

(12) 发明专利

(10) 授权公告号 CN 102318314 B

(45) 授权公告日 2013. 09. 11

(21) 申请号 201180001196. 0

H04L 29/12 (2006. 01)

(22) 申请日 2011. 07. 29

(56) 对比文件

(85) PCT申请进入国家阶段日
2011. 08. 31

CN 1630252 A, 2005. 06. 22, 全文 .
CN 101056178 A, 2007. 10. 17, 全文 .

(86) PCT申请的申请数据
PCT/CN2011/077781 2011. 07. 29

审查员 万沙沙

(87) PCT申请的公布数据
W02012/109854 ZH 2012. 08. 23

(73) 专利权人 华为技术有限公司
地址 518129 中国广东省深圳市龙岗区坂田
华为总部办公楼

(72) 发明人 唐鹏合

(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 29/06 (2006. 01)

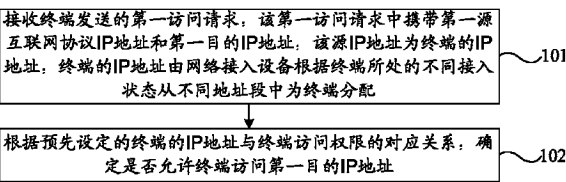
权利要求书3页 说明书9页 附图3页

(54) 发明名称

访问权限控制方法和设备

(57) 摘要

本发明实施例涉及一种访问权限控制方法和设备。方法包括 :接收终端发送的第一访问请求,所述访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,所述第一源 IP 地址为所述终端的 IP 地址,所述终端的 IP 地址由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配 ;根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许所述终端访问所述第一目的 IP 地址。本发明实施例通过访问权限控制方法和设备,实现节约 NAD 的存储资源,确保 NAD 对终端的访问进行控制。



1. 一种访问权限控制方法,其特征在于,包括:

接收终端发送的第一访问请求,所述访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,所述第一源 IP 地址为所述终端的 IP 地址,所述终端的 IP 地址由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配;

根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许所述终端访问所述第一目的 IP 地址。

2. 根据权利要求 1 所述的方法,其特征在于,所述终端的 IP 地址与终端访问权限的对应关系包括:

终端的 IP 地址为任意地址,则对应的终端访问权限为公共权限;

终端的 IP 地址位于地址池中的第一地址段,则对应的终端访问权限为用户组最小授权权限;

终端的 IP 地址位于所述地址池中的第二地址段,则对应的终端访问权限为用户组权限;

终端的 IP 地址位于所述地址池中的第三地址段,则对应的终端访问权限为用户组隔离受限权限。

3. 根据权利要求 2 所述的方法,其特征在于,所述接收终端发送的第一访问请求之前,还包括:

若在终端认证和身份识别通过后,且状态检查通过前接收到所述终端发送的第一获取 IP 地址请求,则从所述地址池中的所述第一地址段中为所述终端分配 IP 地址;

或者,若接收到状态检查服务器发送的终端状态检查通过通知消息,则从所述地址池中的所述第二地址段中为所述终端分配 IP 地址;

或者,若接收到所述状态检查服务器发送的终端隔离通知消息,则从所述地址池中的第三地址段中为所述终端分配 IP 地址;

或者,若接收到所述状态检查服务器发送的终端状态修复完成通知,则从所述地址池中的第二地址段中为所述终端分配 IP 地址。

4. 根据权利要求 3 所述的方法,其特征在于,从所述第一地址段中为所述终端分配的 IP 地址为临时地址,从所述第二地址段中为所述终端分配的 IP 地址为正常地址,从所述第三地址段中为所述终端分配的 IP 地址为隔离地址。

5. 根据权利要求 4 所述的方法,其特征在于,所述若接收到状态检查服务器发送的终端状态检查通过通知消息,则从所述地址池中的所述第二地址段中为所述终端分配 IP 地址,具体为:

若接收到所述状态检查服务器发送的终端状态检查通过通知消息后,接收到所述终端发送的续租报文消息,所述续租报文消息用于请求续租所述临时地址,则向所述终端发送动态主机配置协议否定响应 DHCP NAK 报文,以触发所述终端发起第二获取 IP 地址请求;

根据所述终端发起的所述第二获取 IP 地址请求,从所述地址池中的所述第二地址段中为所述终端分配所述正常地址。

6. 根据权利要求 4 所述的方法,其特征在于,所述若接收到所述状态检查服务器发送的终端隔离通知消息,则从所述地址池中的第三地址段中为所述终端分配 IP 地址,具体为:

若接收到所述状态检查服务器发送的终端隔离通知消息,向所述终端发送扩展协议 EAP 消息,以触发所述终端发起第一释放 IP 地址请求及发起第三获取 IP 地址请求,所述第一释放 IP 地址请求用于请求释放所述正常地址;

根据所述终端发起的所述第三获取 IP 地址请求,从所述地址池中的第三地址段中为所述终端分配所述隔离地址。

7. 根据权利要求 4 所述的方法,其特征在于,所述若接收到所述状态检查服务器发送的终端状态修复完成通知,则从所述地址池中的第二地址段中为所述终端分配 IP 地址,具体为:

若接收到所述状态检查服务器发送的终端状态修复完成通知,则向所述终端发送扩展协议 EAP 消息,以触发所述终端发起第二释放 IP 地址请求及发起第四获取 IP 地址请求,所述第二释放 IP 地址请求用于请求释放所述隔离地址;

根据所述终端发起的所述第四获取 IP 地址请求,从所述地址池中的第二地址段中为所述终端分配所述正常地址。

8. 根据权利要求 3-7 任一项所述的方法,其特征在于,所述接收到状态检查服务器发送的终端隔离通知消息之后,还包括:

接收所述状态检查服务器下发的所述终端的访问控制列表 ACL。

9. 根据权利要求 8 所述的方法,其特征在于,所述接收所述状态检查服务器下发的所述终端的访问控制列表 ACL 之后,还包括:

接收所述终端发送的第二访问请求,所述第二访问请求中携带第二源 IP 地址和第二目的 IP 地址;

根据所述终端的 ACL,确定是否允许所述终端访问所述第二目的 IP 地址。

10. 一种网络接入设备,其特征在于,包括:

接收器,用于接收终端发送的第一访问请求,所述访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,所述第一源 IP 地址为所述终端的 IP 地址,所述终端的 IP 地址由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配;

处理器,用于根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许所述终端访问所述第一目的 IP 地址。

11. 根据权利要求 10 所述的网络接入设备,其特征在于,所述终端的 IP 地址与终端访问权限的对应关系包括:

终端的 IP 地址为任意地址,则对应的终端访问权限为公共权限;

终端的 IP 地址位于地址池中的第一地址段,则对应的终端访问权限为用户组最小授权权限;

终端的 IP 地址位于所述地址池中的第二地址段,则对应的终端访问权限为用户组权限;

终端的 IP 地址位于所述地址池中的第三地址段,则对应的终端访问权限为用户组隔离受限权限。

12. 根据权利要求 11 所述的网络接入设备,其特征在于,所述接收器还用于:接收终端发送的第一获取 IP 地址请求、状态检查服务器发送的终端状态检查通过通知消息、状态检查服务器发送的终端隔离通知消息和状态检查服务器发送的终端状态修复完成通知。

13. 根据权利要求 12 所述的网络接入设备,其特征在于,所述处理器还用于:

若所述接收器在所述终端认证和身份识别通过后,且状态检查通过前接收到所述终端发送的所述第一获取 IP 地址请求,则从所述地址池中的所述第一地址段中为所述终端分配 IP 地址;或者,若所述接收器接收到状态检查服务器发送的终端状态检查通过通知消息,则从所述地址池中的所述第二地址段中为所述终端分配 IP 地址;或者,若所述接收器接收到所述状态检查服务器发送的终端隔离通知消息,则从所述地址池中的第三地址段中为所述终端分配 IP 地址;或者,若所述接收器接收到所述状态检查服务器发送的终端状态修复完成通知,则从所述地址池中的第二地址段中为所述终端分配 IP 地址。

14. 根据权利要求 13 所述的网络接入设备,其特征在于,所述处理器从所述第一地址段中为所述终端分配的 IP 地址为临时地址,所述处理器从所述第二地址段中为所述终端分配的 IP 地址为正常地址,所述处理器从所述第三地址段中为所述终端分配的 IP 地址为隔离地址。

15. 根据权利要求 14 所述的网络接入设备,其特征在于,还包括:

第一发送器,用于若所述接收器接收到所述状态检查服务器发送的终端状态检查通过通知消息后,接收到所述终端发送的续租报文消息,所述续租报文消息用于请求续租所述临时地址,则向所述终端发送动态主机配置协议否定响应 DHCP NAK 报文,以触发所述终端发起第二获取 IP 地址请求;

所述处理器还用于:根据所述终端发起的所述第二获取 IP 地址请求,从所述地址池中的所述第二地址段中为所述终端分配所述正常地址。

16. 根据权利要求 14 所述的网络接入设备,其特征在于,还包括:

第二发送器,用于若所述接收器接收到所述状态检查服务器发送的终端隔离通知消息,则向所述终端发送扩展协议 EAP 消息,以触发所述终端发起第一释放 IP 地址请求及发起第三获取 IP 地址请求,所述第一释放 IP 地址请求用于请求释放所述正常地址;

所述处理器还用于:根据所述终端发起的第三获取 IP 地址请求,从所述地址池中的第三地址段中为所述终端分配所述隔离地址。

17. 根据权利要求 14 所述的网络接入设备,其特征在于,还包括:

第三发送器,用于若所述接收器接收到所述状态检查服务器发送的终端状态修复完成通知,则向所述终端发送扩展协议 EAP 消息,以触发所述终端发起第二释放 IP 地址请求及发起第四获取 IP 地址请求,所述第二释放 IP 地址请求用于请求释放所述隔离地址;

所述处理器还用于:根据所述终端发起的所述第四获取 IP 地址请求,从所述地址池中的第二地址段中为所述终端分配所述正常地址。

18. 根据权利要求 13-17 任一项所述的网络接入设备,其特征在于,所述接收器接收到状态检查服务器发送的终端隔离通知消息后,还用于:接收所述状态检查服务器下发的所述终端的访问控制列表 ACL。

19. 根据权利要求 18 所述的网络接入设备,其特征在于,所述接收器还用于:接收所述终端发送的第二访问请求,所述第二访问请求中携带 第二源 IP 地址和第二目的 IP 地址;

所述处理器还用于:根据所述终端的 ACL,确定是否允许所述终端访问所述第二目的 IP 地址。

访问权限控制方法和设备

技术领域

[0001] 本发明实施例涉及信息技术领域,特别涉及一种访问权限控制方法和设备。

背景技术

[0002] 网络准入控制 (Network Admission Control, NAC) 是一种“端到端”的安全结构,终端与网络接入设备 (Network Access Device, NAD),例如:交换机或者路由器之间的信息交互,通过 EAPoU DP 报文进行,也可通过 EAPo802.1X 接口(支持基于端口的认证)进行。

[0003] 现有技术中,终端通过 NAD 接入网络,认证/授权服务器(可以是远端用户拨号认证系统 (Remote Authentication Dial In User Service, RADIUS) 或者终端访问控制器访问控制系统 (Terminal Access Controller Access-Control System, TACACS)) 向 NAD 下发每个的终端的访问控制列表 (Access Control List, ACL),当 NAD 接收到终端发送的访问请求后,查找该终端的 ACL 来确定接受或拒绝终端的访问请求。然而,接入点需要保存每个终端的 ACL,并且每个终端在上线、下线或者状态改变时,认证/授权服务器需要重新向 NAD 下发或更新终端的 ACL,可能导致 NAD 中存储 ACL 的资源不足,进而使 NAD 无法对终端的访问进行控制。

发明内容

[0004] 本发明实施例提供一种访问权限控制方法和设备,以解决现有技术中 NAD 中存储 ACL 的资源不足,进而 NAD 无法对终端的访问进行控制的问题。

[0005] 本发明实施例提供了一种访问权限控制方法,包括:

[0006] 接收终端发送的第一访问请求,所述访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,所述第一源 IP 地址为所述终端的 IP 地址,所述终端的 IP 地址由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配;

[0007] 根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许所述终端访问所述第一目的 IP 地址。

[0008] 本发明实施例还提供一种网络接入设备,包括:

[0009] 接收器,用于接收终端发送的第一访问请求,所述访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,所述第一源 IP 地址为所述终端的 IP 地址,所述终端的 IP 地址由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配;

[0010] 处理器,用于根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许所述终端访问所述第一目的 IP 地址。

[0011] 本发明实施例通过访问权限控制方法和设备, NAD 根据终端的不同接入状态从不同地址段中为终端分配 IP 地址,使 NAD 接收到终端的访问请求时,能够根据预先设定的终端的 IP 地址与终端访问权限的对应关系,控制终端的访问权限,实现节约 NAD 的存储资源,确保 NAD 对终端的访问进行控制。

附图说明

[0012] 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。

[0013] 图 1 为本发明提供的访问权限控制方法一个实施例的流程图;

[0014] 图 2 为局域网中网络准入控制的结构框架图;

[0015] 图 3a 为本发明提供的终端接入网络前的终端认证流程图;

[0016] 图 3b 为本发明提供的终端接入网络过程中的终端状态检查流程图;

[0017] 图 3c 为本发明提供的终端接入网络后的流程图;

[0018] 图 4 为本发明提供的网络接入设备一个实施例的结构示意图;

[0019] 图 5 为本发明提供的网络接入设备又一个实施例的结构示意图。

具体实施方式

[0020] 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。

[0021] 图 1 为本发明提供的访问权限控制方法一个实施例的流程图,如图 1 所示,该方法包括:

[0022] S101、接收终端发送的第一访问请求,该第一访问请求中携带第一源互联网协议 IP 地址和第一目的 IP 地址,该第一源 IP 地址为终端的 IP 地址,终端的 IP 地址是由网络接入设备根据终端所处的不同接入状态从不同地址段中为终端分配的。

[0023] S102、根据预先设定的终端的 IP 地址与终端访问权限的对应关系,确定是否允许终端访问第一目的 IP 地址。

[0024] 以上步骤的执行主体为网络接入设备 NAD。

[0025] 本发明适用于企业网等各种类型的局域网,图 2 所示为局域网中网络准入控制的结构框架图,如图 2 所示的局域网中可以包括提供多种信息的服务器,图 2 所示的网络架构中,将信息划分为敏感信息区、核心信息区和一般信息区。每个信息区可以包括一个或多个提供信息的服务器。终端可以通过 NAD 接入网络中,由 NAD 控制终端对提供信息的服务器进行访问。

[0026] 终端接入网络时,可以登录门户服务器(portal 服务器),在 portal 服务器上输入用户名和密码,portal 服务器通过 portal 协议将终端输入的用户名和密码发送给 NAD。终端还可以通过 802.1x 协议直接访问 NAD,待 NAD 向终端返回响应后,终端可以将用户名和密码发送给 NAD。

[0027] 终端在接入网络前、接入网络过程中以及接入网络后,通常处于不同的接入状态,具体的:NAD 可以将终端的用户名和密码发送给认证和授权服务器(通常为 RADIUS 服务器),由认证和授权服务器对终端进行认证和身份识别,因此,在接入网络前,终端所处的接

入状态可以分为：“认证和身份识别通过前”和“认证和身份识别通过后”；终端在认证和身份识别通过后，状态检查服务器需要检查终端是否存在违规现象，具体是状态检查服务器触发终端上的客户端代理软件对终端进行扫描，例如：扫描终端的病毒库是否没有更新、终端是否没有安装安全软件、终端是否没有安装各种补丁等等，客户端代理软件对终端的扫描结束后，将扫描结果发送给状态检查服务器。如果终端不存在违规现象，则状态检查服务器的检查结果为检查通过，终端处于“状态检查通过”的接入状态，如果终端存在违规现象，则终端处于“状态检查违规”的接入状态；终端状态检查通过后，状态检查服务器可以定期触发终端的客户端代理软件对终端进行扫描，当检测到终端状态异常时，例如：终端感染病毒时，如果终端的异常状态对网络造成威胁，则需要对终端进行隔离，禁止终端接入网络，则终端处于“状态检测异常”的接入状态。

[0028] 而终端在处于不同的接入状态时，通常具有不同的访问权限，例如：当终端处于“认证和身份识别通过前”的接入状态时，终端具有的访问权限为公共权限，终端的 IP 地址为任意时均具有公共权限，公共权限是指能够访问局域网中提供共享资源的服务器，例如：对于企业网中的任意终端，均具有访问本公司公共资源的权限；当终端处于“认证和身份识别通过后”且“状态检查通过前”的接入状态时，终端具有的访问权限为用户组最小授权权限，在企业网等类型的局域网中，通常可以划分为多个用户组，例如：公司的研发部的多个终端可以划分为一个用户组，公司市场部的多个终端可以划分为一个用户组等等。用户组的最小授权权限可以是用户组内的公共权限，具有用户组的最小授权权限的终端可以访问用户组内提供共享资源的服务器；当终端处于“状态检查通过”接入状态时，终端具有的访问权限为用户组权限，具有用户组权限的终端，除了可以访问用户组内提供共享资源的服务器之外，还可以访问该用户组内的某些提供特定资源的服务器，这些特定资源可以是一些重要信息，也可以由各个用户组来设定；当终端处于“状态检测异常”接入状态时，则终端具有的访问权限为用户组隔离受限权限，其中，当终端“状态检测异常”，但终端对网络不构成危害时，可以通过状态修复服务器对终端的状态进行修复；如果终端对网络构成威胁时，则终端可以具有公共权限。

[0029] 由于终端处于不同接入状态时具有不同的访问权限，因此，NAD 可以在终端处于不同接入状态时，从不同的地址段为终端分配 IP 地址。NAD 可以预先建立终端的 IP 地址与终端访问权限的对应关系，从而使 NAD 在接收到终端的访问请求时，能够根据终端的 IP 地址判断终端是否具有访问目的地址的权限。

[0030] 具体的，NAD 可以在本地将地址池（具体可以是 NAD 管理的全部或部分地址段）划分为不同的地址段，每一地址段可以对应终端的一种接入状态，进而对应终端的一种访问权限，当终端处于该种接入状态时，NAD 可以从对应的地址段中为终端分配 IP 地址，当终端访问网络时，NAD 接收到终端发送的访问请求后，能够根据终端的 IP 地址获知终端对应的访问权限，从而根据终端的访问权限确定是否允许终端访问目的地址。或者，还可以在认证和授权服务器（RADIUS 服务器）上将地址池（具体可以是认证和授权服务器内存单元中存储的全部或部分地址段）划分为不同的地址段，每一地址段可以对应终端的一种接入状态，进而对应终端的一种访问权限，当终端处于该种接入状态时，认证和授权服务器（RADIUS 服务器）可以从对应地址段向 NAD 下发一个 IP 地址，NAD 将该 IP 地址分配给终端。

[0031] 需要说明的是,本实施例中仅以终端的“认证和身份识别通过前”、“认证和身份识别通过后”、“状态检查通过”、“状态检测异常”等接入状态为例进行说明,对应的,本实施例提供了以上几种接入状态对应的访问权限分别为:公共权限、用户组最小授权权限、用户组权限、用户组隔离受限权限。可以理解的是,本实施例仅是给出了终端的几种可能的接入状态极其对应的访问权限,实际上,终端在接入网络前、接入网络过程中和接入网络中,还可以进一步细化分为其他接入状态,相应的,对于终端的其他接入状态,各种局域网中也有相应的访问权限规定。因此,本发明实施例提供的终端接入状态类型及其对应的访问权限并不对本发明造成限制。

[0032] 本发明实施例通过访问权限控制方法和设备, NAD 根据终端的不同接入状态从不同地址段中为终端分配 IP 地址,使 NAD 接收到终端的访问请求时,能够根据设定的终端的 IP 地址与终端访问权限的对应关系,控制终端的访问权限,能够节约 NAD 的存储资源,确保 NAD 对终端的访问进行控制。

[0033] 图 3a- 图 3c 为本发明提供的访问权限控制方法又一个实施例的流程图,如图 3a- 图 3c 所示,本实施例提供了终端接入网络前、接入网络过程中和接入网络后, NAD 根据终端的接入状态从不同的地址段为终端分配 IP 地址的完整方法。该方法包括:

[0034] 一、终端接入网络前的终端认证流程,参见图 3a:

[0035] S201、终端通过 802. 1x 协议向 NAD 发送接入请求,请求接入接入局域网中。

[0036] 802. 1x 协议是 NAC 结构中常用的终端接入方式,可以理解的是,终端还可以通过其他协议或接口接入局域网中,本实施例中不一一赘述。

[0037] S202、NAD 向终端返回接入请求响应。

[0038] S203、终端向 NAD 发送用户名和密码。

[0039] S204、NAD 将终端的用户名和密码发送给认证和授权服务器(通常可以是 RADIUS 服务器)。

[0040] S205、认证和授权服务器根据终端的用户名和密码对终端进行认证和身份识别。

[0041] 此时,终端处于“认证和身份识别通过前”接入状态,终端具有的访问权限为公共权限。

[0042] S206、认证和授权服务器通知终端认证和身份识别通过后,NAD 记录终端的接入状态为“认证和身份识别通过”。

[0043] S207、终端通过动态主机配置协议(Dynamic Host Configuration Protocol, DHCP) 向 NAD 发送第一获取 IP 地址请求。

[0044] 本发明实施例中, NAD 可以预先设定终端的 IP 地址与终端访问权限的对应关系,从而在终端处于不同接入状态时,从地址池中的不同地址段为终端分配 IP 地址。

[0045] 本实施例中, NAD 可以预先设定地址池中第一地址段的 IP 地址与“用户组最小授权权限”相对应,当终端处于“认证和身份识别通过”接入状态时,NAD 从第一地址段中为终端分配 IP 地址;NAD 可以预先设定地址池中第二地址段的 IP 地址与“用户组权限”相对应,当终端处于“状态检查通过”接入状态时,NAD 从第二地址段中为终端分配 IP 地址;NAD 可以预先设定地址池中的第三地址段的 IP 地址与“用户组隔离受限权限”相对应,当终端处于“状态检测异常”接入状态时,NAD 从第三地址段中为终端分配 IP 地址。

[0046] S208、NAD 根据终端所处的“认证和身份识别通过”接入状态,从地址池中的第一地

址段中为终端分配 IP 地址。

[0047] 需要说明的是,终端处于“认证和身份识别通过”接入状态后,NAD 为终端分配的 IP 地址通常为临时地址。

[0048] 二、终端接入网络过程中的终端状态检查流程,参见图 3b:

[0049] S209、终端获取到临时地址后,状态检查服务器对终端进行状态检查,如果状态检查通过,则执行 S210,否则执行 S212。

[0050] 其中,状态检查服务器对终端进行状态检查的过程为:状态检查服务器触发终端上的客户端代理软件对终端进行扫描,具体可以是扫描终端上是否安装特定类型的软件,例如:杀毒软件等,扫描终端的病毒库是否更新等等。NAD 可以按照局域网内实际需求设定终端状态检查通过或不通过。例如:可以设定终端病毒库没有更新,则终端状态检查不通过;或者,还可以设定终端没有安装特定类型的软件,则终端状态检查不通过等,在此不一一列举。

[0051] 客户端代理软件完成对终端的扫描后,将扫描结果发送给状态检查服务器。

[0052] S210、状态检查服务器通过动态授权修改协议(例如:RADISU CoA 报文)向 NAD 发送终端状态检查通过通知消息,NAD 将记录的终端的接入状态修改为“状态检查通过”。

[0053] S211、NAD 从地址池中的第二地址段中为终端分配 IP 地址。

[0054] 其中,S208 中,NAD 为终端分配的 IP 地址通常为临时地址,而临时地址一般仅用于与状态服务器进行交互,检查终端的接入状态,因此,临时地址的地址租期时间通常可以设置为一个较小的值(例如:1 分钟),当终端状态检查通过后,NAD 接收到状态检查服务器通过 RADIUS CoA 报文或者扩展的 RADIUS 属性等消息发出的终端状态检查通过通知消息后,如果 NAD 接收到终端发送 DHCP 续租报文消息,则 NAD 可以向终端返回 DHCP 否定响应(Negative Acknowledge;NAK)报文,以触发终端发起第二获取 IP 地址请求,从而 NAD 可以从地址池中的第二地址段为终端分配 IP 地址,该 IP 地址通常为正常的 IP 地址。

[0055] S212、如果状态检查过程中检查到终端违规,则 NAD 不会改变终端的 IP 地址,状态修复服务器对终端进行修复。

[0056] 具体的,可以由终端的客户端代理软件与状态修复服务器进行交互,由状态修复服务器指导终端完成状态修复流程。

[0057] S213、终端修复完成后,状态修复服务器通知状态检查服务器对终端进行状态检查,如果状态检查通过,则状态检查服务器向 NAD 发送终端状态检查通过通知消息,NAD 从地址池中的第二地址段中为终端分配 IP 地址。

[0058] S213 中 NAD 从地址池中的第二地址段中为终端分配 IP 地址的过程可参见 S211 中的相关描述。

[0059] 三、终端接入网络后的流程,参见图 3c:

[0060] S214、在终端状态检查通过并获取正常地址后,终端可正常使用所属用户组内的网络资源,状态检查服务器定期对终端进行状态检测,当状态检查服务器发现终端状态异常时,判断该异常状态是否威胁网络安全,如果异常状态不会威胁网络,则执行 S215,如果异常状态会威胁网络,则执行 S216。

[0061] 其中,状态检查服务器可以与终端的客户端代理软件定期交互,定期对终端进行状态检测。

[0062] S215、通过状态修复服务器对终端进行修复。

[0063] S216、状态检查服务器通过动态授权协议（例如：RADIUS CoA(Change of Authorization Messages) 报文）向 NAD 发送终端隔离通知消息，NAD 记录终端状态的改变。

[0064] 当终端状态异常且会威胁网络，则需要对终端进行隔离，禁止终端接入网络，以保证其他终端的安全。

[0065] 其中，S217 为对终端进行隔离的一种可行的实施方式，S218-S219 为对终端进行隔离的另一种可行的实施方式。

[0066] S217、状态检查服务器可以通过 RADIUS CoA 协议等方式向 NAD 下发终端的访问控制列表 ACL，以使 NAD 在接收终端发送的第二访问请求时，第二访问请求中携带第二源 IP 地址和第二目的 IP 地址，NAD 能够根据终端的 ACL 确定是否允许终端访问第二目的 IP 地址。

[0067] S218、NAD 向终端发送扩展协议 EAP 消息，以触发终端发起第一释放 IP 地址请求及发起第三获取 IP 地址请求。

[0068] S218 中，终端请求释放的 IP 地址，为 NAD 在地址池中第二地址段为终端分配的 IP 地址。

[0069] S219、NAD 根据终端发起的第三获取 IP 地址请求，从地址池中的第三地址段中为终端分配 IP 地址。

[0070] 由于状态检查通过后，NAD 从地址池的第二地址段为终端分配的 IP 地址为正常的 IP 地址，租期较长，当状态检查服务器检测到终端异常后，可以通过扩展协议通知 NAD 设备（例如：可以通过 RADIUS CoA 报文中扩展的 RADIUS 属性通知 NAD 设备），NAD 记录终端状态为状态异常。NAD 可以通过扩展协议通知终端的客户端代理软件发送 DHCP 第一释放 IP 地址请求，并发起第三获取 IP 地址请求，NAD 可以根据终端处于“状态检测异常”接入状态，从地址池中的第三地址段中为终端分配 IP 地址，该 IP 地址为隔离地址。

[0071] S220、状态修复服务器对终端进行状态修复。

[0072] 具体的，客户端代理软件可以与状态修复服务器建立连接，完成终端修复流程。

[0073] S221、当终端状态修复后，状态修复服务器可以指示状态检查服务器向 NAD 发送终端状态修复完成通知。

[0074] S222、NAD 从地址池中的第二地址段中为终端分配 IP 地址。

[0075] 在终端状态修复完成后，由状态检查服务器通过动态授权协议（例如：为 RADIUS CoA 协议）通知 NAD 设备终端状态修复完成，NAD 可以向终端发送 EAP 扩展协议消息，以触发终端发起第二释放 IP 地址请求，并发起第四获取 IP 地址请求，具体的，NAD 可以在 EAP 请求 (Request) 消息的数据 (data) 中的名称 (name) 后面的 NULL 字符 (0 字符) 后面扩展一个自定义的字段，指示终端代理软件重新发起 DHCP 申请过程。NAD 根据终端发起的第四获取 IP 地址请求，从地址池中的第二地址段中为终端分配 IP 地址，该 IP 地址为正常 IP 地址。

[0076] 本实施例提供的访问权限控制方法，NAD 根据终端的不同接入状态从不同地址段中为终端分配 IP 地址，使 NAD 接收到终端的访问请求时，能够根据预先设定的终端的 IP 地址与终端访问权限的对应关系，控制终端的访问权限，实现节约 NAD 的存储资源，确保 NAD 对终端的访问进行控制。本发明无需改变现有局域网的网络架构，并且无需对新增网络设

备和对现有网络设备进行升级。

[0077] 需要说明的是：对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。

[0078] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述的部分，可以参见其他实施例的相关描述。

[0079] 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。

[0080] 图4为本发明提供的网络接入设备一个实施例的结构示意图，如图4所示，该网络接入设备包括：接收器11和处理器12；

[0081] 接收器11，用于接收终端发送的第一访问请求，该第一访问请求中携带第一源互联网协议IP地址和第一目的IP地址，所述第一源IP地址为所述终端的IP地址，所述终端的IP地址是由网络接入设备根据所述终端所处的不同接入状态从不同地址段中为所述终端分配的；

[0082] 处理器12，用于根据预先设定的终端的IP地址与终端访问权限的对应关系，确定是否允许终端访问第一目的IP地址。

[0083] 图5为在图4基础上扩展的网络接入设备又一个实施例的结构示意图，如图5所示，该网络接入设备包括：接收器11和处理器12；

[0084] 其中，处理器12根据预先设定的终端的IP地址与终端访问权限的对应关系，确定是否允许终端访问第一目的IP地址中，预先设定的终端的IP地址与终端访问权限的对应关系可以包括：

[0085] 终端的IP地址为任意地址，则对应的终端访问权限为公共权限；

[0086] 终端的IP地址位于地址池中的第一地址段，则对应的终端访问权限为用户组最小授权权限；

[0087] 终端的IP地址位于地址池中的第二地址段，则对应的终端访问权限为用户组权限；

[0088] 终端的IP地址位于地址池中的第三地址段，则对应的终端访问权限为用户组隔离受限权限。

[0089] 本实施例提供的接收器11，还可以进一步用于：接收终端发送的第一获取IP地址请求、状态检查服务器发送的终端状态检查通过通知消息、状态检查服务器发送的终端隔离通知消息和状态检查服务器发送的终端状态修复完成通知中的一个或多个；

[0090] 相应的，若接收器11在终端认证和身份识别通过后接收到终端发送的第一获取IP地址请求，则处理器12还可以用于：从地址池中的第一地址段中为终端分配IP地址。此时，终端处于“认证和身份识别通过后”的接入状态时，处理器12为终端分配的IP地址通常为临时地址，临时地址的租期较短。

[0091] 或者，若接收器11接收到状态检查服务器发送的终端状态检查通过通知消息，则处理器12从地址池中的第二地址段中为终端分配IP地址。在终端处于“状态检查通过”的

接入状态时,处理器 12 为终端分配的 IP 地址为正常地址。

[0092] 或者,若接收器 11 接收到状态检查服务器发送的终端隔离通知消息,则处理器 12 从地址池中的第三地址段中为终端分配 IP 地址。在终端处于“状态检查异常”接入状态时,处理器 12 为终端分配的 IP 地址为隔离地址。

[0093] 或者,若接收器 11 接收到状态检查服务器发送的终端状态修复完成通知,则处理器 12 从地址池中的第二地址段中为终端分配 IP 地址。

[0094] 本实施例提供的网络接入设备,还可以进一步包括:

[0095] 第一发送器 13,用于在接收器 11 接收到状态检查服务器发送的终端状态检查通过通知消息后,接收到终端发送的续租报文消息,该续租报文消息用于请求续租临时地址,则向终端发送动态主机配置协议否定响应 DHCP NAK 报文,以触发终端发起第二获取 IP 地址请求。其中,接收器 11 接收到的终端发送的续租报文消息为临时地址续租请求,第一发送器 13 向终端发送 DHCP NAK 报文,以拒绝终端的临时地址续租请求,并触发终端发起第二获取 IP 地址请求。

[0096] 相应的,处理器 12 还可以用于:根据终端发起的第二获取 IP 地址请求,从地址池中的第二地址段中为终端分配正常地址。

[0097] 本实施例提供的网络接入设备,还可以包括:

[0098] 第二发送器 14,用于若接收器 11 接收到状态检查服务器发送的终端隔离通知消息,则向终端发送扩展协议 EAP 消息,以触发终端发起第一释放 IP 地址请求及发起第三获取 IP 地址请求,该第一释放 IP 地址请求用于请求释放所述正常地址。

[0099] 相应的,处理器 12 还可以用于:根据终端发起的第三获取 IP 地址请求,从地址池中的第三地址段中为终端分配隔离地址。

[0100] 本实施例提供的网络接入设备,还可以包括:

[0101] 第三发送器 15,用于若接收器 11 接收到状态检查服务器发送的终端状态修复完成通知,则向终端发送扩展协议 EAP 消息,以触发终端发起第二释放 IP 地址请求及发起第四获取 IP 地址请求。其中,终端发起的第二释放 IP 地址的请求用于请求释放隔离地址。

[0102] 相应的,处理器 12 还可以用于:根据终端发起的第四获取 IP 地址请求,从地址池中的第二地址段中为终端分配正常地址。

[0103] 进一步的,接收器 11 还可以用于:接收状态检查服务器下发的终端的访问控制列表 ACL;

[0104] 在接收器 11 接收到状态检查服务器下发的终端的 ACL 后,如果接收到终端发送的第二访问请求,该第二访问请求中携带第二源 IP 地址和第二目的 IP 地址,则处理器 12 还可以用于:根据终端的 ACL,确定是否允许终端访问第二目的 IP 地址。

[0105] 本实施例提供的网络接入设备,与本发明实施例提供的访问权限控制方法相对应,网络接入设备为实现访问权限控制方法的执行设备,网络接入设备执行访问权限控制的具体过程可参见本发明提供的方法实施例,在此不再赘述。

[0106] 本发明实施例通过网络接入设备, NAD 根据终端的不同接入状态从不同地址段中为终端分配 IP 地址,使 NAD 接收到终端的访问请求时,能够根据预先设定的终端的 IP 地址与终端访问权限的对应关系,控制终端的访问权限,实现节约 NAD 的存储资源,确保 NAD 对终端的访问进行控制。

[0107] 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。

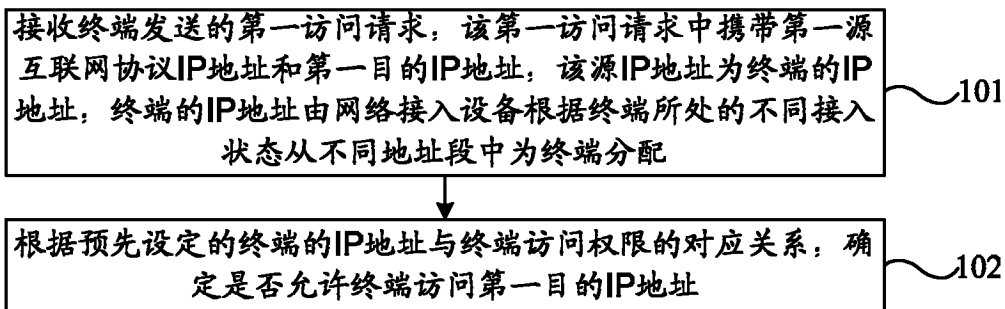


图 1

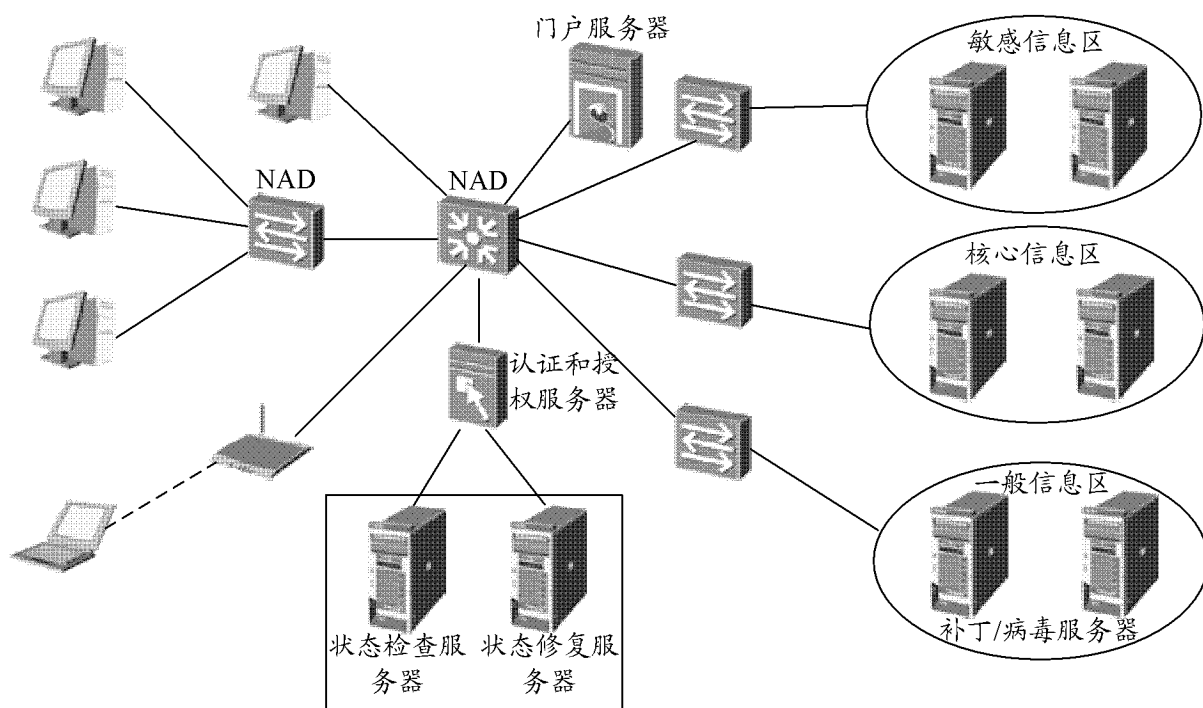


图 2

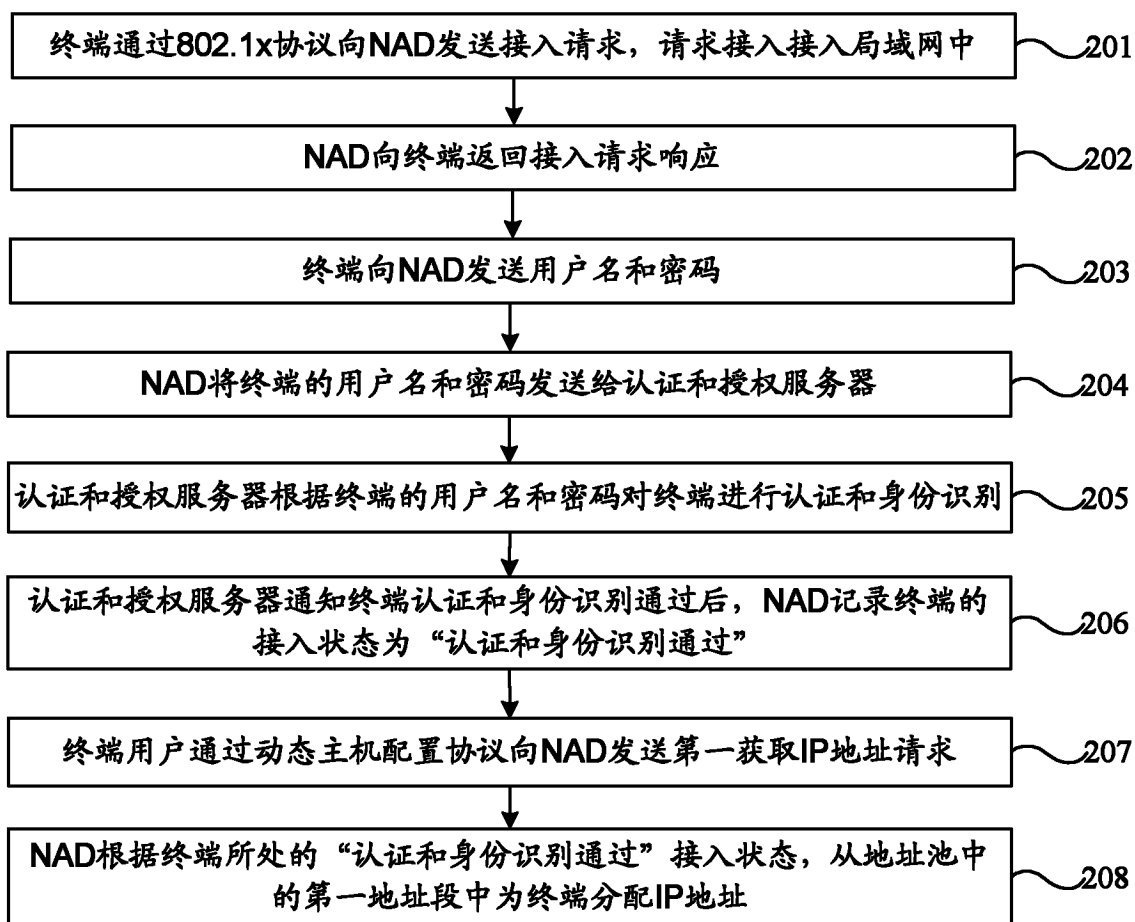


图 3a

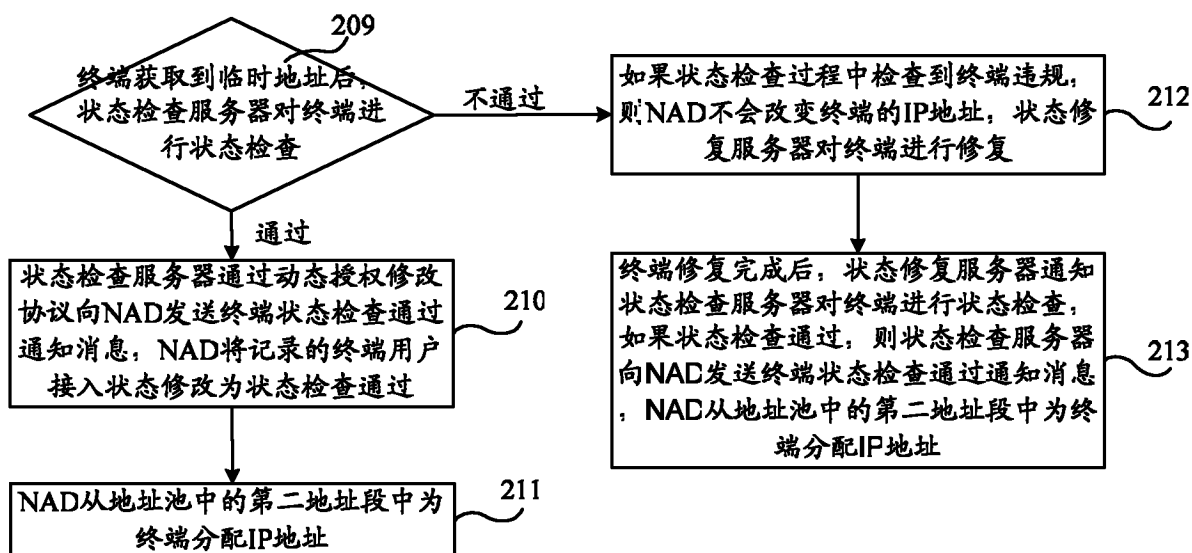


图 3b

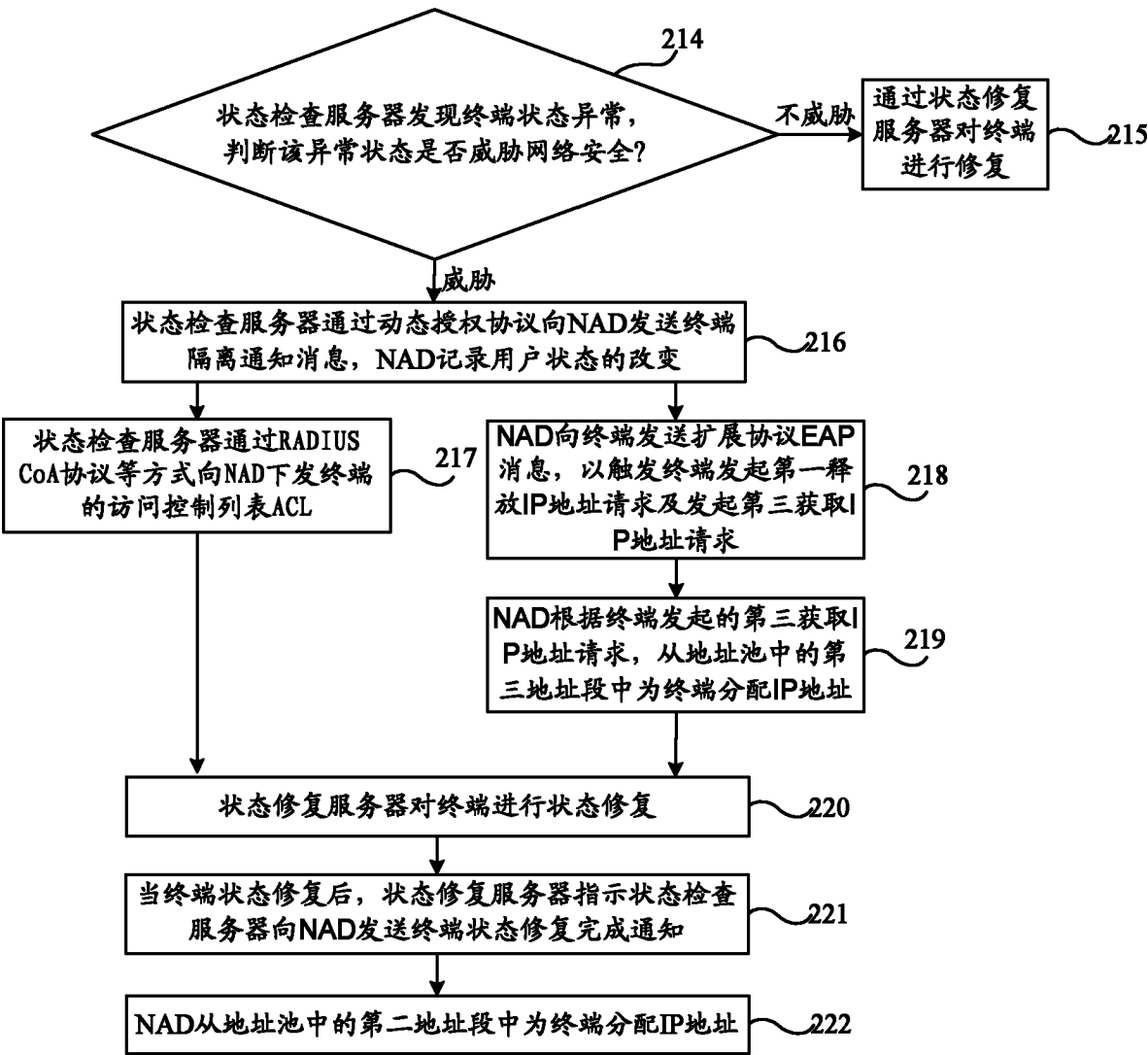


图 3c

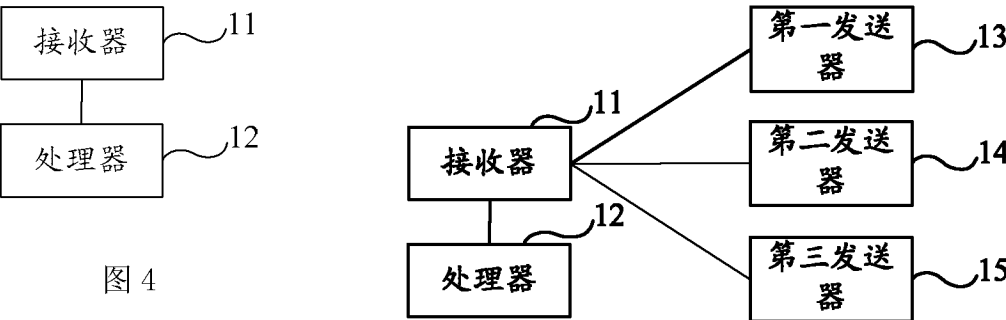


图 4

图 5