)		
CLAIM FEE		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	EXTRA CLAIMS PRESENT	RATE	ADD'L CLAIM FEE	RATE	ADD'L CLAIM FEE
TOTAL		11	MINUS	11	= 0	x 40 =	\$	x 80 =	\$0.00
INDEPENDENT		2	MINUS	2	= 0	x 210 =	\$	x 420 =	\$0.00
<input type="checkbox"/>	FIRST PRESENTATION OF MULTIPLE CLAIM					+ 390 =	\$	+ 780 =	\$0.00
OTHER FEES AS DESCRIBED:					\$		\$0.00		
TOTAL AMOUNT TO BE CHARGED TO DEPOSIT ACCOUNT					TOTAL	\$	TOTAL	\$0.00	

- ☒ The Commissioner is hereby authorized to charge any deficiencies in the following fees associated with this communication or credit any overpayment to Deposit Account No. 12-1216.
- ☒ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.
- ☒ Any patent application processing fees under 37 CFR 1.17.



/Gerald T. Gray/  
 Gerald T. Gray, Reg. No. 41,797  
 Telephone: 925-482-0100  
 Facsimile: 312-616-5700

Date: January 29, 2015

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875				Application or Docket Number <b>14/572,514</b>	Filing Date <b>12/16/2014</b>	<input type="checkbox"/> To be Mailed
ENTITY: <input checked="" type="checkbox"/> LARGE <input type="checkbox"/> SMALL <input type="checkbox"/> MICRO						
<b>APPLICATION AS FILED – PART I</b>						
(Column 1)		(Column 2)				
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)	
<input type="checkbox"/> BASIC FEE (37 CFR 1.18(a), (b), or (c))	N/A	N/A	N/A			
<input type="checkbox"/> SEARCH FEE (37 CFR 1.18(a), (b), or (c))	N/A	N/A	N/A			
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.18(a), (b), or (c))	N/A	N/A	N/A			
TOTAL CLAIMS (37 CFR 1.18(b))	minus 20 =	*	X \$		=	
INDEPENDENT CLAIMS (37 CFR 1.18(b))	minus 3 =	*	X \$		=	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.18(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.18(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.18(g))						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			
<b>APPLICATION AS AMENDED – PART II</b>						
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT	<b>01/29/2015</b>	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.18(b))	- 11	Minus	- 20	= 0	
	Independent (37 CFR 1.18(b))	- 3	Minus	- 3	= 0	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.18(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.18(g))					
TOTAL ADD'L FEE					0	
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.18(b))	-	Minus	-	=	
	Independent (37 CFR 1.18(b))	-	Minus	-	=	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.18(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.18(g))					
TOTAL ADD'L FEE						
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.						

 LIE  
 /JULIET MCMILLAN/

This collection of information is required by 37 CFR 1.18. The information is required to obtain or retain a benefit by the public which is to be filed (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1080  
Alexandria, Virginia 22315-1080  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/572,514	12/16/2014	Jiancheng GUO	HW719388

CONFIRMATION NO. 2255

POA ACCEPTANCE LETTER



0000000072990668

77399

Leydig, Voit & Mayer, Ltd  
(for Huawei Technologies Co., Ltd)  
Two Prudential Plaza Suite 4900  
180 North Stetson Avenue  
Chicago, IL 60601

Date Mailed: 01/26/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/15/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/s/stephanos/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

**POWER OF ATTORNEY BY APPLICANT**

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

- ☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

77399

OR

- ☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

- ☒ The address associated with the above-mentioned Customer Number.

OR

- ☐ The address associated with Customer Number:

77399

OR

☐ Firm or Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the Applicant:

- ☐ Inventor or Joint Inventor
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature

Date

Nov 24, 2014

Name

Telephone

Title and Company President of Huswel Technologies Co., Ltd.

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below.

- ☒ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE  
REGISTERED PRACTITIONERS****NOTE:** This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	14/572,514
Filing Date	December 16, 2014
First Named Inventor	GUO, Jiancheng
Title	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM
Art Unit	2464
Examiner Name	NGO, Ricky Quoc
Attorney Docket Number	HW719388

**SIGNATURE of Applicant or Patent Practitioner**

Signature	/John B. Conklin/	Date	January 15, 2015
Name	John B. Conklin	Telephone	(312)616-5600
Registration Number	30,369		

**NOTE:** This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications.
☐ \*Total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Electronic Acknowledgement Receipt

EFS ID:	21217342
Application Number:	14572514
International Application Number:	
Confirmation Number:	2255
Title of Invention:	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Jiancheng GUO
Customer Number:	77399
Filer:	John B. Conklin/Brad Bares
Filer Authorized By:	John B. Conklin
Attorney Docket Number:	HW719388
Receipt Date:	15-JAN-2015
Filing Date:	18-DEC-2014
Time Stamp:	12:42:46
Application Type:	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / .zip	Pages (if appl.)
1	Power of Attorney	General-POA_Technologies.pdf	1649527 4212d992b1c9925943161e64317148c304 /000	no	1

Warnings:

Information:

2	Power of Attorney	POA_Transmittal.pdf	128829	no	1
<small>US-688756829-20811617-PoA-121621085-5/1/21</small>					
Warnings:					
Information:					
Total Files Size (in bytes):				1759456	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u>          If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u>          If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u>          If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					





## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address CORRESPONDENCE FOR PATENTS  
P.O. Box 1480  
Alexandria, Virginia 22315-1480  
www.uspto.gov

APPLICATION NUMBER	FILING or 371(a) DATE	OR PARY ENT	PELSEE REC'D	ATTY.DOCSET NO	TOT CLAIMS	IND CLAIMS
14/572,514	12/16/2014	2414	1600	HW719388	11	2

CONFIRMATION NO. 2255

77399

Leydig, Voit & Mayer, Ltd  
(for Huawei Technologies Co., Ltd)  
Two Prudential Plaza Suite 4900  
180 North Stetson Avenue  
Chicago, IL 60601

## FILING RECEIPT



\*0000000072627402\*

Date Mailed: 01/05/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

## Inventor(s)

Jiancheng GUO, Shenzhen, CHINA;  
Zhenggang YOU, Shenzhen, CHINA;

## Applicant(s)

Huawei Technologies Co., Ltd., Shenzhen, CHINA

Power of Attorney: None

## Domestic Priority data as claimed by applicant

This application is a CON of PCT/CN2012/077994 06/30/2012

**Foreign Applications** for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

*Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.*

If Required, Foreign Filing License Granted: 12/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/572,514**

Projected Publication Date: 04/16/2015

Non-Publication Request: No

Early Publication Request: No

Title

PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM

Preliminary Class

370

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

## **LICENSE FOR FOREIGN FILING UNDER**

**Title 35, United States Code, Section 184**

**Title 37, Code of Federal Regulations, 5.11 & 5.15**

### **GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

### **NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

## **SelectUSA**

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875						Application or Docket Number 14/572,514			
<b>APPLICATION AS FILED - PART I</b>									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE <small>(37 CFR 1.18(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	380		
SEARCH FEE <small>(37 CFR 1.18(b), (c), or (d))</small>	N/A	N/A	N/A			N/A	600		
EXAMINATION FEE <small>(37 CFR 1.15(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	720		
TOTAL CLAIMS <small>(37 CFR 1.18(i))</small>	11	minus 20**			OR	x 80**	0.00		
INDEPENDENT CLAIMS <small>(37 CFR 1.18(i))</small>	2	minus 5***				x 420**	0.00		
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.15(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.15(j))</small>							0.00		
			TOTAL			TOTAL	1600		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
<b>APPLICATION AS AMENDED - PART II</b>									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.18(i))</small>	N/A**	**	x	**	OR	x	**	
	Independent <small>(37 CFR 1.18(i))</small>	N/A***	***	x	**	OR	x	**	
	Application Size Fee <small>(37 CFR 1.16(s))</small>					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.15(j))</small>					OR			
			TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total <small>(37 CFR 1.18(i))</small>	N/A**	**	x	**	OR	x	**	
	Independent <small>(37 CFR 1.18(i))</small>	N/A***	***	x	**	OR	x	**	
	Application Size Fee <small>(37 CFR 1.16(s))</small>					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.15(j))</small>					OR			
			TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 5, enter "5". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. HW719388

Client Reference No. 83465722US02

First Inventor Jiancheng GUO

Title PACKET RECEIVING METHOD, DEEP PACKET  
INSPECTION DEVICE AND SYSTEM

ADDRESS Commissioner for Patents  
TO: P.O. Box 1450  
Alexandria, VA 22313-1450

## APPLICATION ELEMENTS

1. ☒ Utility Patent Application Transmittal Form
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification (including claims and abstract)  
[Total Pages 21]
4. ☒ Drawings [Total Sheets 3]
5. ☒ Inventor Declaration [Total Pages 2]
  - a. ☒ Newly executed
  - b. ☐ Copy from prior application  
[Note Box 6 below]
    - i. ☐ ~~Deletion of Inventor(s)~~ Signed statement attached deleting inventor(s) named in the prior application.
6. ☐ Incorporation by Reference: The entire disclosure of the prior application, from which a declaration is supplied under Box 5b is considered as part of the disclosure of the accompanying application and is hereby incorporated by reference.
7. ☒ Application Data Sheet. See 37 CFR 1.76
8. ☐ Large Table or Computer Program (Appendix) in Computer Readable Form (CRF), or on CD-ROM or CD-R in duplicate.
9. Nucleotide and/or Amino Acid Sequence Submission
  - a. ☐ Computer Readable Form (CRF)
  - b. Specification Sequence Listing on:
    - i. ☐ CD-ROM or CD-R (2 copies); or
    - ii. ☐ Paper Copy
  - c. ☐ Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

10. ☐ Applicant requests early publication (include publication fee under 37 CFR 1.18(d))
11. ☐ Assignment Papers (cover sheet and document(s))
12. ☐ 37 CFR 3.73(b) Statement (when there is an Assignee)
13. ☐ Power of Attorney
14. ☐ English Translation Document (if applicable)
15. ☐ Information Disclosure Statement (IDS)
  - ☐ Form PTO-1449
  - ☐ Copies of References (except for U.S. patents and applications)
16. ☐ Preliminary Amendment
17. ☐ Return Receipt Postcard (Should be specifically itemized)
18. ☐ Claim of Priority & Certified Copy of Priority Document(s)
19. ☐ Request & Certification Under 35 USC 122(b)(2)(B)(i) (Form PTO/SB/35 or its equivalent must be submitted with this application to prevent publication at 18 months)
20. ☐

21. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below:

☐ Continuation ☐ Divisional ☐ Continuation-in-part of prior application no.

Prior application information: Examiner ; Group Art Unit:

## APPLICATION FEES

				SMALL ENTITY		OTHER THAN A SMALL ENTITY	
FILING FEE				\$70 (EFS)		\$280	
SEARCH FEE				\$300		\$600	
EXAM FEE				\$360		\$720	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	ADD'L CLAIM FEE	RATE	ADD'L CLAIM FEE	
Total Claims	11	- 20 =	0	x 40 =	x 80 =		
Independent Claims	3	- 3 =	0	x 210 =	x 420 =		
<input type="checkbox"/> First Presentation of Multiple Dependent Claim				+ 390 =	+ 780 =		
<input type="checkbox"/> Application Size Fee - If the specification, claims, abstract, drawings, and preliminary amendment exceed 100 sheets of paper, enter number of sheets here: - If application is filed in paper form, enter this number in Total Sheets, below. - If application is filed via EFS-Web, multiply this number by 0.75 and enter result in Total Sheets, below.							
Total Sheets =	- 100 =	- 50 =	(round up to a whole number)	x 200 =	x 400 =		
<input type="checkbox"/> Assignment Fee				+ 40 =	+ 40 =		
<input type="checkbox"/> Early Publication Fee				+ 300 =	+ 300 =		
<b>TOTAL AMOUNT TO BE CHARGED</b>				<b>TOTAL</b>	<b>TOTAL</b>	<b>\$1600</b>	

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b>		Attorney Docket No. HW719388	
		Client Reference No. 83465722US05	
22. <input checked="" type="checkbox"/> Please charge Deposit Account No. 12-1216 in the amount of \$1600.			
23. The Commissioner is hereby authorized to credit overpayments or charge any additional fees of the following types to Deposit Account No. 12-1216:			
a. <input checked="" type="checkbox"/> Fees required under 37 CFR 1.16.			
b. <input checked="" type="checkbox"/> Fees required under 37 CFR 1.17.			
24. <input checked="" type="checkbox"/> The Commissioner is hereby generally authorized under 37 CFR 1.136(a)(3) to treat any future reply in this or any related application filed pursuant to 37 CFR 1.53 requiring an extension of time as incorporating a request therefor, and the Commissioner is hereby specifically authorized to charge Deposit Account No. 12-1216 for any fee that may be due in connection with such a request for an extension of time.			
25. CORRESPONDENCE ADDRESS			
<input checked="" type="checkbox"/> Customer No. 77399			
Name	Gerald T. Gray, Reg. No. 41,797		
Signature	/Gerald T. Gray/		
Contact Information	 Telephone: 925-482-0100 Facsimile: 312-616-6700		
Date	December 16, 2014		

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. HW719388

Client Reference No. 83465722US02

First Inventor Jiancheng GUO

Title PACKET RECEIVING METHOD, DEEP PACKET  
INSPECTION DEVICE AND SYSTEM

ADDRESS Commissioner for Patents  
TO: P.O. Box 1450  
Alexandria, VA 22313-1450

## APPLICATION ELEMENTS

1. ☒ Utility Patent Application Transmittal Form
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification (including claims and abstract)  
[Total Pages 21]
4. ☒ Drawings [Total Sheets 3]
5. ☒ Inventor Declaration [Total Pages 2]
  - a. ☒ Newly executed
  - b. ☐ Copy from prior application  
[Note Box 6 below]
    - i. ☐ Deletion of Inventor(s) Signed statement attached deleting inventor(s) named in the prior application.
6. ☐ Incorporation by Reference: The entire disclosure of the prior application, from which a declaration is supplied under Box 5b is considered as part of the disclosure of the accompanying application and is hereby incorporated by reference.
7. ☒ Application Data Sheet. See 37 CFR 1.76
8. ☐ Large Table or Computer Program (Appendix) in Computer Readable Form (CRF), or on CD-ROM or CD-R in duplicate.
9. Nucleotide and/or Amino Acid Sequence Submission
  - a. ☐ Computer Readable Form (CRF)
  - b. Specification Sequence Listing on:
    - i. ☐ CD-ROM or CD-R (2 copies); or
    - ii. ☐ Paper Copy
  - c. ☐ Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

10. ☐ Applicant requests early publication (include publication fee under 37 CFR 1.18(d))
11. ☐ Assignment Papers (cover sheet and document(s))
12. ☐ 37 CFR 3.73(b) Statement (when there is an Assignee)
13. ☐ Power of Attorney
14. ☐ English Translation Document (if applicable)
15. ☐ Information Disclosure Statement (IDS)
  - ☐ Form PTO-1449
  - ☐ Copies of References (except for U.S. patents and applications)
16. ☐ Preliminary Amendment
17. ☐ Return Receipt Postcard (Should be specifically itemized)
18. ☐ Claim of Priority & Certified Copy of Priority Document(s)
19. ☐ Request & Certification Under 35 USC 122(b)(2)(B)(i) (Form PTO/SB/35 or its equivalent must be submitted with this application to prevent publication at 18 months)
20. ☐

21. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below:

☐ Continuation ☐ Divisional ☐ Continuation-in-part of prior application no.

Prior application information: Examiner ; Group Art Unit:

## APPLICATION FEES

				SMALL ENTITY		OTHER THAN A SMALL ENTITY	
FILING FEE				\$70 (EFS)		\$280	
SEARCH FEE				\$300		\$600	
EXAM FEE				\$360		\$720	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	ADD'L CLAIM FEE	RATE	ADD'L CLAIM FEE	
Total Claims	11	- 20 =	0	x 40 =	x 80 =		
Independent Claims	3	- 3 =	0	x 210 =	x 420 =		
<input type="checkbox"/> First Presentation of Multiple Dependent Claim				+ 390 =	+ 780 =		
<input type="checkbox"/> Application Size Fee - If the specification, claims, abstract, drawings, and preliminary amendment exceed 100 sheets of paper, enter number of sheets here: - If application is filed in paper form, enter this number in Total Sheets, below. - If application is filed via EFS-Web, multiply this number by 0.75 and enter result in Total Sheets, below.							
Total Sheets =	- 100 =	- 50 =	(round up to a whole number)	x 200 =	x 400 =		
<input type="checkbox"/> Assignment Fee				+ 40 =	+ 40 =		
<input type="checkbox"/> Early Publication Fee				+ 300 =	+ 300 =		
TOTAL AMOUNT TO BE CHARGED				TOTAL	TOTAL	\$1500	

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b>		Attorney Docket No. HW719388	
		Client Reference No. 83465722US05	
22. <input checked="" type="checkbox"/> Please charge Deposit Account No. 12-1216 in the amount of \$1600.			
23. The Commissioner is hereby authorized to credit overpayments or charge any additional fees of the following types to Deposit Account No. 12-1216:			
a. <input checked="" type="checkbox"/> Fees required under 37 CFR 1.16.			
b. <input checked="" type="checkbox"/> Fees required under 37 CFR 1.17.			
24. <input checked="" type="checkbox"/> The Commissioner is hereby generally authorized under 37 CFR 1.136(a)(3) to treat any future reply in this or any related application filed pursuant to 37 CFR 1.53 requiring an extension of time as incorporating a request therefor, and the Commissioner is hereby specifically authorized to charge Deposit Account No. 12-1216 for any fee that may be due in connection with such a request for an extension of time.			
25. CORRESPONDENCE ADDRESS			
<input checked="" type="checkbox"/> Customer No. 77399			
Name	Gerald T. Gray, Reg. No. 41,797		
Signature	/Gerald T. Gray/		
Contact Information	<div style="display: flex; align-items: center;"> <div style="border: 2px solid black; padding: 5px; margin-right: 10px;"> <b>LEYDIG</b> </div> <div> Telephone: 925-482-0100  Facsimile: 312-616-6700 </div> </div>		
Date	December 16, 2014		



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388
		Application Number	
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

## Secrecy Order 37 CFR 5.2

<input type="checkbox"/>	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

## Inventor Information:

Inventor 1					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Jiancheng		GUO			
Residence Information (Select One) <input type="radio"/> US Residency <input checked="" type="radio"/> Non US Residency <input type="radio"/> Active US Military Service						
City	Shenzhen		Country of Residence <sup>i</sup>	CN		
Mailing Address of Inventor:						
Address 1		Huawei Administration Building				
Address 2		Bantian, Longgang District				
City	Shenzhen, Guangdong		State/Province			
Postal Code	518129		Country <sup>i</sup>	CN		
Inventor 2					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Zhenggang		YOU			
Residence Information (Select One) <input type="radio"/> US Residency <input checked="" type="radio"/> Non US Residency <input type="radio"/> Active US Military Service						
City	Shenzhen		Country of Residence <sup>i</sup>	CN		
Mailing Address of Inventor:						
Address 1		Huawei Administration Building				
Address 2		Bantian, Longgang District				
City	Shenzhen, Guangdong		State/Province			
Postal Code	518129		Country <sup>i</sup>	CN		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
						Add

## Correspondence Information:

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388	
		Application Number		
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM			
Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).				
<input type="checkbox"/> An Address is being provided for the correspondence information of this application.				
Customer Number	77399			
Email Address	chgpatent@leydig.com		<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

**Application Information:**

Title of the Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM			
Attorney Docket Number	HW719388	Small Entity Status Claimed		<input type="checkbox"/>
Application Type	Nonprovisional			
Subject Matter	Utility			
Total Number of Drawing Sheets (if any)	3	Suggested Figure for Publication (if any)	1	

**Filing By Reference :**

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

**Publication Information:**

<input type="checkbox"/> Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/> <b>Request Not to Publish.</b> I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application <b>has not and will not</b> be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

**Representative Information:**

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	77399		

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388
		Application Number	
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM		

### Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status	Pending	<a href="#">Remove</a>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	PCTCN2012077994	2012-06-30
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the <b>Add</b> button.			<a href="#">Add</a>

### Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

<a href="#">Remove</a>			
Application Number	Country <sup>i</sup>	Filing Date (YYYY-MM-DD)	Access Code (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the <b>Add</b> button.			<a href="#">Add</a>

### Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

<p>This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.</p> <p><input type="checkbox"/> NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.</p>
--

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388
		Application Number	
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM		

## Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

## Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

**Applicant 1**

[Remove](#)

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

[Clear](#)

☒ Assignee      ☐ Legal Representative under 35 U.S.C. 117      ☐ Joint Inventor

☐ Person to whom the inventor is obligated to assign.      ☐ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name

Huawei Technologies Co., Ltd.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388
		Application Number	
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM		

<b>Mailing Address Information For Applicant:</b>			
Address 1	Huawei Administration Building		
Address 2	Bantian, Longgang District, Guangdong		
City	Shenzhen	State/Province	
Country i	CN	Postal Code	518129
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. <span>Add</span>			

## Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

<b>Assignee 1</b>				
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
				<span>Remove</span>
If the Assignee or Non-Applicant Assignee is an Organization check here.				<input type="checkbox"/>
Prefix	Given Name	Middle Name	Family Name	Suffix
<b>Mailing Address Information For Assignee including Non-Applicant Assignee:</b>				
Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. <span>Add</span>				

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	HW719388
		Application Number	
Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM		

**Signature:**[Remove](#)

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

<b>Signature</b>	/Gerald T. Gray/		<b>Date (YYYY-MM-DD)</b>	2014-12-16	
<b>First Name</b>	Gerald T.	<b>Last Name</b>	Gray	<b>Registration Number</b>	41797

Additional Signature may be generated within this form by selecting the Add button.

[Add](#)

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

# DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of  
Invention

PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM

As the below named inventor, I hereby declare that:

This declaration  
is directed to:



The attached application, or



United States application or PCT international application number \_\_\_\_\_

filed on \_\_\_\_\_

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

## WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

## LEGAL NAME OF INVENTOR

Inventor: Jiancheng GUO

Date (Optional): \_\_\_\_\_

Signature: *Jiancheng Guo*

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1460, Alexandria, VA 22313-1460. DO NOT SEND PSES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

(If you need assistance in completing the form, call 1-800-PTO-0198 and select option 2.)



# DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM
--------------------	---

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number \_\_\_\_\_ filed on \_\_\_\_\_

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

**WARNING:**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR
Inventor: Zhenggang YOU Date (Optional): _____
Signature: <u>Zhenggang YOU</u>

Note: An application data sheet (PTO/SD/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO in process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1480, Alexandria, VA 22313-1480. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1480, Alexandria, VA 22313-1480.

If you need assistance in completing the form, call 1-800-PTO-0199 and select option 2.

# **PACKET RECEIVING METHOD, DEEP PACKET INSPECTION DEVICE AND SYSTEM**

## **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application is a continuation of International Patent Application No. PCT/CN2012/077994, filed June 30, 2012, which is hereby incorporated by reference in its entirety.

## **TECHNICAL FIELD**

[0002] The present invention relates to the field of communications and, more particularly, to a packet receiving method, a deep packet inspection device and system.

## **BACKGROUND**

[0003] Nowadays, Internet services become increasingly sophisticated, and types of the services are gradually increasing, a user terminal is able to access websites such as video websites and game websites, and such websites are either free or charged on operator's demands, and the user terminal can select to access on his own demands.

[0004] Generally, a service server used by a user to access a website corresponds to an IP (Internet Protocol, Internet protocol) address, the user can send a packet carrying a domain name and relevant information of the visiting website, generally, when a DPI (Deep Packet Inspection, deep packet inspection) device strategically matches the packet information, a full URL (Uniform Resource Location, uniform resource locator) information containing a host field needs to be used, which is different from the packet processing principle of the existing service server, thus bugs may occur in the DPI device detection, for example, the service server merely inspects path information in the URL of the packet, and does not inspect the host field, such that the service server can return access results according to the path

information without determining whether the path information is consistent with the path provided by the host field, that is, without determining whether the user has altered the host field without authorization. As a result, the user can successfully access the charged service through altering the packet without authorization, but the DPI device fails to identify whether the user terminal has altered the host field in the packet to achieve a purpose of fraudulent accessing a charged website for free.

### SUMMARY

[0005] Embodiments of the present invention provide a packet receiving method, a deep packet inspection device and system, which can improve the capability for identifying the packet of the deep packet inspection device, and prevent occurrence of bugs caused by insufficient identification.

[0006] To achieve the above object, embodiments of the present invention provide technical solutions as follows:

[0007] One aspect of the invention provides a packet receiving method, including:

[0008] receiving a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device;

[0009] resolving the received server domain name to obtain a service server Internet protocol (IP) address; and

[0010] discarding the packet if the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list.

[0011] Another aspect of the invention provides a deep packet inspection (DPI) device, including:

[0012] a receiving unit, configured to receive a service request packet sent by a terminal

device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device;

[0013] a resolving unit, configured to resolve the server domain name received by the receiving unit to obtain a service server Internet protocol (IP) address; and

[0014] a processing unit, configured to discard the packet if the service server IP address resolved by the resolving unit does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list.

[0015] Still another aspect of the invention provides a system, including:

[0016] a DPI device as described above; and

[0017] a terminal device, configured to send a service request packet to the DPI device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device.

[0018] According to the packet receiving method, the DPI device and the system provided by embodiments of the present invention, the DPI device receives a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request, resolves the received server domain name to obtain a service server Internet protocol (IP) address, and discards the packet if the service server IP address does not belong to the preset service server IP address corresponding to the terminal domain name in a preset list. In this way, the DPI device can determine whether the packet is normal or abnormal by comparing the service server IP address of the packet with the preset service server IP address corresponding to the terminal domain name of the terminal device in a preset list to determine whether the service server IP address of the packet is consistent with the preset service server IP address, and discard the abnormal packet, thereby improving the capability

for identifying the packet of the DPI device, and preventing the bugs from occurring when the DPI device normally processes the abnormal packet due to insufficient identification.

### **BRIEF DESCRIPTION OF DRAWINGS**

[0019] To illustrate the technical solution according to embodiments of the present invention or the prior art more clearly, the following briefly describes the accompanying drawings used in description of embodiments of the present invention or the prior art. Apparently, the accompanying drawings below are merely for illustrating some embodiments of the present invention, and other drawings can be obtained by persons skilled in the art based on these drawings without creative efforts.

[0020] FIG. 1 is a schematic flow chart of a packet receiving method according to an embodiment of the present invention;

[0021] FIG. 2 is a comparison diagram between a true packet and a packet which has been altered without authorization according to an embodiment of the present invention;

[0022] FIG. 3 is a schematic flow chart of a packet receiving method according to another embodiment of the present invention;

[0023] FIG. 4 is a schematic structural diagram of a DPI device according to an embodiment of the present invention;

[0024] FIG. 5 is a schematic structural diagram of a DPI device according to another embodiment of the present invention; and

[0025] FIG. 6 is a schematic structural diagram of a system according to an embodiment of the present invention.

### **DESCRIPTION OF EMBODIMENTS**

[0026] The technical solutions of the embodiments of the present invention are hereinafter described clearly and completely with reference to the accompanying drawings in

embodiments of the present invention. Obviously, the embodiments described here are only a part of embodiments of the present invention, rather than all embodiments of the present invention. All other embodiments obtained by persons skilled in the art based on embodiments of the present invention without any creative efforts shall fall within the protection scope of the present invention.

[0027] Embodiments of the present invention provide a packet receiving method, as shown in FIG. 1, the method includes:

[0028] S101, a DPI device receives a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device.

[0029] It should be noted that, a suitable network in this embodiment may perform communication and connection on the basis of the TCP/IP (Transmission Control Protocol/Internet Protocol, transmission control protocol/Internet protocol), in such a network, each of terminal devices and service servers connected to the network has a unique identifier, so as to distinguish tens of thousands of terminal devices and service servers in the network. Generally, such a unique identifier may be a character address, namely a domain name. Since each terminal device and each service server have a unique domain name of its own, the terminal device only needs to notify the DPI device of its own domain name as the terminal domain name when the terminal device requests services to the DPI device, the DPI device can find the terminal device by the terminal domain name, and forward or provide services required by the terminal device to the terminal device. Furthermore, the terminal device can implement the access to the service server required by the service request by writing the domain name of the service server, as the server domain name, into the packet.

[0030] Illustratively, the terminal device needs to access available resources on the network, such as a hypertext markup language document, an image, a video segment, and a program.

Service servers supporting different websites can be identified by the server domain name which is taken as the unique identification ID. When the terminal device needs to access a website, the terminal device sends a URL packet, into which packet a server domain name of a service server corresponding to the website has been written. The server domain name is a character address of the service server corresponding to the website needs to be accessed by the terminal device. For example, when a user needs to access a website of A company by using the terminal device, the URL can be written as www.A.com or the like.

[0031] S102, the DPI device resolves the received server domain name to obtain a service server IP address.

[0032] Further, the DPI device performs a DNS (Domain Name Server, domain name service) resolution to the server domain name, such as resolving in a manner of local query, cache query and iterative query, so that the domain name which is readily memorized by a user, such as www.baidu.com and www.google.com, can be converted to a machine recognizable IP address such as 1.1.1.10 and 2.2.2.2, and the machine recognizable IP address is taken as the service server IP address. Thereby the DPI device can help the terminal device access the service server by using the service server IP address, and then the service server can provide services for the terminal device.

[0033] S103, if the service server IP address resolved by the DPI device does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list, the DPI device discards the packet.

[0034] It should be noted that, a preset list is preset in the DPI device in advance, as shown in Table 1, in the preset list the terminal domain name of each terminal device is correspondingly provided with accessible service server IP addresses under an access authority of the terminal device. The accessible service server IP addresses are taken as the preset service server IP addresses. One terminal device can correspond to a plurality of preset service server IP addresses.

Terminal domain name	Preset service server IP address
	1.1.1.1
www.huawei.com	2.2.2.20
www.google.com	2.2.2.2

Table 1

[0035] Illustratively, as shown in Table 1, the terminal domain name of a terminal device A is www.huawei.com, and the terminal device A can only access two preset service servers of 1.1.1.1 and 2.2.2.20, provided that neither of the two preset service servers is charged; the terminal domain name of a terminal device B is www.google.com, the terminal device B can access to 2.2.2.2, and the preset service server corresponding to this IP address is charged. As shown in FIG. 2, provided that the IP address corresponding to www.huawei.com is 1.1.1.1 while the IP address corresponding to www.google.com is 2.2.2.2, that is, the terminal device A can only access the preset service server of www.huawei.com for free, but cannot access the preset service server of www.google.com. In the prior art, however, during processing of URL in the packet, the service server only focuses on a path after a GET request without inspecting a host field, and returns the access results according to the path after the GET request without judging whether the path information is consistent with the path provided by the host field; the service server only reads addresses after the host and then accesses without checking whether the fields after the host are the correct fields for a free accessible website. As a result, if the terminal device A changes the domain name after the host from www.google.com to www.huawei.com, then the terminal device A can access www.google.com for free, and the access result can be returned to the terminal device A by the www.huawei.com after the GET. In this way, the user can successfully access the charged



service through altering the packet, but the DPI device fails to identify whether the user terminal has altered the host field in the packet to achieve a purpose of fraudulent accessing a charged website for free.

[0036] According to embodiments of the present invention, the DPI device sets the terminal domain name `www.huawei.com` of the terminal device A and the accessible service server thereof, which is taken as the preset service server, in a preset list; if the service server IP address corresponding to the server domain name obtained by resolving for the terminal device A does not belong to the preset service server IP address in Table 1 corresponding to the terminal domain name `www.huawei.com`, that is, corresponding to the terminal device A, for example, if the IP address obtained by resolving the server domain name is `2.2.2.2`, neither `1.1.1.1` nor `2.2.2.20`, then the packet is considered to be abnormal, and the abnormal packet is discarded so as to prevent the terminal device A from successfully accessing the charged service through altering the packet without authorization; if the IP address obtained by resolving the server domain name is `2.2.2.20`, which is one of `1.1.1.1` and `2.2.2.20`, then the packet is considered to be normal, and a connection between the terminal device A and the service server of which the IP address is `2.2.2.20` according to the service request requested by the packet, such that the service server provides the service corresponding to the service request to the terminal device A.

[0037] In the packet receiving method according to embodiments of the present invention, the DPI device receives a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request, resolves the received server domain name to obtain a service server Internet protocol (IP) address, and discards the packet if the service server IP address does not belong to the preset service server IP address corresponding to the terminal domain name in a preset list. In this way, the DPI device can determine whether the packet is normal or abnormal by comparing the service server IP

address of the packet with the preset service server IP address corresponding to the terminal domain name of the terminal device in a preset list to determine whether the service server IP address of the packet is consistent with the preset service server IP address, and discard the abnormal packet, thereby improving the capability for identifying the packet of the DPI device, and preventing the bugs from occurring when the DPI device normally processes the abnormal packet due to insufficient identification.

[0038] A packet receiving method according to another embodiment of the present invention is described by taking a gateway device having a DNS resolution function as an example, while other devices having the DNS resolution function shall also fall within the protection scope of the present invention. As shown in FIG. 3, the method may include:

[0039] S201, a gateway device receives a DNS packet sent by a terminal device, where the DNS packet carries a terminal domain name indicating a terminal device and a true domain name of at least one accessible service server corresponding to the terminal domain name.

[0040] It should be pointed out that, the gateway device may send a DNS query request to a terminal device during an idle time, so that each terminal device sends a DNS packet to the gateway device; Or when receiving a DNS packet of the terminal device without sending the query request, the gateway device may also obtain the terminal domain name indicating the terminal device and the true domain name of at least one accessible service server corresponding to the terminal domain name, which are carried in the DNS packet.

[0041] S202, the gateway device resolves the received true domain name to obtain at least one accessible service server IP address.

[0042] It should be noted that, the gateway device resolves the true domain name to obtain a server IP address which the terminal device is authorized to access, such as an IP address which can be accessed for free.

[0043] S203, the gateway device takes the resolved at least one accessible service server IP address as a preset service server IP address, and sets, corresponding relation between the

terminal domain name and the preset service server IP address in a preset list.

[0044] Illustratively, the gateway device sets, corresponding relation between the terminal domain name HTTP/1.1\r\n, and the resolved accessible service server IP address of the terminal device A such as 2.2.2.20 and 1.1.1.1 in the preset list, where the accessible service server IP address is referred to as the preset service server IP address, and sets, corresponding relation between the terminal domain name HTTP/1.2\r\n, and the resolved accessible service server IP address of the terminal device B such as 2.2.2.2 in the preset list, where the accessible service server IP address is referred to as the preset service server IP address, and so on. Thus, the preset list is established, so that the gateway device can judge whether the service server, which is requested by the terminal device A or terminal device B corresponding to the subsequently received terminal domain name, is within the accessible range, according to the preset service server IP address corresponding to the terminal domain name in the list.

[0045] It should be noted that, there is no sequence relationship among S201, S202, S203, S204 and S205, as long as S201, S202 and S203 are performed before S206, S207 or S208.

[0046] S204, the gateway device receives a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device.

[0047] S205, the gateway device resolves the received server domain name to obtain a service server Internet protocol (IP) address.

[0048] It should be noted that, after S205, if the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list, then perform step S206; if the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list, then perform step S207 or S208 according to requirement of the

gateway device.

[0049] S206, the gateway device discards the packet.

[0050] Because the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list, the gateway device can determine the packet is a malicious and fraudulent packet or an abnormal packet, and discard the packet, where the specific method has been disclosed in the above embodiments, and will not be repeated here.

[0051] S207, the gateway device establishes a connection between the terminal device and a service server corresponding to the service server IP address, so that the service server provides a service corresponding to the service request of the terminal device to the terminal device.

[0052] It should be noted that, because the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list, that is, the terminal device only needs to normally access the accessible service server, then the gateway device can establish a connection between the terminal device and the service server, so that the service server provides services such as video data or audio data, which is requested by the terminal device, to the terminal device.

[0053] S208, the gateway device determines a service type of the service request according to the terminal domain name of the terminal device.

[0054] Illustratively, if the gateway device needs to identify the encrypted service type sent by the terminal device or identify the service type of terminal devices having constantly changing IP addresses, the service type may be obtained by comparing the terminal domain name and the preset service server IP address in the preset list. That is, if the service request of the terminal device is encrypted, for example, a certain download tool or a certain mail tool is encrypted, then the gateway device fails to obtain the specific service application type by resolving features such as URL of these encrypted applications. However, the gateway

needs to limit all the download tools. At this time, after determining the preset service server IP address in the preset list and the service server IP address of the terminal device are the same, the gateway device automatically match the service type according to terminal domain name of the terminal device in the preset list; if the service type of the terminal device A is an encrypted download tool, and the service type of the terminal device B is an encrypted mail tool, then the gateway device can identify and limit the downloading of the terminal device A. In this way, the case can be avoided that during the resolution, since an anti-recognition software is encountered, the service type cannot be obtained and the encrypted service type cannot be operated.

[0055] Furthermore, if the service type of the terminal device B is mail download encrypted, and the service type has no significant feature and specific IP address, that is, the IP address is in dynamic state, then, after determining the preset service server IP address in the preset list and the service server IP address of the terminal device are the same based on the preset list, the gateway device obtains the terminal device B according to the terminal domain name of terminal device B in the preset list and, thus, identifies the specific service type. If the corresponding relation between the domain name and the service type is configured in the gateway device, for example, the service type corresponding to the domain name "www.gmail.com" is configured as email, the gateway device can determine that the service type of the terminal device B is a mail according to the terminal domain name www.gmail.com.

[0056] It should be noted that, either step S207 or step S208 may be selected to be performed according to different processing manners required by the gateway device. Specifically, if the gateway device needs to determine that the packet is normal and to establish a connection between the terminal device and the service server, the gateway device performs S207; if the gateway device needs to know the service type, the gateway device performs S208.

[0057] In the packet receiving method according to embodiments of the present invention, the gateway device receives a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request, resolves the received server domain name to obtain a service server Internet protocol (IP) address, and discards the packet if the service server IP address does not belong to the preset service server IP address in a preset list corresponding to the terminal domain name. In this way, the gateway device can determine whether the packet is normal or abnormal by comparing the service server IP address of the packet with the preset service server IP address in a preset list corresponding to the terminal domain name of the terminal device to determine whether the service server IP address of the packet is consistent with the preset service server IP address, and discard the abnormal packet, thereby improving the capability for identifying the packet of the gateway device, and preventing the bugs from occurring when the gateway device normally processes the abnormal packet due to insufficient identification.

[0058] Embodiments of the present invention provide a DPI device 30, as shown in FIG. 4, including:

[0059] a receiving unit 301, configured to receive a service request packet sent by a terminal device 40, where the packet carries a terminal domain name indicating the terminal device 40 and a server domain name indicating a service server required by the service request sent by the terminal device 40.

[0060] It should be noted that, the DPI device 30 can establish a connection between the terminal device 40 and the service server required by the terminal device 40 according to the terminal domain name and server domain name received by the receiving unit 301, such that the terminal device 40 can obtain the service required by the service request, which will not be described in detail here.

[0061] a resolving unit 302, configured to resolve the server domain name received by the

receiving unit 301 to obtain a service server Internet protocol (IP) address.

[0062] It should be noted that, the resolving unit 302 can achieve a mutual conversion between a domain name which is readily memorized by a user and a machine recognizable IP address.

[0063] a processing unit 303, configured to discard the packet, if the service server IP address resolved by the resolving unit 302 does not belong to the preset service server IP address in a preset list corresponding to the terminal domain name received by the receiving unit 301.

[0064] It should be noted that, if the terminal domain name received by the receiving unit 301 in the preset list is not correspond to the service server which is accessible and should be corresponded to the terminal domain name, i.e., the preset service server recorded in the preset list, it proves that the accessed packet is abnormal, such as a malicious and fraudulent packet and a packet for accessing a charged website for free, the processing unit 303 discards the packet.

[0065] the processing unit 303 is further configured to establish a connection between the terminal device 40 and the service server corresponding to the service server IP address if the service server IP address resolved by the resolving unit 302 belongs to the preset service server IP address corresponding to the terminal domain name in the preset list, which is received by the receiving unit 301, so that the service server provides the service corresponding to the service request of the terminal device 40 to the terminal device 40. Alternatively, if the service server IP address resolved by the resolving unit 302 belongs to the preset service server IP address corresponding to the terminal domain name in the preset list, which is received by the receiving unit 301, the processing unit 303 determines the service type of the service request according to the terminal domain name of the terminal device 40.

[0066] Further, the DPI device 30, as shown in FIG. 5, also includes:

[0067] a sending unit, configured to send a DNS query request to the terminal device 40, so that the terminal device 40 sends the DNS packet.

[0068] Where, the receiving unit 301 is further configured to receive the DNS packet sent by the terminal device 40, the DNS packet carries the terminal domain name and a true domain name of at least one accessible service server corresponding to the terminal domain name.

[0069] the resolving unit 302 is further configured to resolve the true domain name received by the receiving unit 301 to obtain at least one accessible service server IP address.

[0070] At this time, the processing unit 303 sets, corresponding relation between the terminal domain name received by the receiving unit 301, and the at least one accessible service server IP address resolved by the resolving unit 302 in the preset list, where the at least one accessible service server IP address is taken as the preset service server IP address, so that the subsequent receiving unit 301 performs comparing in the preset list according to the terminal domain name after receiving the service request packet, so as to avoid performing normal process to the packet when the service server IP address to be accessed by the packet does not correspond to the preset service server IP address corresponding to the terminal domain name in the preset list.

[0071] The above DPI device 30 corresponds to the above method embodiments, and the DPI device 30 can be applied in steps of the above method embodiments, where the specific application in each step may refer to the above method embodiments and will not be described in detail here.

[0072] Embodiments of the present invention provide a DPI device 30. The DPI device 30 receives a service request packet sent by a terminal device 40, where the packet carries a terminal domain name indicating the terminal device 40 and a server domain name indicating a service server required by the service request, resolves the received server domain name to obtain a service server Internet protocol (IP) address, and discards the packet if the service



server IP address does not belong to the preset service server IP address corresponding to the terminal domain name in a preset list. In this way, the DPI device 30 can determine whether the packet is normal or abnormal by comparing the service server IP address of the packet with the preset service server IP address corresponding to the terminal domain name of the terminal device 40 in a preset list to determine whether the service server IP address of the packet is consistent with the preset service server IP address, and discard the abnormal packet, thereby improving the capability for identifying the packet of the DPI device 30, and preventing the bugs from occurring when the DPI device normally processes the abnormal packet due to insufficient identification.

[0073] Embodiments of the present invention provide a system, as shown in FIG. 6, including:

[0074] a DPI device 30, configured to receive a service request packet sent by a terminal device 40, and the packet carries a terminal domain name indicating the terminal device 40 and a server domain name indicating the service request; resolve the received service server domain name to obtain a service server Internet protocol (IP) address; and discard the packet if the service server IP address does not belong to the preset service server IP address corresponding to the terminal domain name in a preset list.

[0075] a terminal device 40, configured to send the service request packet to the DPI device 30.

[0076] The above DPI device 30 and terminal device 40 correspond to the above method embodiments, and the DPI device 30 and the terminal device 40 can be applied in steps of the above method embodiment, where the specific application in each step may refer to the above method embodiment. The specific structure of the DPI device 30 and the structure of the terminal and the DPI device provided by the above embodiments are the same, which will not be described in detail here.

[0077] In the system according to embodiments of the present invention, the DPI device 30

receives a service request packet sent by a terminal device 40, where the packet carries a terminal domain name indicating the terminal device 40 and a server domain name indicating a service server required by the service request, resolves the received server domain name to obtain a service server Internet protocol (IP) address, and discards the packet if the service server IP address does not belong to the preset service server IP address corresponding to the terminal domain name in a preset list. In this way, the DPI device 30 can determine whether the packet is normal or abnormal by comparing the service server IP address of the packet with the preset service server IP address corresponding to the terminal domain name of the terminal device 40 in a preset list to determine whether the service server IP address of the packet is consistent with the preset service server IP address, and discard the abnormal packet, thereby improving the capability for identifying the packet of the DPI device 30, and preventing the bugs from occurring when the DPI device normally processes the abnormal packet due to insufficient identification.

[0078] The above description are merely some specific embodiments of the present invention, but not intended to limit the protection scope of the present invention. Any modifications, variations or replacement that can be easily derived by persons skilled in the art within the technical scope of the present invention shall fall within the protection scope of the present invention. Therefore, the protection scope of the present invention is subject to the appended claims.

## CLAIMS

What is claimed is:

1. A packet receiving method, comprising:
  - receiving a service request packet sent by a terminal device, wherein the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device;
  - resolving the received server domain name to obtain a service server Internet protocol (IP) address; and
  - discarding the packet if the resolved service server IP address does not belong to a preset service server IP address corresponding to the received terminal domain name in a preset list.
2. The method according to claim 1, wherein, before the discarding the packet if the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list, further comprising:
  - receiving a domain name system (DNS) packet sent by the terminal device, wherein the DNS packet carries the terminal domain name and a true domain name of at least one accessible service server corresponding to the terminal domain name;
  - resolving the received true domain name to obtain at least one accessible service server IP address; and
  - taking the resolved at least one accessible service server IP address as the preset service server IP address, and setting, corresponding relation between the terminal domain name and the preset service server IP address in the preset list.
3. The method according to claim 2, wherein, before the receiving the domain name system (DNS) packet sent by the terminal device, further comprising:
  - sending a DNS query request to the terminal device, so that the terminal device sends the DNS packet.
4. The method according to claim 1, wherein, after the resolving the received server

domain name to obtain the service server Internet protocol (IP) address, further comprising:

if the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list, establishing a connection between the terminal device and the service server corresponding to the service server IP address, so that the service server provides a service corresponding to the service request of the terminal device to the terminal device.

5. The method according to claim 1, wherein, after the resolving the received server domain name to obtain the service server Internet protocol (IP) address, further comprising:

if the resolved service server IP address belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list, determining a service type of the service request according to the terminal domain name of the terminal device.

6. A deep packet inspection (DPI) device, comprising:

a receiving unit, configured to receive a service request packet sent by a terminal device, wherein the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device;

a resolving unit, configured to resolve the server domain name received by the receiving unit to obtain a service server Internet protocol (IP) address; and

a processing unit, configured to discard the packet if the service server IP address resolved by the resolving unit does not belong to a preset service server IP address corresponding to the received terminal domain name in a preset list.

7. The DPI device according to claim 6, wherein,

the receiving unit is further configured to receive a domain name system (DNS) packet sent by the terminal device, wherein the DNS packet carries the terminal domain name and a true domain name of at least one accessible service server corresponding to the terminal domain name;

the resolving unit is further configured to resolve the true domain name received by the receiving unit to obtain at least one accessible service server IP address; and

the processing unit is further configured to take the at least one accessible service server IP address resolved by the resolving unit as the preset service server IP address, and set, corresponding relation between the terminal domain name and the preset service server IP address in the preset list.

8. The DPI device according to claim 7, further comprising:

a sending unit, configured to send a DNS query request to the terminal device, so that the terminal device sends the DNS packet.

9. The DPI device according to claim 6, wherein,

the processing unit is further configured to: if the service server IP address resolved by the resolving unit belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list which is received by the receiving unit, establish a connection between the terminal device and the service server corresponding to the service server IP address, so that the service server provides a service corresponding to the service request of the terminal device to the terminal device.

10. The DPI device according to claim 6, wherein,

the processing unit is further configured to: if the service server IP address resolved by the resolving unit belongs to the preset service server IP address corresponding to the received terminal domain name in a preset list which is received by the receiving unit, determine a service type of the service request according to the terminal domain name of the terminal device.

11. A system, comprising:

a DPI device according to claim 6; and

a terminal device, configured to send a service request packet to the DPI device, wherein the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request sent by the terminal device.

## **ABSTRACT**

Embodiments of the present invention provide a packet receiving method, a deep packet inspection device and system, which relates to the field of communications. The packet receiving method includes: receiving a service request packet sent by a terminal device, where the packet carries a terminal domain name indicating the terminal device and a server domain name indicating a service server required by the service request; resolving the received server domain name to obtain a service server Internet protocol (IP) address; and discarding the packet if the resolved service server IP address does not belong to the preset service server IP address corresponding to the received terminal domain name in a preset list. Embodiments of the present invention are applied to the processing of the packet.

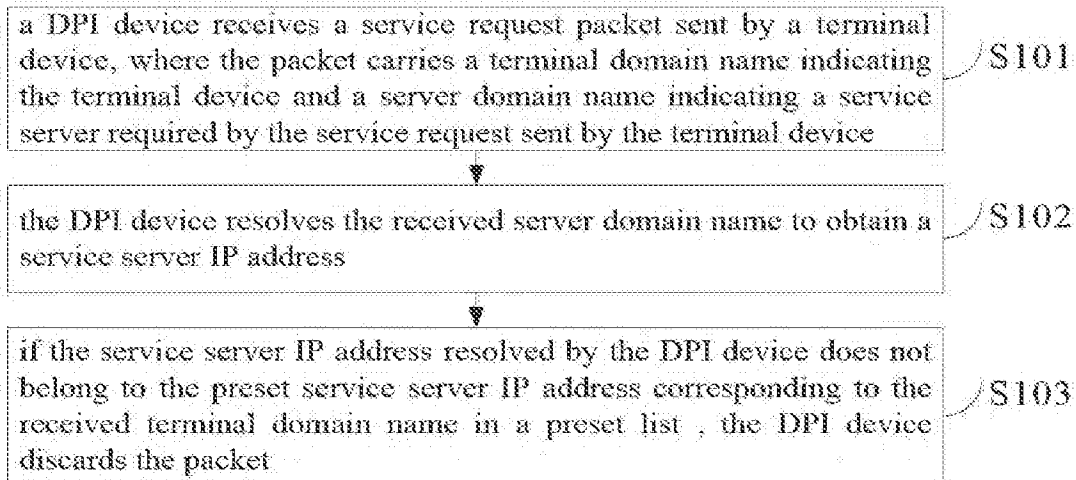


FIG. 1

A true packet

```

HTTP/1.1 200 OK
Content-Type: text/html
Accept: image/gif, image/x-bitmap, image
Accept-Language: zh-cn\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE
Host: www.google.com\r\n
Connection: keep-alive\r\n
\r\n
  
```

A packet which has been altered without authorization

```

HTTP/1.1 200 OK
Content-Type: text/html
Accept: image/gif, image/x-bitmap, image
Accept-Language: zh-cn\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE
Host: www.huawei.com\r\n
Connection: keep-alive\r\n
\r\n
  
```

FIG. 2

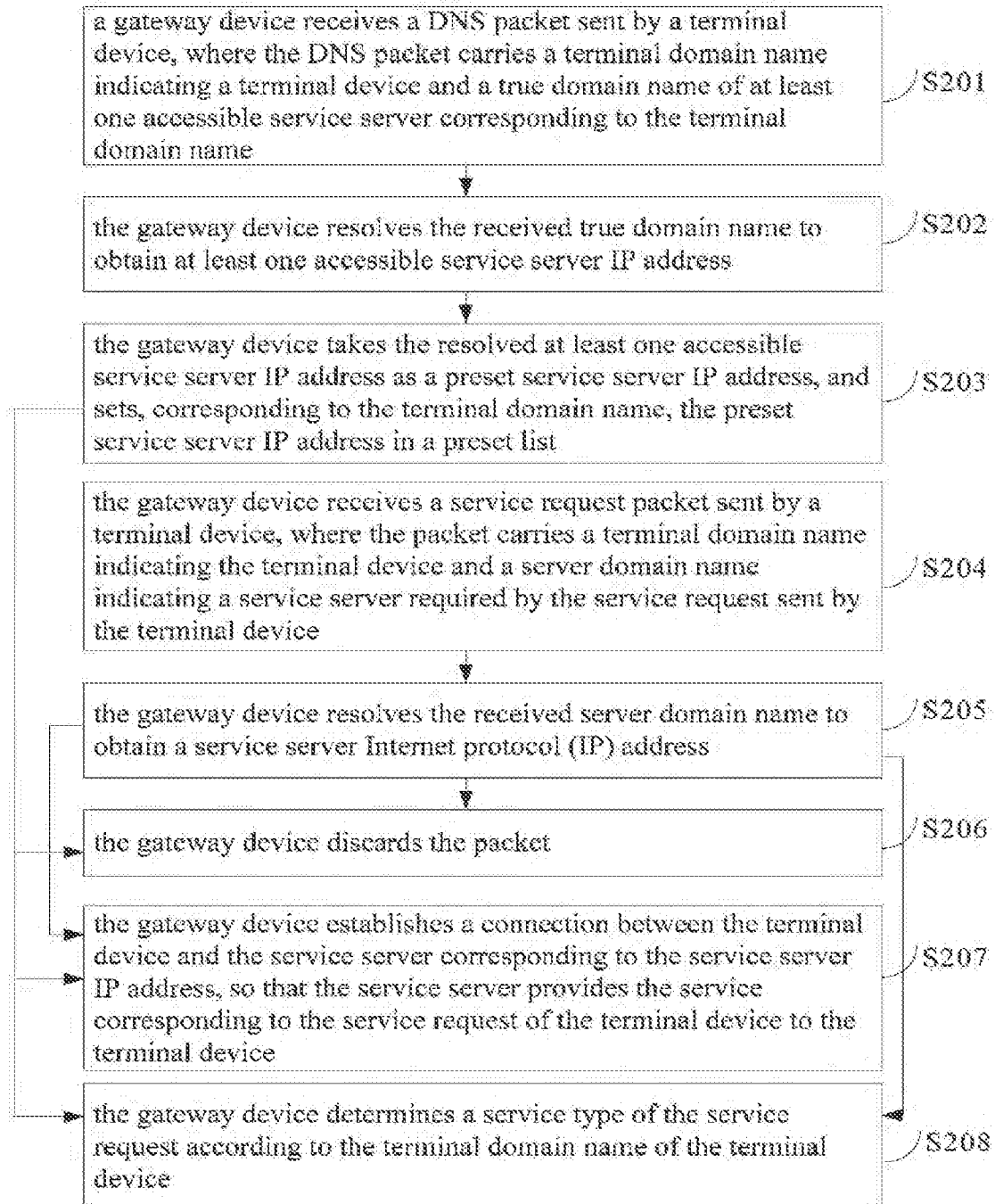


FIG. 3



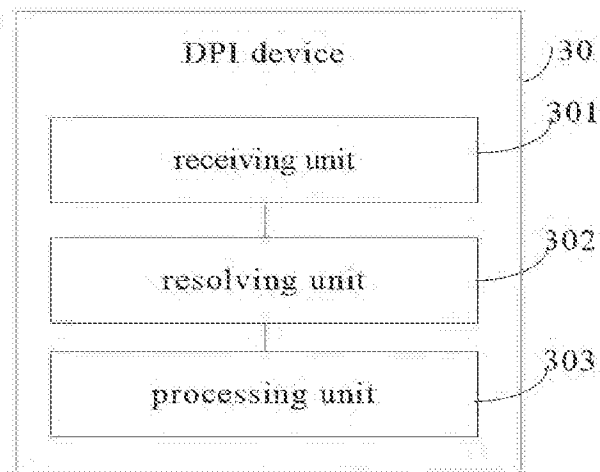


FIG. 4

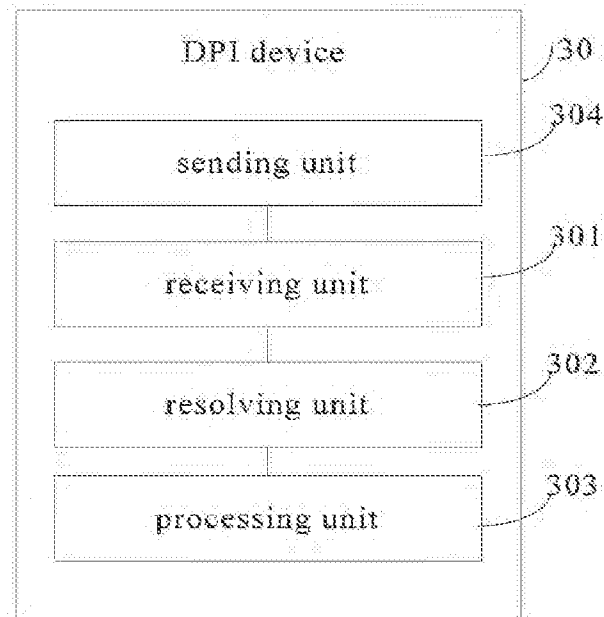


FIG. 5

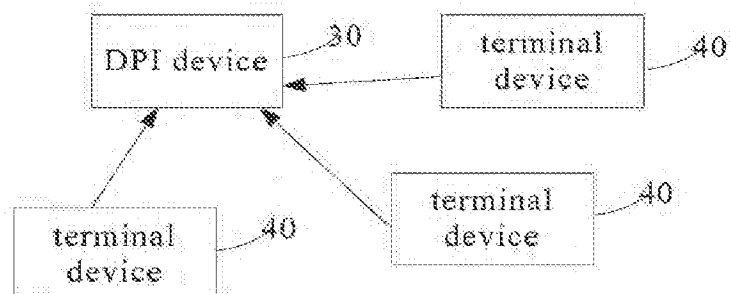


FIG. 6

## Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of invention:	PACKET RECEIVING METHOD, DEEP POCKET INSPECTION DEVICE AND SYSTEM			
First Named Inventor/Applicant Name:	Jiancheng GUO			
Filer:	Gerald Todd Gray/Leanna Bullema			
Attorney Docket Number:	HW719368			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent Appeals and Interferences:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1600

## Electronic Acknowledgement Receipt

EFS ID:	30981952
Application Number:	14572514
International Application Number:	
Confirmation Number:	3255
Title of Invention:	PACKET RECEIVING METHOD, DEEP POCKET INSPECTION DEVICE AND SYSTEM
First Named Inventor/Applicant Name:	Jiancheng GUO
Customer Number:	77399
Filer:	Gerald Todd Gray./Leanna Bultema
Filer Authorized By:	Gerald Todd Gray.
Attorney Docket Number:	HW719388
Receipt Date:	15-DEC-2014
Filing Date:	
Time Stamp:	18:24:33
Application Type:	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1600
RAM confirmation Number	5457
Deposit Account	121216
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	Application_Transmittal.pdf	100764 2024101910343118801104773731210210ad7f5804b	no	2
Warnings:					
Information:					
2	Application Data Sheet	ADS.pdf	1294824 1294101910343118801104773731210210ad7f5804b1294824	no	7
Warnings:					
Information:					
3	Oath or Declaration filed	Declaration.pdf	3006427 30064101910343118801104773731210210ad7f5804b3006427	no	2
Warnings:					
Information:					
4	Specification	Application.pdf	253817 2538101910343118801104773731210210ad7f5804b253817	no	24
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	35435 3543501910343118801104773731210210ad7f5804b35435	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			5291267		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.