(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 9 月 15 日 (15.09.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/141808 A1

(51) 国际专利分类号:
H04L 12/70 (2013.01) *H04L 29/08* (2006.01)

(21) 国际申请号: PCT/CN2016/074422

(22) 国际申请日: 2016 年 2 月 24 日 (24.02.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510099111.7 2015 年 3 月 6 日 (06.03.2015) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Cayman Islands (KY)。

(72) 发明人; 及

(71) 申请人 (仅对美国): 李立中 (LI, Lizhong) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (CN)。

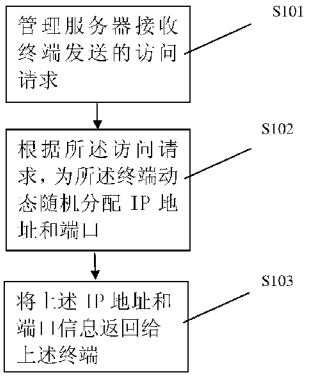
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: SECURITY MANAGEMENT METHOD AND APPARATUS FOR SERVER

(54) 发明名称 : 一种服务器的安全管理方法及装置



S101 A MANAGEMENT SERVER RECEIVES AN ACCESS REQUEST SENT BY A TERMINAL
S102 DYNAMICALLY AND RANDOMLY ALLOCATE, ACCORDING TO THE ACCESS REQUEST, AN IP ADDRESS AND A PORT FOR THE TERMINAL
S103 RETURN INFORMATION ABOUT THE IP ADDRESS AND THE PORT TO THE TERMINAL

图 2

(57) Abstract: Disclosed is a security management method for a server. The method comprises: a management server receives an access request sent by a terminal; dynamically and randomly allocate, according to the access request, an IP address and a port for the terminal; and return information about the IP address and the port to the terminal so as to allow the terminal to be connected to a server corresponding to the IP address and the port. By means of the method, an IP address and a port for a terminal to access a server are allocated randomly by a management server, thereby preventing the malicious access of the terminal, and effectively protecting the security of the server.

(57) 摘要: 本申请公开了一种服务器的安全管理方法，其中，所述方法包括：管理服务器接收终端发送的访问请求；根据所述访问请求，为所述终端动态随机分配 IP 地址和端口；将所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。通过上述方法，终端访问服务器的 IP 地址和端口，由管理服务器随机分配，从防止终端的恶意访问，有效的保护服务器的安全。

WO 2016/141808 A1

一种服务器的安全管理方法及装置

技术领域

本申请涉及计算领域的安全领域，尤其涉及一种服务器的安全管理方法及装置。

背景技术

在当今互联网时代，服务器给世界各地的用户提供各种各样的在线服务，例如预订酒店、预订机票、在线购物、提供资讯等。在服务器提供在线服务的同时，也需要对服务器进行防护，以避免黑客或入侵者对攻击服务器。

服务器因需要提供在线服务，需要接入外网或内网，现有服务器的管理端口大多都是静态开放的。故，黑客或入侵者可以利用扫描器通过服务器的网络之间互连的协议（Internet Protocol，IP）地址对服务器的端口进行暴力穷举等方式扫描服务器的端口，从而查找可以入侵或控制服务器端口，达到恶意攻击服务器的目的。

故，本发明将提供一种新服务器的安全管理方法，以克服上述问题。

发明内容

本申请实施例提供一种服务器的安全管理方法及装置，可以有效保护服务器的安全。

为解决上述问题，本申请实施例提供一种服务器的安全管理方法及装置。

一种服务器的安全管理方法，包括:

管理服务器接收终端发送的访问请求;

根据所述访问请求，为所述终端动态随机分配 IP 地址和端口;

将所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。

一种服务器的安全管理装置，包括:

接收单元，用于接收终端的访问请求;

处理单元，用于根据所述接收单元接收的所述访问请求，为所述终端动态随机分配 IP 地址和端口;

发送单元，用于将所述处理单元分配的所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。

由以上本申请实施例提供的技术方案可见，本申请实施例中，当终端发起服务的访问请求时，由管理服务器随机分配服务的IP地址和端口，使提供服务的IP和端口信息无需处于静态开放状态，以防止黑客或入侵者的恶意访问，有效的保护服务器的安全。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中:

图 1 为本申请实施例提供的集群式服务器的结构图;

图 2 为本申请一个实施例提供的服务器的安全管理方法流程图;

图 3 为本申请一个实施例提供的为终端动态随机分配 IP 地址和端口的流程图;

图 4 为本申请另一个实施例提供的服务器的安全管理方法流程图;

图 5 为本申请实施例提供的服务器的安全管理装置结构图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施

例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请一种服务器的安全管理方法应用于集群式服务器，如图 1 所示，为一种集群式服务器的一种实施例的结构示意图，其包括一个管理服务器和若干与其连接的服务器（服务器 1、服务器 2、服务器 3、……服务器 N），管理服务器与上述若干服务器连接，管理服务器可以为服务器分配浮动的 IP 地址和端口，上述管理服务器可以通过服务器的固定 IP 地址与服务器连接，并且通过上述固定 IP 地址为服务器分配浮动的 IP 地址和端口，需要访问上述服务器的终端，可以通过上述浮动的 IP 地址和端口连接到服务器。管理服务器预先定义若干浮动 IP 地址和若干端口，所述预先定义的 IP 地址和端口可以为所有的适用的 IP 地址和端口，也可以是自定义的 IP 地址和端口，根据访问终端的服务请求，管理服务器从上述若干浮动 IP 地址和若干端口中随机选取一个或多个 IP 地址以及一个或多个端口，再从上述与管理服务器连接的服务中随机选取一个或多个可以提供上述服务请求的服务的服务器，将上述随机选取的 IP 地址和端口分配给上述服务器，然后将上述随机分配的 IP 地址和端口的信息传递给终端，建立终端与上述 IP 地址和端口之间的映射关系，这样，终端可以通过上述 IP 地址和端口访问到可以提供其所请求的服务的服务器。

通过上述方式，管理服务器根据终端的服务请求为其随机分配 IP 地址和端口，终端根据上述 IP 地址和端口的信息访问到相应的服务器。另，即使提供服务的服务器被切换，例如提供在线支付服务的服务器由服务器 1 变成服务器 2，管理服务器会将相应的 IP 地址和端口分配给服务器 2，这样，终端可以继续通过上述 IP 地址和端口信息继续访问到服务器 2，并且进行相应的在线支付操作。

如图 2 所示，为本申请的一种服务器的安全管理方法的实施例，其具体工作步骤如下：

S101：管理服务器接收终端发送的访问请求。

终端向管理服务器发送访问请求，该访问请求中包含终端所请求的服务信息，具体可以携带所请求的服务的服务标识。

上述终端的访问请求可以通过访问管理服务器的形式发送，也可以通过发送短信的形式发送给管理服务器，例如，当需要发送访问请求时，先发送一条包含具体指令的短信给管理服务器，管理服务器根据上述接收到的短信确定终端的服务请求。

S102：根据所述访问请求，为所述终端动态随机分配 IP 地址和端口。

其中，所述 IP 地址为浮动 IP 地址；所述端口为随机分配的端口。

具体地，如图 3 所示，为所述终端动态随机分配 IP 地址和端口，可以包括:

S1021、管理服务器根据终端的访问请求确定所述访问请求所请求的服务。具体可以根据所请求的服务的服务标识来确定。

S1022、根据终端的访问请求的服务，查找到提供所述服务的服务器。

根据服务标识，查找到能够提供该服务的服务器，或者，查找到能够提供该服务的 IP 地址和端口。此时，可以是服务器的固定 IP 地址和端口，是存储于管理服务器上的集群中的内部信息，该固定 IP 地址和端口信息可以不公开给终端。

S1023、随机选择一个查找到的服务器，为所述服务器随机地分配动态的 IP 地址和端口。

管理服务器从预先定义的若干 IP 地址和若干端口中选取一个或 IP 地址以及一个或多个端口，为选择的服务器随机地分配动态的 IP 地址和端口。

上述预先定义的 IP 地址是由管理服务器预先定义的，以浮动 IP 地址的形式由管理服务器选取，例如管理服务器可以预先定义 IP:124.158.26.30 - IP:124.158.26.39 的 IP 地址段为预先定义的 IP 地址，则当终端访问管理服务器时，管理服务器会从上述预先定义的 IP 地址段中随机选取一个或多个 IP 地址。另，管理服务器也可以根据终端的不同的服务请求分别预先定义若干 IP 地址，

例如，管理服务器预先定义在线支付的服务请求的 IP 地址为 IP:124.158.26.30 - 124.158.26.39 的 IP 地址段；定义在线预订酒店的服务请求的 IP 地址为 IP:124.158.26.10 - 124.158.26.19 的 IP 地址段；定义在线检索的服务请求的 IP 地址为 IP:124.158.26.40 - 124.158.26.49 的 IP 地址段，这样，当终端的服务请求为在线支付时，管理服务器从 IP:124.158.26.30 - 124.158.26.39 的 IP 地址段中随机选取一个或多个 IP 地址；当终端的服务请求为在线预订酒店时，管理服务器从 IP:124.158.26.10 - 124.158.26.19 的 IP 地址段中随机选取一个或多个 IP 地址；当终端的服务请求为在线检索时，管理服务器从 IP:124.158.26.40 - 124.158.26.49 的 IP 地址段中随机选取一个或多个 IP 地址。

同理，管理服务器也可以预先定义若干端口号，例如 1-100，当终端访问管理服务器时，管理服务器会从上述预先定义的端口号中选取一个或多个。另管理服务器也可以预先定义在线支付的服务请求的端口号为：10-40；定义在线预订酒店的服务请求的端口号为：60-90；定义在线检索的服务请求的端口号为 100-130，这样，当终端的服务请求为在线支付时，管理服务器从端口号为：10-40 的端口号中随机选取一个或多个端口号；当终端的服务请求为在线预订酒店时，管理服务器从端口号为：60-90 的端口号中随机选取一个或多个端口号；当终端的服务请求为在线检索时，管理服务器从端口号为：100-130 的端口号中随机选取一个或多个端口号。

另，上述 IP 地址和端口号被管理服务器选取前，处于被关闭状态，被管理服务器选取后，被选取的 IP 地址和端口被开放。

在服务器列表中随机选择一个服务器，并且将上述IP地址和端口分配给所选择的服务器。

S1024、将所述动态的IP地址和端口分配给所述终端，形成所述终端信息与分配的所述服务器的动态的IP地址和端口信息之间的映射关系，所述终端信息包括客户端特征或终端IP地址。

管理服务器从服务器列表中选取一个可以提供上述服务的服务器，将上述

选取的IP地址和端口分配给被选取的服务器，使终端可以通过上述IP地址和端口访问相应的服务器。

上述分配的IP地址也可以先和服务器的固定IP地址建立映射关系，当终端访问服务器时，通过上述分配的IP地址与服务器的固定IP地址的映射关系，使上述终端可以访问到相应的服务器。

可选地，在为所述终端动态随机分配IP地址和端口之后，还包括：存储所述终端信息与分配的所述IP地址和端口信息之间形成的映射关系。

S103：将上述IP地址和端口信息返回给上述终端。

管理服务器将选取的IP地址和端口信息返回给终端。

管理服务器可以通过终端的访问界面返回给终端，也可以通过短信的形式返回给终端。

这样，服务器的IP地址和端口信息可以不用对外公开，由管理服务器进行统一随机动态地分配IP地址和端口，使提供服务的IP和端口信息无需处于静态开放状态，以防止黑客或入侵者的恶意访问，有效的保护服务器的安全。

可选地，将IP地址和端口信息返回给终端后，还包括：接收所述终端发送的登录请求，所述登录请求中携带有所述客户端特征或终端IP地址；利用所述映射关系，根据所述登录请求中的客户端特征或终端IP地址验证所述登录请求的合法性，若符合，则通过验证，允许所述终端连接所述IP地址和端口所对应的服务器。

管理服务器会验证终端的信息是否合法，即请求访问的终端是否为合法用户，例如可以通过账号和密码、证书、终端IP地址等方式验证所请求的终端是否为合法用户，也可以通过短信验证码的方式验证其是否为合法用户。

当上述终端的身份通过验证后，通过上述映射关系终端可以访问到相应的服务器。

上述映射关系建立之后，管理服务器储存上述映射关系，以使终端和服务器之间保持连接状态。另外，在形成所述终端信息与分配的IP地址和端口信息

之间的映射关系之后，管理服务器还可以设置所述映射关系的有效时间，以便在所述映射关系的有效时间允许所述终端连接所述IP地址和端口所对应的服务器。

可选地，所述方法还包括：接收所述终端发送的延长所述映射关系的有效时间的请求，并延长所述映射关系的有效时间。这样，可以根据终端的请求，延长终端与所述IP地址和端口所对应的服务器的连接时间。

如图4所示，在另一实施例中，本申请的一种服务器的安全管理方法，具体工作步骤如下：

S201：管理服务器接收终端发送的访问请求。

S202：根据所述访问请求，为所述终端动态随机分配IP地址和端口。

S203：将上述IP地址和端口信息返回给上述终端。

S204：在服务器列表中随机选者一个服务器，并且将上述IP地址和端口分配给所选择的服务器。

S205：建立上述IP地址和端口与终端的之间的映射关系。

上述实施例中，管理服务器会先将选取的IP地址和端口返回给终端，然后再将上述IP地址和端口分配给相应的服务器。当然，管理服务器也可以将S203和S204同时执行，即在返回给终端IP地址和终端的同时，将上述IP地址和端口分配给相应的服务器。

上述IP地址和端口的分配时间被设定成一个固定的时长，即终端与被分配的IP地址和终端之间的映射关系的有效时间为一个固定的时长，例如IP地址和端口与终端的映射关系建立后，管理服务器将对其进行计时，当建立映射的时长超过预设的时长时，上述IP地址和端口将被释放，并且被关闭，即管理服务器会中断上述IP地址和端口与相应服务器之间的映射关系。这样，终端将不能继续访问上述服务器。当终端需要延长访问服务器的时长时，即需要延长上述IP地址和端口与终端的映射关系的有效时间时，需要终端提出申请。上述延时的申请，可以通过终端的登入界面申请，也可以通过发送短信的形式申请。另，

当终端退出登入时，上述IP地址和端口会被及时释放，并且被关闭，即上述IP地址和端口与终端之间的映射关系会被立即中断。这样，上述被释放的IP地址和端口将进入空闲状态，等待管理服务器再次选取。

通过上述方式，终端每次连接到服务器需要管理服务器为其随机分配IP地址和端口，而且，在一段有效时间之后IP地址和端口可能又将进行动态变化，这样，可以有效规避通过扫描器暴力穷举找到对应的IP地址和端口，可以有效地阻止非法终端的恶意连接，从而有效地保护了服务器的安全。

如图 5 所示，以下介绍本申请的一种服务器的安全管理装置的实施例:

接收单元 301，用于接收终端的访问请求;

处理单元 302，用于根据所述接收单元接收的所述访问请求，为所述终端动态随机分配 IP 地址和端口;;

发送单元 303，用于将所述处理单元分配的所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。

上述处理单元 302 包括:

确定子单元 3021，用于确定所述访问请求所请求的服务;

查找子单元 3022，用于根据所述确定子单元确定的所述服务，查找到提供所述服务的服务器;

分配子单元 3023，用于随机选择一个查找到的服务器，为所述服务器随机地分配动态的 IP 地址和端口;

映射子单元 3024，用于将所述分配子单元分配的所述动态的 IP 地址和端口分配给所述终端，形成所述终端信息与所述服务器的动态的 IP 地址和端口信息之间的映射关系，所述终端信息包括客户端特征或终端 IP 地址;

设置子单元 3025，用于设置所述映射子单元形成的所述映射关系的有效时间，以便在所述映射关系的有效时间允许所述终端连接所述 IP 地址和端口所对应的服务器。

本申请的一种服务器的安全管理装置还包括：存储单元 304，用于存储所

述映射子单元形成的所述终端信息与分配的所述 IP 地址和端口信息之间形成的映射关系。

可选地，所述接收单元 301 还用于在将所述 IP 地址和端口信息返回给所述终端之后，接收所述终端发送的登录请求，所述登录请求中携带有所述客户端特征或终端 IP 地址；以及接受所述终端发送的延长所述有效映射关系的有效时间的请求。

所述处理单元 302 还用于利用所述映射子单元形成的所述映射关系，根据所述登录请求中的客户端特征或终端 IP 地址验证所述登录请求的合法性，若符合，则通过验证，允许所述终端连接所述 IP 地址和端口所对应的服务器。

上述各单元的功能可对应于图 2 或图 3 详细描述的上述安全管理方法的处理步骤，于此不再赘述。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个

流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种服务器的安全管理方法，其特征在于，所述方法包括:

管理服务器接收终端发送的访问请求;

根据所述访问请求，为所述终端动态随机分配 IP 地址和端口;

将所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。

2、如权利要求 1 所述的方法，其特征在于，根据所述访问请求，为所述终端动态随机分配 IP 地址和端口，具体包括:

确定所述访问请求所请求的服务;

根据上述请求的服务，查找到提供所述服务的服务器;

随机选择一个查找到的服务器，为所述服务器随机地分配动态的 IP 地址和端口;

将所述动态的 IP 地址和端口分配给所述终端，形成所述终端信息与分配的所述服务器的动态的 IP 地址和端口信息之间的映射关系，所述终端信息包括客户端特征或终端 IP 地址。

3、如权利要求 1 或 2 所述的方法，所述 IP 地址为浮动 IP 地址; 所述端口为随机分配的端口。

4、如权利要求 2 所述的方法，其特征在于，在为所述终端动态随机分配 IP 地址和端口之后，还包括:

存储所述终端信息与分配的所述IP地址和端口信息之间形成的映射关系。

5、如权利要求 2 所述的方法，其特征在于，在将所述 IP 地址和端口信息返回给所述终端之后，还包括:

接收所述终端发送的登录请求，所述登录请求中携带有所述客户端特征或终端 IP 地址;

利用所述映射关系，根据所述登录请求中的客户端特征或终端 IP 地址验证所述登录请求的合法性，若符合，则通过验证，允许所述终端连接所述 IP

地址和端口所对应的服务器。

6、如权利要求 2 所述的方法，其特征在于，在形成所述终端信息与分配的 IP 地址和端口信息之间的映射关系之后，还包括:

设置所述映射关系的有效时间，以便在所述映射关系的有效时间允许所述终端连接所述 IP 地址和端口所对应的服务器。

7、如权利要求 6 所述的方法，其特征在于，所述方法还包括:

接收所述终端发送的延长所述映射关系的有效时间的请求，并延长所述映射关系的有效时间。

8、一种服务器的安全管理装置，其特征在于，包括:

接收单元，用于接收终端的访问请求;

处理单元，用于根据所述接收单元接收的所述访问请求，为所述终端动态随机分配 IP 地址和端口;

发送单元，用于将所述处理单元分配的所述 IP 地址和端口信息返回给所述终端，以允许所述终端连接所述 IP 地址和端口所对应的服务器。

9、如权利要求 8 所述的装置，其特征在于，所述处理单元包括:

确定子单元，用于确定所述访问请求所请求的服务;

查找子单元，用于根据所述确定子单元确定的所述服务，查找到提供所述服务的服务器;

分配子单元，用于随机选择一个查找到的服务器，为所述服务器随机地分配动态的 IP 地址和端口;

映射子单元，用于将所述分配子单元分配的所述动态的 IP 地址和端口分配给所述终端，形成所述终端信息与所述服务器的动态的 IP 地址和端口信息之间的映射关系，所述终端信息包括客户端特征或终端 IP 地址。

10、如权利要求 9 所述的装置，其特征在于，所述装置还包括:

存储单元，用于存储所述映射子单元形成的所述终端信息与分配的所述 IP 地址和端口信息之间形成的映射关系。

11、如权利要求 9 所述的装置，其特征在于，所述接收单元还用于在将所述 IP 地址和端口信息返回给所述终端之后，接收所述终端发送的登录请求，所述登录请求中携带有所述客户端特征或终端 IP 地址；

所述处理单元还用于利用所述映射子单元形成的所述映射关系，根据所述登录请求中的客户端特征或终端 IP 地址验证所述登录请求的合法性，若符合，则通过验证，允许所述终端连接所述 IP 地址和端口所对应的服务器。

12、如权利要求 9 所述的装置，其特征在于，所述处理单元还包括：

设置子单元，用于设置所述映射子单元形成的所述映射关系的有效时间，以便在所述映射关系的有效时间允许所述终端连接所述 IP 地址和端口所对应的服务器。

13、如权利要求 12 所述的装置，其特征在于，所述接收单元还用于接收所述终端发送的延长所述映射关系的有效时间的请求；

所述设置子单元延长所述映射关系的有效时间。

14、如权利要求 8 所述的装置，其特征在于，所述 IP 地址为浮动 IP 地址；所述端口为随机分配的端口。

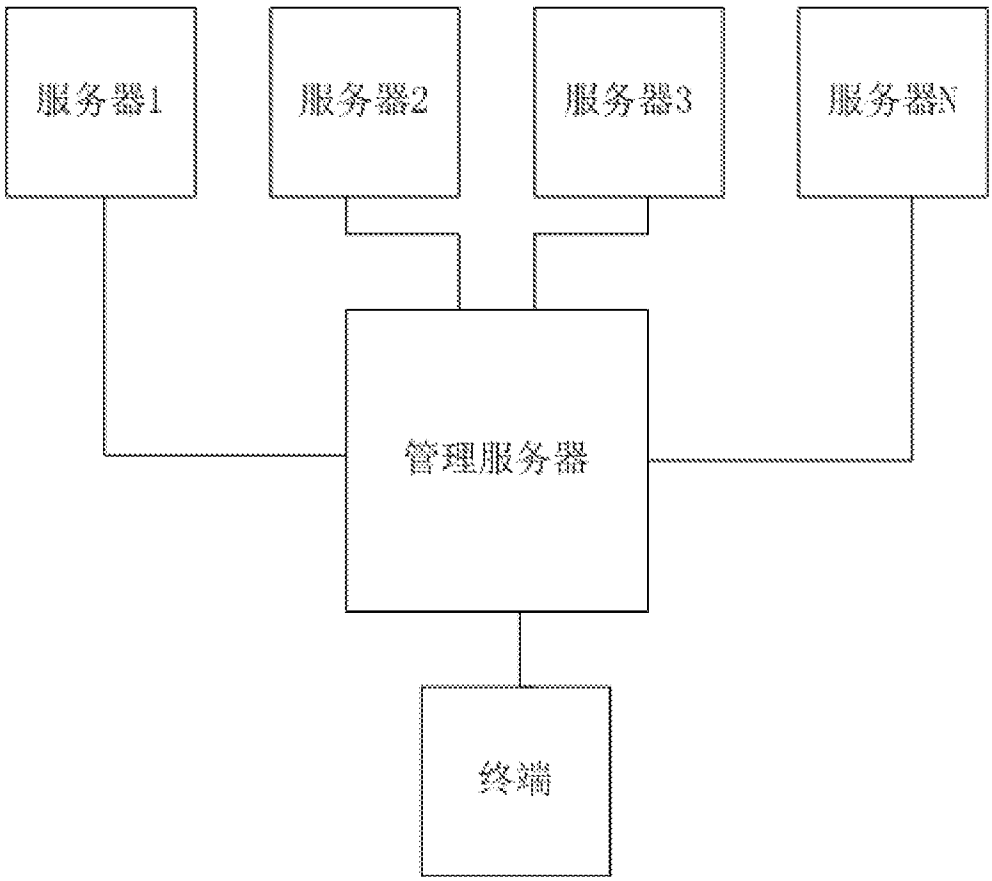


图 1

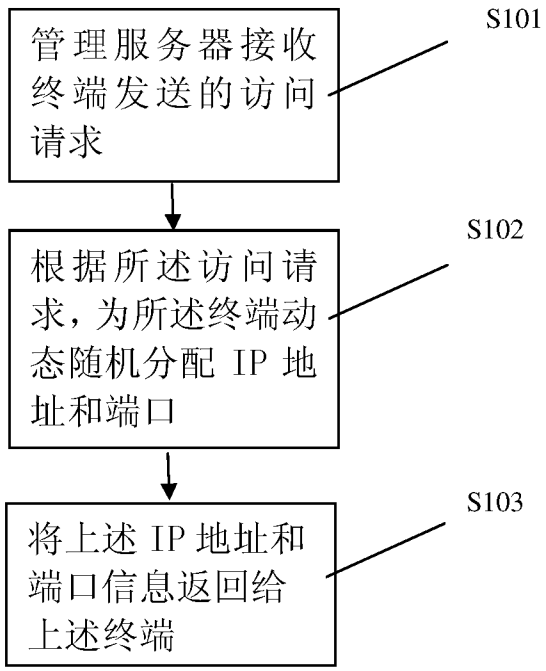

管理服务器接收终端发送的访问请求
S101
根据所述访问请求，为所述终端动态随机分配 IP 地址和端口
S102
将上述 IP 地址和端口信息返回给上述终端
S103

图 2

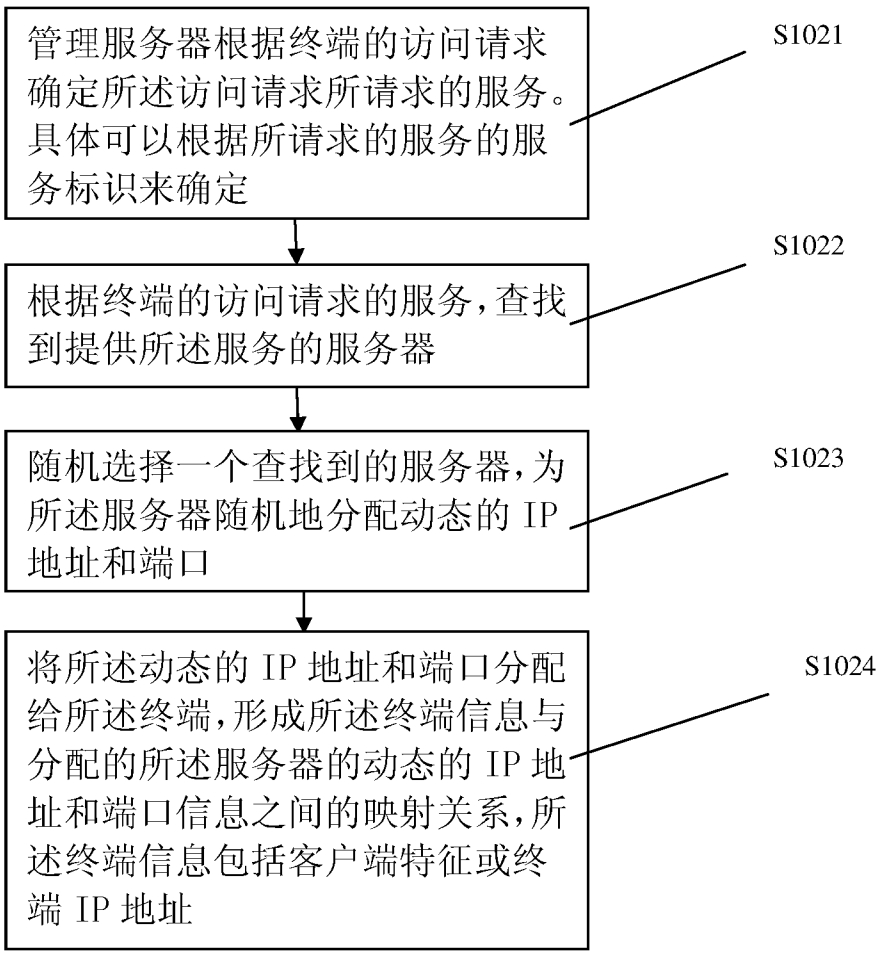

管理服务器根据终端的访问请求确定所述访问请求所请求的服务。具体可以根据所请求的服务的服务标识来确定
S1021
根据终端的访问请求的服务，查找到提供所述服务的服务器
S1022
随机选择一个查找到的服务器，为所述服务器随机地分配动态的 IP 地址和端口
S1023
将所述动态的 IP 地址和端口分配给所述终端，形成所述终端信息与分配的所述服务器的动态的 IP 地址和端口信息之间的映射关系，所述终端信息包括客户端特征或终端 IP 地址
S1024

图 3

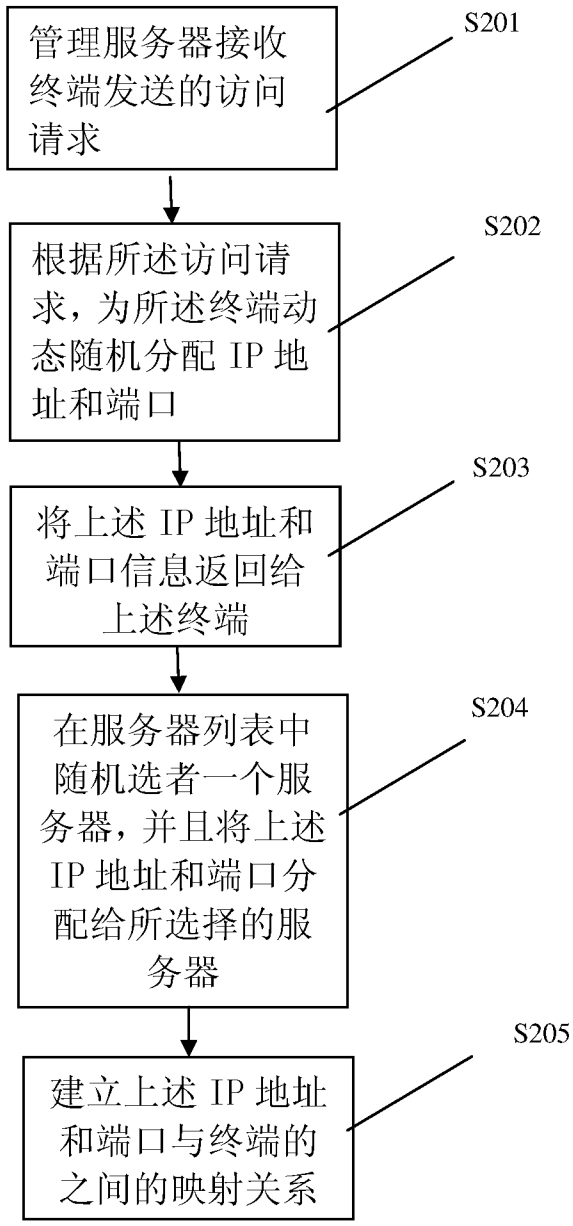

管理服务器接收终端发送的访问请求
S201
根据所述访问请求，为所述终端动态随机分配 IP 地址和端口
S202
将上述 IP 地址和端口信息返回给上述终端
S203
在服务器列表中随机选者一个服务器，并且将上述 IP 地址和端口分配给所选择的服务器
S204
建立上述 IP 地址和端口与终端的之间的映射关系
S205

图 4

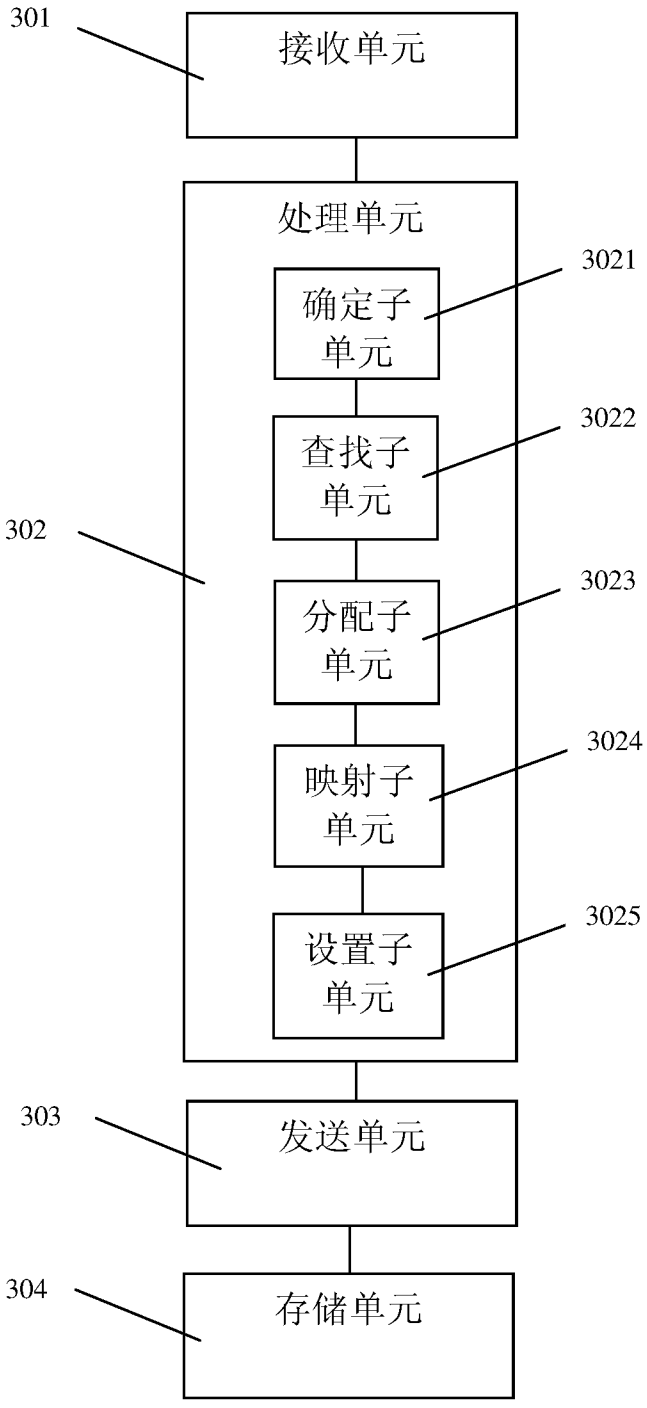

301
接收单元
处理单元
3021
确定子单元
3022
查找子单元
302
3023
分配子单元
3024
映射子单元
3025
设置子单元
303
发送单元
304
存储单元

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/074422

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70 (2013.01) i; H04L 29/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNKI; SIPOABS; VEN: IP, server, allocat+, distribut+, address??, assign+, dynamic, random, access+, map+, safe+, security, fluctuate, time, availab+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104168165 A (UNIV BEIJING JIAOTONG) 26 November 2014 (26.11.2014) description, paragraphs [0056] to [0148], claims 1 to 14, and figures 1 to 3	1-14
X	CN 103916492 A (SINFOR NETWORK TECHNOLOGY SHENZHEN CO.) 09 July 2014 (09.07.2014) description, paragraphs [0018] to [0068], and figures 1 to 3	1-14
X	CN 103888358 A (CHINA MOBILE COMMUNICATION CORP.) 25 June 2014 (25.06.2014) description, paragraphs [0040] to [0073], and figures 1 to 3	1-14
A	US 2011208846 A1 (ITO KIYOSHIGE) 25 August 2011 (25.08.2011) the whole document	1-14
A	CN 1456979 A (ZHIWANG GLOBAL SCI & TECHNOLOGY CO., LTD.) 19 November 2003 (19.11.2003) the whole document	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 May 2016	30 May 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer XUE, Yu Telephone No. (86-10) 62089405

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/074422

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104168165 A	26 November 2014	None	
CN 103916492 A	09 July 2014	None	
CN 103888358 A	25 June 2014	None	
US 2011208846 A1	25 August 2011	US 8452895 B2	28 May 2013
		WO 2010032382 A1	25 March 2010
		JP 5072788 B2	14 November 2012
		JP 2010074610 A	02 April 2010
CN 1456979 A	19 November 2003	None	

国际检索报告

国际申请号
PCT/CN2016/074422

A. 主题的分类

H04L 12/70(2013.01)i; H04L 29/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L, H04W, H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS;CNKI;SIPOABS;VEN:接入, 浮动, 分配, 地址, 随机, 动态, 访问, 时效, 有效时间, 映射, 服务器, 安全; IP, server, allocat+, distribut+, address??, assign+, dynamic, random, access+, map+, safe+,security, fluctuate, time, availab+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 104168165 A (北京交通大学) 2014年 11月 26日 (2014-11-26) 说明书第56-148段, 权利要求1-14, 及图1-4	1-14
X	CN 103916492 A (深信服网络科技深圳有限公司) 2014年 7月 9日 (2014-07-09) 说明书第18-68段, 及图1-3	1-14
X	CN 103888358 A (中国移动通信集团公司) 2014年 6月 25日 (2014-06-25) 说明书第40-73段, 及图1-3	1-14
A	US 2011208846 A1 (ITO KIYOSHIGE) 2011年 8月 25日 (2011-08-25) 全文	1-14
A	CN 1456979 A (智旺全球科技股份有限公司) 2003年 11月 19日 (2003-11-19)	1-14

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型:

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 5月 5日	2016年 5月 30日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	薛钰
传真号 (86-10)62019451	电话号码 (86-10)62089405

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/074422

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104168165	A	2014年 11月 26日	无			
CN	103916492	A	2014年 7月 9日	无			
CN	103888358	A	2014年 6月 25日	无			
US	2011208846	A1	2011年 8月 25日	US	8452895	B2	2013年 5月 28日
				WO	2010032382	A1	2010年 3月 25日
				JP	5072788	B2	2012年 11月 14日
				JP	2010074610	A	2010年 4月 2日
CN	1456979	A	2003年 11月 19日	无			