IP地址管理方法和系统、动态主机配置协议服务器

申请号：201010188309.X
申请日：2010-05-21

申请(专利权)人　中国科学院计算机网络信息中心　北龙中网(北京)科技有限责任公司
地址　100190 北京市海淀区中关村南四街四号
发明(设计)人　毛伟　李晓东　陈涛　沈烁　卢文哲

主分类号　H04L29/12(2006.01)I
分类号　H04L29/12(2006.01)I　H04L29/06(2006.01)I
公开(公告)号　101924801A
公开(公告)日　2010-12-22
专利代理机构　北京同立钧成知识产权代理有限公司　11205
代理人　刘芳

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101924801 A
(43)申请公布日 2010.12.22

(21)申请号 201010188309.X

(22)申请日 2010.05.21

(71)申请人 中国科学院计算机网络信息中心
地址 100190 北京市海淀区中关村南四街四号
申请人 北龙中网(北京)科技有限责任公司

(72)发明人 毛伟 李晓东 陈涛 沈烁 卢文哲

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
H04L 29/12(2006.01)
H04L 29/06(2006.01)

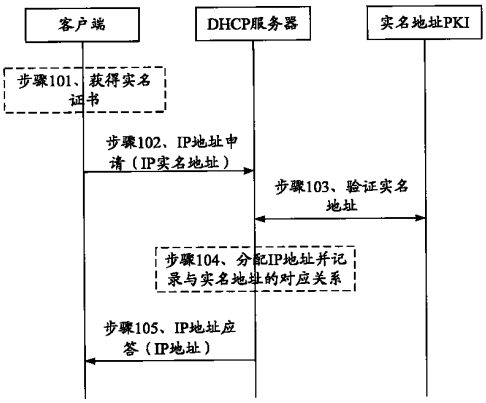
权利要求书 1 页 说明书 6 页 附图 4 页

(54)发明名称

IP地址管理方法和系统、动态主机配置协议服务器

(57)摘要

本发明提供一种IP地址管理方法和系统、动态主机配置协议服务器，其中，方法包括：接收客户端发送的IP地址申请消息，所述IP地址申请消息中携带标识所述客户端的用户身份的IP实名地址；为所述客户端分配IP地址，并将所述IP地址与所述IP实名地址的对应关系记录在数据库中；向所述客户端返回IP地址应答消息，所述IP地址应答消息中携带分配的所述IP地址。本发明通过引入一种IPv6实名地址及其资源PKI，结合扩展的DNS协议增强了DHCP协议的客户认证能力。



CN 101924801 A

1. 一种 IP 地址管理方法，其特征在于，包括：

接收客户端发送的 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；

向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

2. 根据权利要求 1 所述的 IP 地址管理方法，其特征在于，所述实名地址包括：

实名地址空间前缀，用于标识地址空间为实名地址空间；

授权层次关系段，用于存储所述实名地址的各级授权层次关系；

用户 ID，用于与所述客户端的用户身份一一对应。

3. 根据权利要求 1 所述的 IP 地址管理方法，其特征在于，在所述为所述客户端分配 IP 地址之前还包括：

利用实名地址资源公钥基础设施逐级获取上级证书，构建证书链，验证所述 IP 实名地址的真实性。

4. 根据权利要求 1 所述的 IP 地址管理方法，其特征在于，还包括：

记录所述 IP 地址的使用时间、所述客户端的 MAC 地址、接入局域网和端口号。

5. 根据权利要求 1 所述的 IP 地址管理方法，其特征在于，还包括：

将所述 IP 地址与所述 IP 实名地址的对应关系发送至 DNS 服务器。

6. 一种动态主机配置协议服务器，其特征在于，包括：

接收模块，用于接收客户端发送的 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

记录模块，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；

发送模块，用于向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

7. 根据权利要求 6 所述的动态主机配置协议服务器，其特征在于，还包括：

验证模块，用于利用实名地址资源公钥基础设施逐级获取上级证书，构建证书链，验证所述 IP 实名地址的真实性。

8. 根据权利要求 6 所述的动态主机配置协议服务器，其特征在于，所述记录模块，还用于记录所述 IP 地址的使用时间、所述客户端的 MAC 地址、接入局域网和端口号。

9. 根据权利要求 6 所述的动态主机配置协议服务器，其特征在于，所述发送模块，还用于将所述 IP 地址与所述 IP 实名地址的对应关系发送至 DNS 服务器。

10. 一种 IP 地址管理系统，其特征在于，包括：客户端和动态主机配置协议服务器；

所述客户端，用于向所述动态主机配置协议服务器发送 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

所述动态主机配置协议服务器，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；并向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

IP 地址管理方法和系统、动态主机配置协议服务器

技术领域

[0001] 本发明涉及计算机技术，特别涉及一种 IP 地址管理方法和系统、动态主机配置协议服务器。

背景技术

[0002] 为了能够动态地分配 IP 地址，1993 年，国际互联网工程任务组 (InternetEngineering Task Force，简称：IETF) 提出了动态主机配置协议 (Dynamic HostConfiguration Protocol，简称：DHCP)。DHCP 的前身是 BOOTP，BOOTP 原本是用在无磁盘主机连接的网络上面的，网络主机可以使用 BOOT ROM 而不是磁盘启动并连接上网络，BOOTP 则可以自动地为主机设定 TCP/IP 环境。

[0003] DHCP 可以说是 BOOTP 的增强版本，它分为两个部分：一个是服务器端，而另一个是客户端。上网用户属于客户端，其在上网时需要向 DHCP 服务器端申请 IP 地址。所有的 IP 网络设定数据都由 DHCP 服务器集中管理，并负责处理客户端的地址申请请求；而客户端则会使用从服务器分配下来的 IP 环境数据。随着 IPv4 地址的耗尽和 IPv6 地址的使用，IETF RFC3315 中规定了 DHCPv6 协议，专门用来处理 IPv6 地址的自动分配问题。DHCPv6 协议对原有的 DHCP 协议进行了简化，统一了数据包结构，具有更好的协议扩展性。DHCPv6 协议可以提供动态的 IPv6 地址分配服务，有效减轻了网络管理的负担。

[0004] 但是，由于动态 IP 地址分配机制中，IP 地址的分配是随机的，其使用者也是不断变动的，因此，可能带来一些严重的安全问题：网络攻击者可以使用动态 IP 地址进行网络攻击、木马邮件的发送，攻击过程中使用的 IP 地址在攻击过后会被回收并有可能分配给其它机器重新使用。因此，同一 IP 地址可能被多个使用者使用过，无法查证攻击者是哪一个，使得作为攻击追踪重要线索的 IP 地址因为当前的动态分配机制很难发挥可靠的追溯作用。

发明内容

[0005] 本发明的目的是提供一种 IP 地址管理方法和系统、动态主机配置协议服务器，以实现可以得知 IP 地址的使用情况，为追溯网络攻击等网络安全防范工作发挥作用。

[0006] 本发明提供一种 IP 地址管理方法，包括：

[0007] 接收客户端发送的 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

[0008] 为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；

[0009] 向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

[0010] 本发明提供一种动态主机配置协议服务器，包括：

[0011] 接收模块，用于接收客户端发送的 IP 地址申请消息，所述 IP 地址申请消息中携带

标识所述客户端的用户身份的 IP 实名地址；

[0012] 记录模块，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；

[0013] 发送模块，用于向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

[0014] 本发明提供一种 IP 地址管理系统，包括：客户端和动态主机配置协议服务器；

[0015] 所述客户端，用于向所述动态主机配置协议服务器发送 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

[0016] 所述动态主机配置协议服务器，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；并向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

[0017] 本发明的 IP 地址管理方法和系统、动态主机配置协议服务器，通过记录和存储 IP 地址与用户身份之间的对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用；并且，通过将该对应关系发布至 DNS 服务器，使得应用服务器向客户端提供服务之前确定该 IP 地址用户的身份，从而实现了实时有效的身份认证和访问控制；通过引入一种 IPv6 实名地址及其资源 PKI，结合扩展的 DNS 协议增强了 DHCP 协议的客户认证能力。

附图说明

[0018] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0019] 图 1 为本发明 IP 地址管理方法实施例一的信令示意图；

[0020] 图 2 为本发明 IP 地址管理方法实施例一中的 IP 实名地址结构示意图；

[0021] 图 3 为本发明 IP 地址管理方法实施例一中的 PKI 层次设计示意图；

[0022] 图 4 为本发明 IP 地址管理方法实施例二的信令示意图；

[0023] 图 5 为本发明 DHCP 服务器实施例的结构示意图；

[0024] 图 6 为本发明 IP 地址管理系统实施例的结构示意图。

具体实施方式

[0025] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0026] 本发明的主要技术方案为，客户端在向 DHCP 服务器发送的 IP 地址申请消息中，可以携带标识客户端用户身份的 IP 实名地址；DHCP 服务器为客户端分配 IP 地址，将所述 IP 地址发送至客户端，并将所述 IP 地址与 IP 实名地址绑定，将其对应关系记录在数据库中。其中，本方案可以适用于 IPv6 地址的动态分配，通过记录和存储 IP 地址与用户身份之间的

对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用。

[0027] 下面通过附图和具体实施例，对本发明的技术方案做进一步的详细描述。

[0028] 实施例一

[0029] 图 1 为本发明 IP 地址管理方法实施例一的信令示意图，如图 1 所示，本实施例中的 IP 地址可以是指 IPv6 地址，IP 实名地址可以是指 IPv6 实名地址，其可以包括以下步骤：

[0030] 步骤 101、客户端用户申请获得实名证书，该实名证书中包括代表用户身份的 IP 实名地址；

[0031] 在本实施例中，互联网用户在申请动态 IP 地址资源时，必须先取得地址注册机构签发的实名证书。该实名证书是一数字证书，其中包括了能够代表互联网用户身份的 IP 实名地址。该实名地址可以是从 IPv6 地址空间单独分离出的一段不可路由的 IPv6 地址。

[0032] 上述的 IP 实名地址的基本结构可以参见附图 2，图 2 为本发明 IP 地址管理方法实施例一中的 IP 实名地址结构示意图。其可以将 IPv6 地址空间的 128 位 IPv6 地址分成 3 部分，最前面的 n 比特位做为实名地址空间前缀（例如，002），用于区分该 IPv6 地址为可路由单播地址或者 IPv6 实名地址；接下来的 64-n 比特位可以存储该实名地址的授权层次关系，其由管理 IPv6 实名地址空间的国家互联网注册机构 (National Internet Registry，简称：NIR) 先分配给某个骨干网的互联网服务提供商 (Internet Service Provider，简称：ISP) 或本地互联网注册机构 (Local Internet Registry，简称：LIR)，骨干网的 ISP 再将地址块细分，分配给各个地区的中小 ISP；后 64 比特位可以使用散列函数等方法产生与客户端的用户身份一一对应的用户 ID。

[0033] 其中，该 IP 实名地址中的前 64 由地址分配机构进行分配；其后 64 比特位的实名用户 ID，在具体实施中，可以采用用户身份号码、通信公钥和 3bit 安全参数，按照预定的算法产生得到上述的实名用户 ID，因此，该实名用户 ID 是与用户身份号码一一对应的。通过在上述产生实名用户 ID 的过程中采用 3bit 安全参数，可以增加身份破解的难度，加强了安全保障。

[0034] 步骤 102、客户端向 DHCP 服务器发送 IP 地址申请消息，并在该消息中携带标识客户端用户身份的 IP 实名地址；

[0035] 客户端用户在申请得到地址注册机构签发的 IP 实名地址后，则向 DHCP 服务器发送 IP 地址申请消息。具体的，客户端可以先通过广播查找报文得到能提供服务的多个 DHCP 服务器的应答；客户端可以选择一个 DHCP 服务器发送请求 IP 地址的报文，即上述的 IP 地址申请消息，请求获取上网所需的 IP 地址，并将标识其身份的 IP 实名地址携带在 IP 地址申请消息中，发送至 DHCP 服务器。

[0036] 步骤 103、DHCP 服务器通过实名地址资源 PKI 对上述实名地址进行验证，若验证通过，则继续执行步骤 104；否则可以向客户端返回请求失败消息；

[0037] DHCP 服务器在接收到客户端发送的 IP 地址申请消息后，则对该消息中携带的 IP 实名地址进行验证。具体的，可以借助实名地址资源公钥基础设施 (Public Key Infrastructure，简称：PKI) 进行 IP 实名地址的验证。

[0038] 可参见附图 3，图 3 为本发明 IP 地址管理方法实施例一中的 PKI 层次设计示意图。用于验证上述 IPv6 实名地址的实名地址资源 PKI 可以按照图 3 所示的 IP 地址分配管理

层次进行如下设计：实名地址资源 PKI 的信任锚设为 NIR（根 CA）；NIR 为下级 LIR/ISP 分配 IPv6 实名地址段，同时签发代表相应实名地址段管理权的 CA 证书；ISP 得到授权管辖的 IPv6 实名地址段后，当客户端用户申请 IPv6 实名证书时，ISP 将用本级 CA 证书为用户签发 EE 证书，证明用户对该 IPv6 实名地址的使用权。

[0039] 当 DHCP 服务器对 IP 实名地址进行验证时，可以根据图 2 所示的 IP 实名地址的中间段（64-n 比特位）中所存储的层次关系，利用实名地址资源 PKI 逐级获取上级的 ISP CA 证书，组成证书链，从而验证 IPv6 实名证书的真实性。若验证不通过，则可以向客户端返回请求失败消息；否则，可以继续执行步骤 104。通过在 IPv6 地址空间中单独划出一段 IPv6 地址作为上网用户的身份标识，并由地址分配机构签发相应的实名证书给上网用户，使用实名地址资源 PKI 对代表用户身份的 IPv6 实名地址进行验证，解决了互联网统一身份认证的问题。

[0040] 步骤 104、DHCP 服务器为客户端分配 IP 地址，并记录所述 IP 地址与所述 IP 实名地址的对应关系；

[0041] DHCP 服务器在验证 IP 实名地址为真实之后，可以将分配给用户的 IP 地址等信息与该 IP 实名地址的对应关系记录和存储，建立 IPv6 实名地址和用户使用的 IP 地址之间的映射数据库，其中包括 IP 地址使用时间、用户的 MAC 地址、接入 VLAN 和端口号等信息。

[0042] 这些信息使得动态 IP 地址资源的使用情况有统一格式的数据库可以查找，相对于现有技术，大大方便了对于 IP 地址使用情况的查询，为 IP 地址追溯提供了可能。当网络攻击事件发生时，就可以通过与通信 IP 地址相关联的 IP 实名地址来追溯到客户端使用者的真实身份，从而制止网络攻击事件的进一步发展。

[0043] 步骤 105、DHCP 服务器向客户端发送 IP 地址应答消息，将分配的 IP 地址发送至客户端。

[0044] DHCP 服务器在存储了 IP 地址与 IP 实名地址的绑定关系之后，则将该分配的 IP 地址携带在 IP 地址应答消息中，发送至客户端。此外，例如，当该客户端用户 A 使用完后，DHCP 服务器可以将该 IP 地址回收，分配给另外的客户端用户 B 使用，此时，DHCP 服务器会记录该 IP 地址与客户端用户 B 的 IP 实名地址的对应关系，但是，也仍然会保留该 IP 地址与客户端用户 A 的 IP 实名地址之间的对应关系，以及客户端用户 A 使用该 IP 地址的时间等信息，使得后续可以对该 IP 地址使用的相关历史记录进行查询和追溯。

[0045] 本实施例的 IP 地址管理方法，通过记录和存储 IP 地址与用户身份之间的对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用。

[0046] 实施例二

[0047] 图 4 为本发明 IP 地址管理方法实施例二的信令示意图，如图 4 所示，本实施例的方法与实施例一的主要区别在于，为了进一步方便互联网应用访问的实时控制，增加了对于 DNS 服务器的功能扩展；其中，本实施例的方法中，步骤 201 ～ 205 与实施例一的步骤 101 ～ 105 相同，具体可参见实施例一，在此不再赘述，本实施例还增加了互联网应用访问的步骤，具体如下：

[0048] 步骤 201、客户端用户申请获得实名证书，该实名证书中包括代表用户身份的 IP 实名地址；

[0049] 步骤 202、客户端向 DHCP 服务器发送 IP 地址申请消息，并在该消息中携带标识客户端用户身份的 IP 实名地址；

[0050] 步骤 203、DHCP 服务器通过实名地址资源 PKI 对上述实名地址进行验证，若验证通过，则继续执行步骤 104；否则可以向客户端返回请求失败消息；

[0051] 步骤 204、DHCP 服务器为客户端分配 IP 地址，并记录所述 IP 地址与所述 IP 实名地址的对应关系；

[0052] 步骤 205、DHCP 服务器向客户端发送 IP 地址应答消息，将分配的 IP 地址发送至客户端；

[0053] 步骤 206、DHCP 服务器将所述 IP 地址与所述 IP 实名地址的对应关系信息发送至 DNS 服务器；

[0054] 需要说明的是，该步骤和步骤 205 并没有特定的时间先后顺序。在具体实施中，DHCP 服务器可以通过添加一扩展的 DNS RR IPV6ID 记录至 DNS 服务器，将 IP 地址和 IPv6 实名地址的对应关系发布到互联网上。该 RR IPV6ID 记录中包括了 IPv6 实名地址和公钥等信息，其基本格式可以如下：

[0055] IPv6.arpa IN IPV6ID(pk-algorithm /* 加密算法 */

[0056] base16-encoded-hit /* 经过 base16 编码 IPv6 实名地址 */

[0057] base64-encoded-public-key /* 经过 base64 编码的公钥信息 */)

[0058] 通过将动态 IP 地址与其使用者的 IPv6 实名地址记录在 DNS 服务器上，提供了一种查询动态 IP 地址使用者身份的方法，应用服务器可以使用 DNS 查询到动态 IP 地址使用者的身份并进行验证。

[0059] 步骤 207、客户端向应用服务器提出应用服务申请消息，请求使用应用服务器所提供的服务；

[0060] 步骤 208、应用服务器提取客户端的 IP 地址，并向 DNS 服务器发送 IP 查询消息，请求查询客户端用户的身份；其中，所述 IP 查询消息中携带客户端的 IP 地址；

[0061] 步骤 209、DNS 服务器根据其接收到的客户端的 IP 地址，以及其内存储的 RR IPV6ID 记录中的相关信息，得到与该 IP 地址对应的 IPv6 实名地址及公钥信息，将其携带在 IP 应答消息中返回至应用服务器；

[0062] 步骤 210、应用服务器产生一个随机数，并用接收到的所述公钥加密后发送给请求服务的客户端用户；

[0063] 步骤 211、客户端用户使用与公钥对应的私钥解密后，返回原随机数至应用服务器；

[0064] 步骤 212、应用服务器得到 IPv6 实名地址中的用户 ID 等信息，对客户端用户的身份进行验证，当验证通过后，则执行步骤 213；

[0065] 步骤 213、应用服务器向客户端提供其所请求的服务。

[0066] 本实施例的 IP 地址管理方法，通过记录和存储 IP 地址与用户身份之间的对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用；并且，通过将该对应关系发布至 DNS 服务器，使得应用服务器向客户端提供服务之前确定该 IP 地址用户的身份，从而实现了实时有效的身份认证和访问控制；通过引入一种 IPv6 实名地址及其资源 PKI，结合扩展的 DNS 协议增强了 DHCP 协议的客户认证能力。

[0067] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0068] 实施例三

[0069] 图 5 为本发明 DHCP 服务器实施例的结构示意图，如图 5 所示，本实施例的 DHCP 服务器可以包括接收模块 31、记录模块 32 和发送模块 33。

[0070] 其中，接收模块 31，用于接收客户端发送的 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；记录模块 32，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；发送模块 33，用于向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

[0071] 此外，进一步的，该 IP 地址管理系统还可以包括验证模块 34，用于利用实名地址资源 PKI 逐级获取上级的 ISP CA 证书，构建证书链，验证所述 IP 实名地址的真实性。

[0072] 进一步，记录模块 32，还可以用于记录所述 IP 地址的使用时间、所述客户端的 MAC 地址、接入局域网和端口号；发送模块 33，还可以用于将所述 IP 地址与所述 IP 实名地址的对应关系发送至 DNS 服务器。

[0073] 本实施例的 DHCP 服务器，通过记录和存储 IP 地址与用户身份之间的对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用。

[0074] 实施例四

[0075] 图 6 为本发明 IP 地址管理系统实施例的结构示意图，如图 6 所示，该系统可以包括客户端 41 和 DHCP 服务器 42。

[0076] 其中，客户端 41，用于向所述 DHCP 服务器发送 IP 地址申请消息，所述 IP 地址申请消息中携带标识所述客户端的用户身份的 IP 实名地址；

[0077] DHCP 服务器 42，用于为所述客户端分配 IP 地址，并将所述 IP 地址与所述 IP 实名地址的对应关系记录在数据库中；并向所述客户端返回 IP 地址应答消息，所述 IP 地址应答消息中携带分配的所述 IP 地址。

[0078] 本实施例的 IP 地址管理系统，通过记录和存储 IP 地址与用户身份之间的对应关系信息，使得后续可以方便地对 IP 地址的使用情况进行查询和追溯，提高了网络安全防范作用。

[0079] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

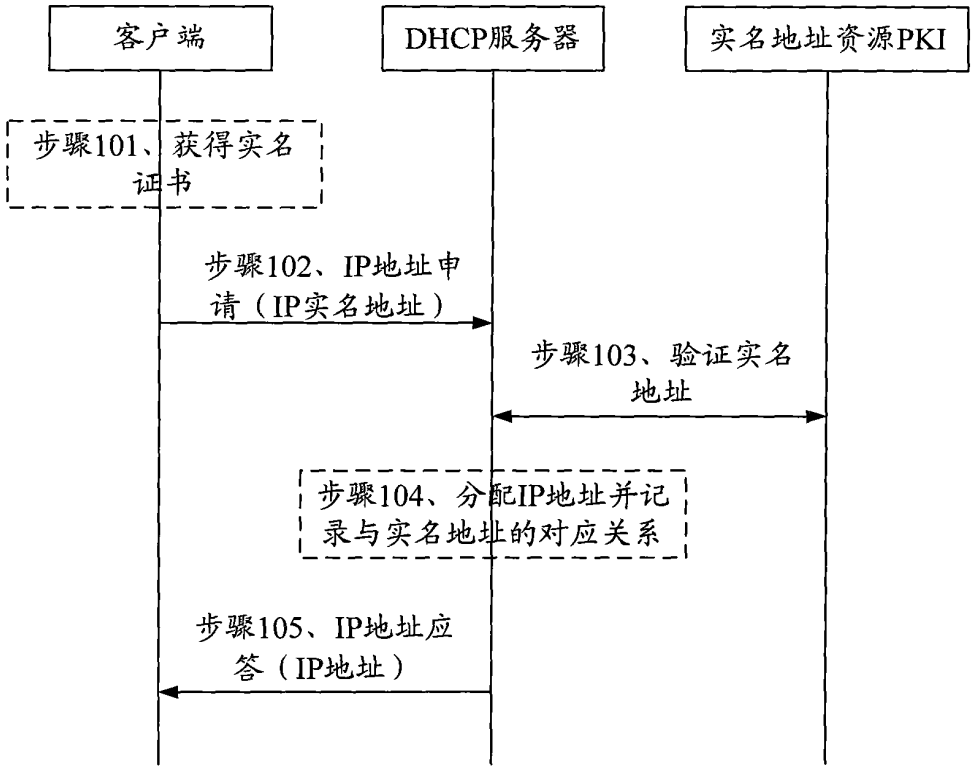

客户端
DHCP服务器
实名地址资源PKI
步骤101、获得实名证书
步骤102、IP地址申请（IP实名地址）
步骤103、验证实名地址
步骤104、分配IP地址并记录与实名地址的对应关系
步骤105、IP地址应答（IP地址）

图 1

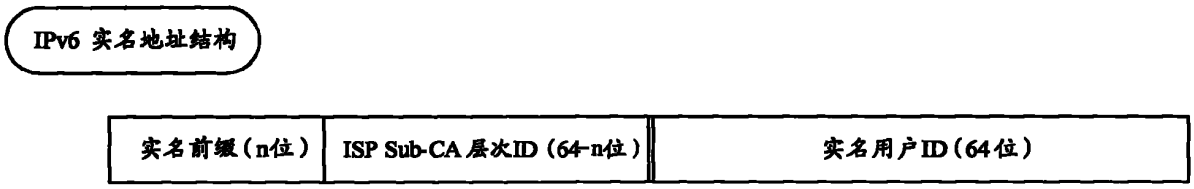

IPv6 实名地址结构
实名前缀（n位）
ISP Sub-CA 层次ID（64-n位）
实名用户ID（64位）

图 2

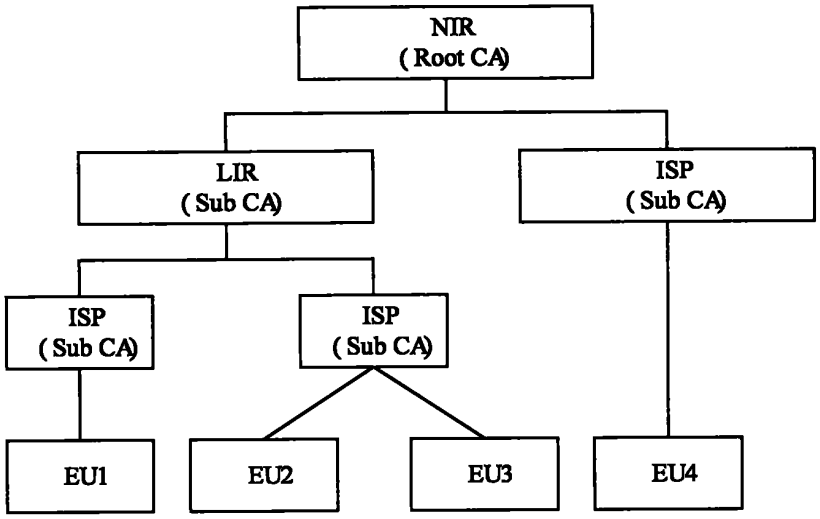

NIR
(Root CA)
LIR
(Sub CA)
ISP
(Sub CA)
ISP
(Sub CA)
ISP
(Sub CA)
EU1
EU2
EU3
EU4

图 3

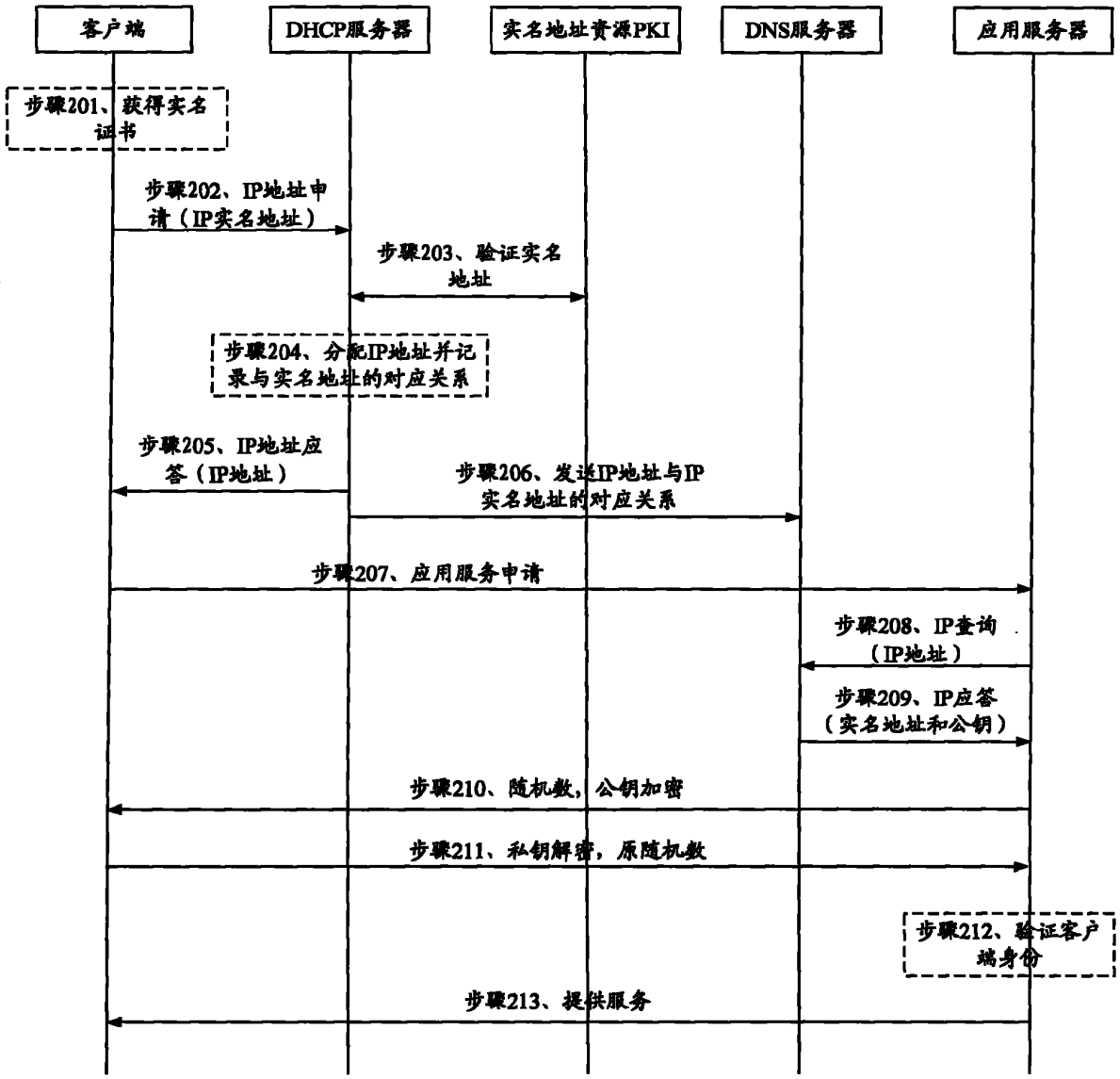

客户端
DHCP服务器
实名地址资源PKI
DNS服务器
应用服务器
步骤201、获得实名证书
步骤202、IP地址申请（IP实名地址）
步骤203、验证实名地址
步骤204、分配IP地址并记录与实名地址的对应关系
步骤205、IP地址应答（IP地址）
步骤206、发送IP地址与IP实名地址的对应关系
步骤207、应用服务申请
步骤208、IP查询（IP地址）
步骤209、IP应答（实名地址和公钥）
步骤210、随机数，公钥加密
步骤211、私钥解密，原随机数
步骤212、验证客户端身份
步骤213、提供服务

图 4

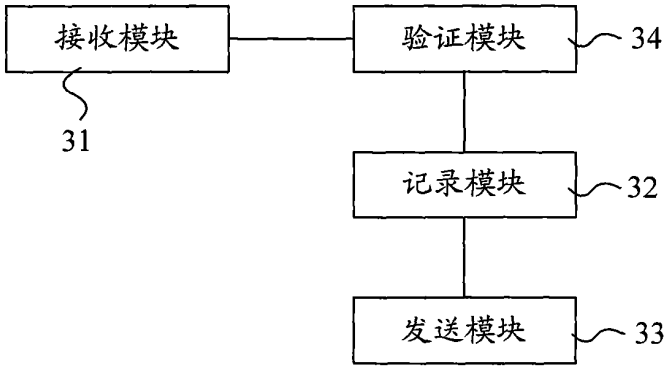

接收模块
31
验证模块
34
记录模块
32
发送模块
33

图 5

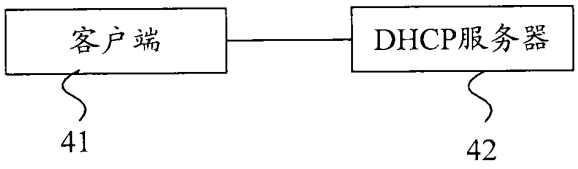


图 6