(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 108881103 A
(43)申请公布日 2018.11.23

(21)申请号 201710318017.5

(22)申请日 2017.05.08

(71)申请人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 杨哲 蒙俊伸 张华彦 邓颖

(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
代理人 王仲凯

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

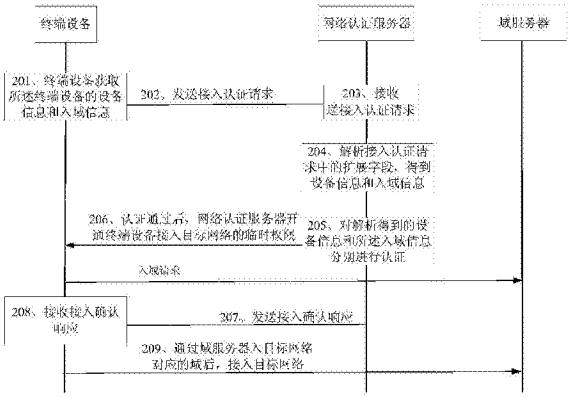
权利要求书2页 说明书12页 附图5页

(54)发明名称

一种接入网络的方法及装置

(57)摘要

一种接入网络的方法及设备，所述方法包括：接收终端设备发送的接入认证请求，接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或终端设备动态生成的标签，所述标签或所述专有协议数据包括终端设备的设备信息和入域信息；解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；对解析得到的所述设备信息和所述入域信息分别进行认证；认证通过后，开通终端设备接入目标网络的临时权限，临时权限是指授权所述终端设备在预设时间内使用所述目标网络；向终端设备发送接入确认响应，以使终端设备通过域服务器进行入所述目标网络对应的域的操作。通过采用本方案，能够提高网络管理效率和降低网络管理成本。



CN 108881103 A

1.一种接入网络的方法，其特征在于，所述方法包括：

接收终端设备发送的接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；

对解析得到的所述设备信息和所述入域信息分别进行认证；

认证通过后，开通所述终端设备接入目标网络的临时权限，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

向所述终端设备发送接入确认响应，以使所述终端设备通过域服务器进行入所述目标网络对应的域的操作。

2.根据权利要求1所述的方法，其特征在于，所述开通所述终端设备接入目标网络的临时权限，包括：

将所述终端设备加入临时白名单。

3.根据权利要求2所述的方法，其特征在于，在所述开通所述终端设备接入所述目标网络的临时权限之后，所述方法还包括：

在所述终端设备成功接入所述目标网络后，将所述终端设备从所述临时白名单中移除。

4.根据权利要求2或3所述的方法，其特征在于，所述解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息，包括：

根据专有协议对所述专有协议数据进行解析，得到所述设备信息和所述入域信息。

5.根据权利要求2或3所述的方法，其特征在于，所述解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息，包括：

调用标签解析工具对所述标签进行解析，得到所述设备信息和所述入域信息。

6.一种接入网络的方法，其特征在于，所述方法包括：

向网络认证服务器发送接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

接收所述网络认证服务器发送的接入确认响应，所述接入确认响应由所述网络认证服务器在解析所述扩展字段，对解析得到的所述设备信息和所述入域信息进行认证通过，开通所述终端设备接入目标网络的临时权限后发送的响应，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

通过域服务器入所述目标网络对应的域后，接入所述目标网络。

7.根据权利要求6所述的方法，其特征在于，在所述接入所述目标网络后，所述方法还包括：

将接入所述目标网络的认证方式设置为终端设备域身份认证，所述终端设备域身份认证是指通过域服务器对所述终端设备的设备信息进行认证。

8.根据权利要求7所述的方法，其特征在于，所述通过域服务器入所述目标网络对应的域，包括：

通过程序调用接口向所述域服务器发送携带所述入域信息的入域请求；

接收入域确认响应，所述入域确认响应是所述域服务器对所述入域信息认证通过后发送的响应。

9.根据权利要求7所述的方法，其特征在于，在向网络认证服务器发送接入认证请求之前，所述方法还包括：

获取输入的身份信息；

对所述身份信息进行动态口令认证，若认证通过，则向所述网络认证服务器发送所述接入认证请求。

10.根据权利要求6-9任一所述的方法，其特征在于，在向网络认证服务器发送接入认证请求之前，所述方法还包括：

获取所述设备信息和所述入域信息；

调用标签生成工具，根据所述设备信息和所述入域信息动态生成所述标签。

11.一种网络认证服务器，其特征在于，所述网络认证服务器包括：

接收模块，用于接收终端设备发送的接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

处理模块，用于解析所述接收模块接收到的所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；

对解析得到的所述设备信息和所述入域信息分别进行认证；

认证通过后，开通所述终端设备接入目标网络的临时权限，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

发送模块，用于向所述终端设备发送接入确认响应，以使所述终端设备通过域服务器进行入所述目标网络对应的域的操作。

12.一种终端设备，其特征在于，所述终端设备包括：

发送模块，用于向网络认证服务器发送接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

接收模块，接收所述网络认证服务器发送的接入确认响应，所述接入确认响应由所述网络认证服务器在解析所述扩展字段，对解析得到的所述设备信息和所述入域信息进行认证通过，开通所述终端设备接入目标网络的临时权限后发送的响应，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

处理模块，用于通过域服务器入所述目标网络对应的域后，接入所述目标网络。

13.根据权利要求12所述的终端设备，其特征在于，所述处理模块在所述终端设备接入所述目标网络后，还用于：

将接入所述目标网络的认证方式设置为终端设备域身份认证，所述终端设备域身份认证是指通过域服务器对所述终端设备的设备信息进行认证。

14.一种计算机存储介质，其特征在于，其包括指令，当其在计算机上运行时，使得计算机执行如权利要求1-5任一所述的方法，或者执行如权利要求6-10任一所述的方法。

15.一种包含指令的计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求1-5任一所述的方法，或者执行上述权利要求6-10任一所述的方法。

一种接入网络的方法及装置

技术领域

[0001] 本申请涉及互联网技术领域，尤其涉及一种接入网络的方法及装置。

背景技术

[0002] 在企业里，为了保证网络的安全性，所有要接入该企业的网络的终端设备都需要先入域后，再进行标准化，然后才被允许接入网络，未入域的终端设备无法接入该企业的网络。考虑到会有新的终端设备想要访问企业的网络，但其在没有网络的情况下，该终端设备无法进行入域和标准化操作，这样该终端设备便无法访问该网络。目前，一般由网络维护人员在特殊的网络环境下提前为该终端设备进行入域操作，使该终端设备能够接入该企业的网络。考虑到待入域的终端设备的数量庞大或者会不断增加，由网络维护人员分别去为每台终端设备提供入域操作的话，所需时长较多，且效率低下。

[0003] 现有机制中，为提高入域和标准化效率，采取提供证书的方式，使得终端设备在入域时，通过导入该证书的方式来临时连接企业的网络，然后通过临时连接的网络向该网络的网络认证服务器自行入域。如果证书泄漏，则会导致非法终端设备接入企业的网络，这样会给企业带来一定的安全风险。

发明内容

[0004] 本申请提供了一种接入网络的方法及装置，能够解决现有技术中无法在不影响企业安全性的前提下，提高终端设备接入企业的网络的效率的问题。

[0005] 本申请第一方面提供一种接入网络的方法，所述方法包括：

[0006] 接收终端设备发送的接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0007] 解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；

[0008] 对解析得到的所述设备信息和所述入域信息分别进行认证；

[0009] 认证通过后，开通所述终端设备接入目标网络的临时权限，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

[0010] 向所述终端设备发送接入确认响应，以使所述终端设备通过域服务器进行入所述目标网络对应的域的操作。

[0011] 本申请第二方面提供一种接入网络的方法，所述方法包括：

[0012] 向网络认证服务器发送接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0013] 接收所述网络认证服务器发送的接入确认响应，所述接入确认响应由所述网络认证服务器在解析所述扩展字段，对解析得到的所述设备信息和所述入域信息进行认证通过，开通所述终端设备接入目标网络的临时权限后发送的响应，所述临时权限是指授权所

述终端设备在预设时间内使用所述目标网络；

[0014] 通过域服务器入所述目标网络对应的域后，接入所述目标网络。

[0015] 本申请第三方面提供一种网络认证服务器，具有实现对应于上述第一方面提供的接入网络的方法的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块，所述模块可以是软件和/或硬件。一种可能的设计中，所述网络认证服务器包括：

[0016] 接收模块，用于接收终端设备发送的接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0017] 处理模块，用于解析所述接收模块接收到的所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；

[0018] 对解析得到的所述设备信息和所述入域信息分别进行认证；

[0019] 认证通过后，开通所述终端设备接入目标网络的临时权限，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

[0020] 发送模块，用于向所述终端设备发送接入确认响应，以使所述终端设备通过域服务器进行入所述目标网络对应的域的操作。

[0021] 本申请第四方面提供一种终端设备，具有实现对应于上述第二方面提供的接入网络的方法的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块，所述模块可以是软件和/或硬件。一种可能的设计中，所述终端设备包括：

[0022] 发送模块，用于向网络认证服务器发送接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0023] 接收模块，接收所述网络认证服务器发送的接入确认响应，所述接入确认响应由所述网络认证服务器在解析所述扩展字段，对解析得到的所述设备信息和所述入域信息进行认证通过，开通所述终端设备接入目标网络的临时权限后发送的响应，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

[0024] 处理模块，用于通过域服务器入所述目标网络对应的域后，接入所述目标网络。

[0025] 相较于现有技术，本申请提供的方案中，接收终端设备发送的携带扩展字段的接入认证请求，其中扩展字段包括专有协议数据或终端设备动态生成的标签，该标签或专有协议数据包括所述终端设备的设备信息和入域信息，然后解析所述扩展字段，对解析得到的所述设备信息和所述入域信息分别进行认证，由于在接入认证请求中加入了专有协议数据或上述标签，可以防止非法用户通过其他协议客户端进行接入认证，从而可以提高接入网络的安全性。在认证通过后，开通所述终端设备接入目标网络的临时权限，这样使得终端设备在后续入域流程中，能够通过临时网络权限去完成入域操作，最后终端设备可成功接入所述目标网络。可见，整个接入网的认证流程都可由合法用户自助完成，相较于现有机制，明显提高网络管理效率和降低网络管理成本。

附图说明

[0026] 图1为本申请中通信系统的一种网络拓扑示意图；

[0027] 图2为本申请中接入网络的方法的一种信令流程示意图；

[0028] 图3为本申请中临时白名单的一种示意图；

[0029] 图4为本申请中终端设备切换接入网络认证方式的一种示意图；

[0030] 图5为本申请中接入网络的方法的另一种信令流程示意图；

[0031] 图6为本申请中网络认证服务器的一种结构示意图；

[0032] 图7为本申请中终端设备的一种结构示意图；

[0033] 图8为本申请中网络认证服务器的另一种结构示意图；

[0034] 图9为本申请中终端设备的另一种结构示意图。

具体实施方式

[0035] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或模块的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或模块，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或模块，本申请中所出现的模块的划分，仅仅是一种逻辑上的划分，实际应用中实现时可以有另外的划分方式，例如多个模块可以结合成或集成在另一个系统中，或一些特征可以忽略，或不执行，另外，所显示的或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，模块之间的间接耦合或通信连接可以是电性或其他类似的形式，本申请中均不作限定。并且，作为分离部件说明的模块可以是也可以不是物理上的分离，可以是也可以不是物理模块，或者可以分布到多个电路模块中，可以根据实际的需要选择其中的部分或全部模块来实现本发明实施例方案的目的。

[0036] 本申请提供了一种接入网络的方法及设备，能够提高网络管理效率和降低网络管理成本，以及提高接入网络的安全性。

[0037] 图1为一种通信系统的网络拓扑结构示意图，图1所示的通信系统包括网络认证服务器、域服务器和至少一个终端设备，网络认证服务器和域服务器在同一网络中，这些终端设备为待接入网络的终端设备。在企业的网络之外，终端设备安装了交互式应用(也可称之为客户端)，该客户端可以是基于802.1X协议扩展的专用客户端，也可以是基于现有机制的802.1X协议的客户端。终端设备可通过其安装的客户端向网络认证服务器请求接入认证，然后在网络认证服务器对该终端设备认证通过后，开通该终端设备使用网络的临时权限。终端设备在获取使用网络的临时权限后，就可以向域服务器请求入域，最后由域服务器对该终端设备发起的入域请求进行认证，若通过认证，则将该终端设备加入网络。

[0038] 其中，需要特别说明的是，本发明实施例涉及的终端设备，可以是指向用户提供语音和/或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。无线终端可以经无线接入网(英文全称:Radio Access Network，英文简称:RAN)与一个或多个核心网进行通信，无线终端可以是移动终端，如移动电话(或称为“蜂窝”电话)和具有移动终端的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者

车载的移动装置，它们与无线接入网交换语音和/或数据。例如，个人通信业务(英文全称：Personal Communication Service，英文简称：PCS)电话、无绳电话、会话发起协议(SIP)话机、无线本地环路(Wireless Local Loop，英文简称：WLL)站、个人数字助理(英文全称：Personal Digital Assistant，英文简称：PDA)等设备。无线终端也可以称为系统、订户单元(Subscriber Unit)、订户站(Subscriber Station)，移动站(Mobile Station)、移动台(Mobile)、远程站(Remote Station)、接入点(Access Point)、远程终端(Remote Terminal)、接入终端(Access Terminal)、用户终端(User Terminal)、终端设备、用户代理(User Agent)、用户设备(User Device)、或用户装备(User Equipment)。

[0039] 为解决上述技术问题，本发明实施例主要提供以下技术方案：

[0040] 本申请基于现有机制中的802.1X协议进行扩展，即终端设备在向网络认证服务器发送接入认证请求之前，先采用专用协议的方式将设备信息和入域信息进行封装(用专用协议进行序列化)，再将封装后的设备信息和入域信息加入802.1X协议的扩展字段中；或者采用生成动态标签的方式(例如采用标签生成工具)将设备信息和入域信息生成标签，再将动态生成的标签加入802.1X协议的扩展字段中。

[0041] 所以，在接入网络的认证流程中，进行认证的网络认证服务器就可以采用对应的方式(例如采用专用协议或标签读取工具)对扩展字段的数据进行解析，最终解析得到上述设备信息和入域信息，随后对设备信息和入域信息进行认证，若认证通过，则开通该终端设备接入网络的临时权限。由于非法用户不知道专用协议或者标签生成的方式，所以，即使获取了上述设备信息和入域信息，也不能通过其他802.1X协议客户端去向本网络的网络认证服务器申请接入认证，通过采用上述两种机制，可以有效提高接入网络的安全性，也能实现用户自助入网，提高入网效率。

[0042] 请参照图2，以下对本申请提供一种接入网络的方法进行举例说明，所述方法包括：

[0043] 201、终端设备获取所述终端设备的设备信息和入域信息。

[0044] 202、终端设备向网络认证服务器发送接入认证请求。

[0045] 其中，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息。

[0046] 入域信息可以为域帐号(英文全称：Active Directory，英文简称：AD)windows的域服务器，与域账号对应的密钥。其中AD可被设计为执行任务：包括创建、删除、修改、移动和设置存储在目录中的对象的权限，这些对象包括组织单位、用户、联系人、组、计算机、打印机和共享的文件对象。

[0047] 一些实施方式中，接入认证请求可基于802.1X协议，802.1X协议是指于Client/Server的访问控制和认证协议，其可以限制未经授权的终端设备通过接入端口访问局域网(英文全称：Local Area Networks，英文简称：LAN)/无线局域网(英文全称：Wireless Local Area Networks，英文简称：WLAN)。终端设备在获得交换机或LAN提供的各种业务之前，基于802.1X协议的网络认证服务器会对连接到交换机端口上的终端设备进行接入认证。在认证通过之前，802.1X协议只允许基于局域网的扩展认证协议(英文全称：Extensible Authentication Protocol，英文简称：EAPOL)的数据通过与上述终端设备连

接的交换机端口，认证通过以后，正常的数据就可以顺利地通过以太网端口。802.1X协议为基于端口的标准，用于对无线网络的接入认证，在接入认证时也采用远程用户拨号认证系统(英文全称:Remote Authentication Dial In User Service，英文简称:RADIUS)协议。

[0048] 若采用专有协议的方式，则终端设备可将设备信息和入域信息采用专有协议进行序列化，生成所述专有协议数据，然后将生成的所述专有协议数据加入扩展字段中。

[0049] 若采用标签的方式，则终端设备可调用标签生成工具，利用标签生成工具将设备信息和入域信息动态生成上述标签，然后将生成的标签加入扩展字段中。

[0050] 203、网络认证服务器接收终端设备发送的接入认证请求。

[0051] 204、网络认证服务器解析所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息。

[0052] 若采用专有协议的方式，则网络认证服务器在读取扩展字段后，根据专有协议对所述专有协议数据进行解析，最终得到所述设备信息和所述入域信息。

[0053] 若采用标签的方式，则网络认证服务器在读取扩展字段后，调用标签解析工具对所述标签进行解析，最终得到所述设备信息和所述入域信息。

[0054] 205、对解析得到的所述设备信息和所述入域信息分别进行认证。

[0055] 206、认证通过后，网络认证服务器开通所述终端设备接入目标网络的临时权限。

[0056] 其中，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络。一种实施方式中，可以通过将所述终端设备加入临时白名单来达到开通临时权限的目的。举例来说，如图3所示，临时白名单中有终端设备1、终端设备2、终端设备3、…终端设备n，表明终端设备1、终端设备2、终端设备3、…终端设备n都是正在进行网络接入认证的终端设备，它们都具备接入网络的临时权限。将例如，网络认证服务器对终端设备3认证通过后，将终端设备3加入图3中的临时白名单中，则表明该终端设备3具备接入网络的临时权限，那么该终端设备就可以使用该临时权限去向域服务器进行入域请求。

[0057] 207、网络认证服务器向所述终端设备发送接入确认响应。

[0058] 208、终端设备接收所述网络认证服务器发送的接入确认响应。

[0059] 209、终端设备通过域服务器入所述目标网络对应的域后，接入所述目标网络。

[0060] 具体来说，终端设备通过域服务器入所述目标网络对应的域的具体操作如下：

[0061] 终端设备可通过程序调用接口向所述域服务器发送携带所述入域信息的入域请求，然后域服务器则对该入域请求中的入域信息进行认证，若认证通过，则将入域确认响应返回给该终端设备，该终端设备接收到该域服务器发送的入域确认响应后，即可进行接入所述目标网络的操作。

[0062] 与现有机制相比，本申请中，网络认证服务器接收终端设备发送的携带扩展字段的接入认证请求，由于扩展字段包括专有协议数据或终端设备动态生成的标签，该标签或专有协议数据包括所述终端设备的设备信息和入域信息。网络认证服务器可通过解析所述扩展字段得到所述设备信息和所述入域信息分别进行认证。可见，由于在接入认证请求中加入了专有协议数据或上述标签，可以防止非法用户通过其他协议客户端进行接入认证，从而可以提高接入网络的安全性。在认证通过后，开通所述终端设备接入目标网络的临时权限，这样使得终端设备在后续入域流程中，能够通过临时网络权限去完成入域操作，最后终端设备可成功接入所述目标网络。可见，整个接入网的认证流程都可由合法用户自助完

成，相较于现有机制，明显提高网络管理效率和降低网络管理成本，也可以减少通过导入证书所带来的安全风险问题。

[0063] 可选的，在一些发明实施例中，由于临时白名单里的终端设备都是没有被标记为正式合法入域的终端设备，如果不从临时白名单中移除该终端设备，那么下次该终端设备接入网络时，网络认证服务器则会依旧认为该终端设备不合法，依然需要再一次进行上述步骤201-步骤209的接入认证流程，这样会造成触发多次不必要的接入认证流程，并且针对同一个终端设备进行频繁的接入认证操作也使得网络认证服务器认为该终端设备操作不正常，将该终端设备标识为非法终端设备，这样会拦截该合法入域的终端设备最终无法接入上述目标网络。所以，在所述开通所述终端设备接入所述目标网络的临时权限之后，网络认证服务器在所述终端设备成功接入所述目标网络后，还可将所述终端设备从所述临时白名单中移除。另外一个好处就是，将所述终端设备从所述临时白名单中移除后，就表示该终端设备为合法用户，那么该终端设备在后期接入上述目标网络时就不需要再次进行接入认证流程了。

[0064] 由此可见，回收白名单的目的是因为以后该终端设备要再次接入该目标网络时，终端设备可直接接入网络。并且，由于终端设备还可直接通过机器域身份认证的方式进行认证，所以就更不需要通过网络认证服务器对该终端设备进行接入认证了，所以用于临时打通网络的临时白名单也不需要。

[0065] 可选的，在一些发明实施例中，在所述接入所述目标网络后，所述终端设备还可在专用客户端上将接入所述目标网络的认证方式设置为终端设备域身份认证，所述终端设备域身份认证是指通过域服务器对所述终端设备的设备信息进行认证。通过改变认证方式，可使得该终端设备通过专用客户端入域成功后，若退域后再次入域时，就不需要重复执行前述步骤201-步骤209中的接入认证流程。

[0066] 其中，本申请中的终端设备域身份认证的方式是指：只对该终端设备的媒体访问控制(英文全称：Medium Access Control，英文简称：MAC)地址进行认证。因为该终端设备在上次入域成功后，作为网络管理后台的域服务器已经注册了该终端设备的硬件信息，当该终端设备再次接入上述目标网络时，域服务器可直接获取该终端设备的硬件信息和MAC地址等，再判断该终端设备是否注册过即可，若已经在先注册过，则该终端设备可接入上述目标网络，从而使用该目标网络所提供的各种业务。

[0067] 举例来说，如图4所示，用户在终端设备上安装的专用客户端上打开设置界面，进入“接入网络认证方式选择”的界面，其中，“网络认证方式”对应的“设置为主要接入网络认证方式”图标为阴影部分，则表示当前的接入网络认证方式是网络认证方式，用户可选择“终端设备域身份认证”所对应的“设置为主要接入网络认证方式”的图标，选择后，就完成了“接入网络认证方式”的切换。

[0068] 可选的，在一些发明实施例中，考虑到本申请所使用的专用客户端可能被非法用户窃取，为防止非法用户通过本申请的专用客户端非法接入上述目标网络，在向网络认证服务器发送接入认证请求之前，所述终端设备还可获取输入的身份信息，然后对输入的所述身份信息进行动态口令认证，若认证通过，则向所述网络认证服务器发送所述接入认证请求。通过采用这种动态认证的方式对启动上述专用客户端的身份信息进行动态认证，可以进一步加强通信系统的安全性，进而减少专用客户端泄漏所带来的安全隐患。

[0069] 一些实施方式中，对输入的身份信息进行动态口令认证的方式可以采用令牌(Token)认证的方式，Token也可以叫暗号，在传输数据之前，要先进行暗号的核对，不同的暗号被授权不同的数据操作。例如在USB1.1协议中定义了4类数据包：Token包、数据(Data)包、订单管理应用服务商(Handshake)包和特定(Special)包。主机和USB设备之间连续数据的交换可以分为三个阶段，第一个阶段由主机发送Token包，不同的Token包内容不一样(暗号不一样)可以告诉设备做不同的工作，第二个阶段发送Data包，第三个阶段由设备返回一个Handshake包。

[0070] 为便于理解，下面以一具体用用场景为例，图5中，终端设备安装了专用客户端，用户启动该专用客户端，通过该专用客户端向与该终端设备连接的交换机端口提交硬件信息、AD帐号和密钥，然后该交换机将收到的硬件信息、AD帐号和密钥转发给RADIUS认证，当RADIUS对硬件信息、AD帐号和密钥认证通过后，则通过原交换机返回认证结果至该终端设备。

[0071] 用户通过该专用客户端通过程序调用接口，将携带认证通过的AD帐号的入域请求发送给AD，AD对接收到的该AD帐号进行认证，认证通过后，AD则将入域确认响应返回给该终端设备。该终端设备接收到AD返回的入域确认响应后，就可以接入网络。

[0072] 以上对本申请中一种接入网络的方法进行说明，以下对执行上述接入网络的方法的网络认证服务器和终端设备分别进行描述。本申请中的网络认证服务器可以是网络策略服务器(英文全称：Network Policy Server，英文简称：NPS)，NPS可以把某一组成员通过服务器上网，可以为客户端运行状况、连接请求身份验证、以及连接请求的授权和创建，并强制使用组织范围的网络访问策略。一些实施方式中，可以在NPS中安装RADIUS客户端，从而将NPS用作RADIUS服务器代理，以便将连接请求转发到在远程RADIUS服务器组中配置的运行NPS的服务器或其他RADIUS服务器。

[0073] 其中，RADIUS服务器上可存储终端设备的身份信息、授权信息以及访问记录，对终端设备进行认证、授权和计费服务。RADIUS服务器可以将无线访问点和VPN服务器等网络访问服务器配置为NPS中的RADIUS客户端。还可以配置NPS用于对连接请求进行授权的网络策略，并且可以配置RADIUS记帐，以便NPS将记帐信息记录到本地硬盘上或数据库中的日志文件。

[0074] 一、参照图6，对网络认证服务器60进行说明，所述网络认证服务器60包括：

[0075] 接收模块601，用于接收终端设备发送的接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0076] 处理模块602，用于解析所述接收模块601接收到的所述接入认证请求中的所述扩展字段，得到所述设备信息和所述入域信息；

[0077] 对解析得到的所述设备信息和所述入域信息分别进行认证；

[0078] 认证通过后，开通所述终端设备接入目标网络的临时权限，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

[0079] 发送模块603，用于向所述终端设备发送接入确认响应，以使所述终端设备通过域服务器进行入所述目标网络对应的域的操作。

[0080] 与现有机制相比，本申请中，由接收模块601接收终端设备发送的携带扩展字段的

接入认证请求，由于扩展字段包括专有协议数据或终端设备动态生成的标签，该标签或专有协议数据包括所述终端设备的设备信息和入域信息。处理模块602可通过解析所述扩展字段得到所述设备信息和所述入域信息分别进行认证。可见，由于在接入认证请求中加入了专有协议数据或上述标签，可以防止非法用户通过其他协议客户端进行接入认证，从而可以提高接入网络的安全性。在认证通过后，开通所述终端设备接入目标网络的临时权限，这样使得终端设备在后续入域流程中，能够通过临时网络权限去完成入域操作，最后终端设备可成功接入所述目标网络。可见，整个接入网的认证流程都可由合法用户自助完成，相较于现有机制，明显提高网络管理效率和降低网络管理成本。

[0081] 可选的，在一些发明实施例中，所述处理模块602具体用于：

[0082] 将所述终端设备加入临时白名单。

[0083] 可选的，在一些发明实施例中，所述处理模块在所述开通所述终端设备接入所述目标网络的临时权限之后，还用于：

[0084] 在所述终端设备成功接入所述目标网络后，将所述终端设备从所述临时白名单中移除。

[0085] 可选的，在一些发明实施例中，所述处理模块602具体用于：

[0086] 根据专有协议对所述专有协议数据进行解析，得到所述设备信息和所述入域信息。

[0087] 可选的，在一些发明实施例中，所述处理模块602具体用于：

[0088] 调用标签解析工具对所述标签进行解析，得到所述设备信息和所述入域信息。

[0089] 二、参照图7，对终端设备70进行说明，所述终端设备70包括：

[0090] 发送模块701，用于向网络认证服务器发送接入认证请求，所述接入认证请求携带扩展字段，所述扩展字段包括专有协议数据或所述终端设备动态生成的标签，所述标签或所述专有协议数据包括所述终端设备的设备信息和入域信息；

[0091] 接收模块702，用于接收所述网络认证服务器发送的接入确认响应，所述接入确认响应由所述网络认证服务器在解析所述扩展字段，对解析得到的所述设备信息和所述入域信息进行认证通过，开通所述终端设备接入目标网络的临时权限后发送的响应，所述临时权限是指授权所述终端设备在预设时间内使用所述目标网络；

[0092] 处理模块703，用于通过域服务器入所述目标网络对应的域后，接入所述目标网络。

[0093] 与现有机制相比，本申请中，接收模块701接收终端设备发送的携带扩展字段的接入认证请求，由于扩展字段包括专有协议数据或终端设备动态生成的标签，该标签或专有协议数据包括所述终端设备的设备信息和入域信息。网络认证服务器可通过解析所述扩展字段得到所述设备信息和所述入域信息分别进行认证。可见，由于处理模块703在接入认证请求中加入上述专有协议数据或上述标签，然后由发送模块702将接入认证请求发送给网络认证服务器，可以防止非法用户通过其他协议客户端进行接入认证，可以提高接入网络的安全性。所述终端设备在获取接入目标网络的临时权限后，在后续入域流程中即可直接通过临时网络权限去完成入域操作，最后终端设备可成功接入所述目标网络。可见，整个接入网的认证流程都可由合法用户自助完成，相较于现有机制，明显提高网络管理效率和降低网络管理成本。

[0094] 可选的，在一些发明实施例中，所述处理模块702在所述终端设备接入所述目标网络后，还用于：

[0095] 将接入所述目标网络的认证方式设置为终端设备域身份认证，所述终端设备域身份认证是指通过域服务器对所述终端设备的设备信息进行认证。

[0096] 可选的，在一些发明实施例中，所述处理模块702具体用于：

[0097] 通过程序调用接口向所述域服务器发送携带所述入域信息的入域请求；

[0098] 通过所述接收模块701接收入域确认响应，所述入域确认响应是所述域服务器对所述入域信息认证通过后发送的响应。

[0099] 可选的，在一些发明实施例中，所述处理模块702在向网络认证服务器发送接入认证请求之前，还用于：

[0100] 通过所述接收模块701获取输入的身份信息；

[0101] 对所述身份信息进行动态口令认证，若认证通过，则通过所述发送模块703向所述网络认证服务器发送所述接入认证请求。

[0102] 可选的，在一些发明实施例中，所述处理模块702在所述发送模块703向网络认证服务器发送接入认证请求之前，还用于：

[0103] 通过所述接收模块701获取所述设备信息和所述入域信息；

[0104] 调用标签生成工具，根据所述设备信息和所述入域信息动态生成所述标签。

[0105] 可选的，在一些发明实施例中，所述处理模块702在所述发送模块703向网络认证服务器发送接入认证请求之前，还用于：

[0106] 通过所述接收模块701获取所述设备信息和所述入域信息；

[0107] 根据专有协议，将所述设备信息和所述入域信息生成所述专有协议数据。

[0108] 上面从模块化功能实体的角度对本发明实施例中的网络认证服务器和终端设备进行了描述，下面从硬件处理的角度分别对本发明实施例中的网络认证服务器和终端设备进行描述。需要说明的是，在本发明图6所示的实施例中的发送模块对应的实体设备可以为发射器，获取模块对应的实体设备可以为输入/输出单元，处理模块对应的实体设备可以为处理器，显示模块所对应的实体设备可以是显示屏等显示单元。图6所示的装置可以具有如图8所示的结构，当图6所示的装置具有如图8所示的结构时，图8中的处理器、发射器和接收器能够实现前述对应该装置的装置实施例提供的处理模块、发送模块和接收模块相同或相似的功能，图8中的中央存储器存储处理器执行上述接入网络的方法时需要调用的程序代码。在本发明图6所示的实施例中的发送模块和接收模块所对应的实体设备可以为输入输出接口，处理模块对应的实体设备可以为处理器。图7所示的装置可以具有如图9所示的结构，当图7所示的装置具有如图9所示的结构时，图9中的处理器和RF电路能够实现前述对应该装置的装置实施例提供的处理模块、发送模块和接收模块相同或相似的功能，图9中的存储器存储处理器执行上述接入网络的方法时需要调用的程序代码。

[0109] 图8是本发明实施例提供的另一种网络认证服务器结构示意图，该网络认证服务器800可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上中央处理器(英文全称:Central Processing Units，英文简称:CPU)822(例如，一个或一个以上处理器)和存储器832，一个或一个以上存储应用程序842或数据844的存储介质830(例如一个或一个以上海量存储设备)。其中，存储器832和存储介质830可以是短暂存储或持久存储。存储在

存储介质830的程序可以包括一个或一个以上模块(图示没标出),每个模块可以包括对服务器中的一系列指令操作。更进一步地,中央处理器822可以设置为与存储介质830通信,在服务器800上执行存储介质830中的一系列指令操作。

[0110] 网络认证服务器800还可以包括一个或一个以上电源826,一个或一个以上有线或无线网络接口850,一个或一个以上输入输出接口858,和/或,一个或一个以上操作系统841,例如Windows ServerTM,Mac OS XTM,UnixTM,LinuxTM,FreeBSDTM等等。

[0111] 本发明实施例涉及的服务器可以具有比图8所示出的更多或更少的部件,可以组合两个或更多个部件,或者可以具有不同的部件配置或设置,各个部件可以在包括一个或多个信号处理和/或专用集成电路在内的硬件、软件或硬件和软件的组合实现。

[0112] 通过调用存储介质830中存储的指令,中央处理器822至少可可用于执行上述图6所对应的实施例中的所有操作。

[0113] 本发明实施例还提供了另一种终端设备,如图9所示,为了便于说明,仅示出了与本发明实施例相关的部分,具体技术细节未揭示的,请参照本发明实施例方法部分。下面以终端为手机为例:

[0114] 图9示出的是与本发明实施例提供的终端设备相关的手机的部分结构的框图。参考图9,手机包括:射频(英文全称:Radio Frequency,英文简称:RF)电路910、存储器920、输入单元930、显示单元940、传感器950、音频电路960、无线保真(英文全称:wireless fidelity,英文简称:WiFi)模块970、处理器980、以及电源990等部件。本领域技术人员可以理解,图9中示出的手机结构并不构成对手机的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0115] 下面结合图9对手机的各个构成部件进行具体的介绍:

[0116] RF电路910可用于收发信息或通话过程中,信号的接收和发送,特别地,将基站的下行信息接收后,给处理器980处理;另外,将设计上行的数据发送给基站。通常,RF电路910包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器(英文全称:Low Noise Amplifier,英文简称:LNA)、双工器等。此外,RF电路910还可以通过无线通信与网络和其他设备通信。上述无线通信可以使用任一通信标准或协议,包括但不限于全球移动通讯系统(英文全称:Global System of Mobile communication,英文简称:GSM)、通用分组无线服务(英文全称:General Packet Radio Service,英文简称:GPRS)、码分多址(英文全称:Code Division Multiple Access,英文简称:CDMA)、宽带码分多址(英文全称:Wideband Code Division Multiple Access,英文简称:WCDMA)、长期演进(英文全称:Long Term Evolution,英文简称:LTE)、电子邮件、短消息服务(英文全称:Short Messaging Service,英文简称:SMS)等。

[0117] 存储器920可用于存储软件程序以及模块,处理器1080通过运行存储在存储器920的软件程序以及模块,从而执行手机的各种功能应用以及数据处理。存储器920可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器920可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0118] 输入单元930可用于接收输入的数字或字符信息，以及产生与手机的用户设置以及功能控制有关的键信号输入。具体地，输入单元930可包括触控面板931以及其他输入设备932。触控面板931，也称为触摸屏，可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触控面板931上或在触控面板931附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触控面板931可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器980，并能接收处理器980发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板931。除了触控面板931，输入单元930还可以包括其他输入设备932。具体地，其他输入设备932可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0119] 显示单元940可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元940可包括显示面板941，可选的，可以采用液晶显示器(英文全称：Liquid Crystal Display，英文简称：LCD)、有机发光二极管(英文全称：Organic Light-Emitting Diode，英文简称：OLED)等形式来配置显示面板941。进一步的，触控面板931可覆盖显示面板941，当触控面板931检测到在其上或附近的触摸操作后，传送给处理器980以确定触摸事件的类型，随后处理器980根据触摸事件的类型在显示面板941上提供相应的视觉输出。虽然在图9中，触控面板931与显示面板941是作为两个独立的部件来实现手机的输入和输入功能，但是在某些实施例中，可以将触控面板931与显示面板941集成而实现手机的输入和输出功能。

[0120] 手机还可包括至少一种传感器950，比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示面板941的亮度，接近传感器可在手机移动到耳边时，关闭显示面板941和/或背光。作为运动传感器的一种，加速计传感器可检测各个方向上(一般为三轴)加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等；至于手机还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0121] 音频电路960、扬声器961，传声器962可提供用户与手机之间的音频接口。音频电路960可将接收到的音频数据转换后的电信号，传输到扬声器961，由扬声器961转换为声音信号输出；另一方面，传声器962将收集的声音信号转换为电信号，由音频电路960接收后转换为音频数据，再将音频数据输出处理器980处理后，经RF电路910以发送给比如另一手机，或者将音频数据输出至存储器920以便进一步处理。

[0122] WiFi属于短距离无线传输技术，手机通过WiFi模块970可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图9示出了WiFi模块970，但是可以理解的是，其并不属于手机的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0123] 处理器980是手机的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器920内的软件程序和/或模块，以及调用存储在存储器920内的数据，执行手机的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器980可包

括一个或多个处理单元;优选的,处理器980可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器980中。

[0124] 手机还包括给各个部件供电的电源990(比如电池),优选的,电源可以通过电源管理系统与处理器980逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

[0125] 尽管未示出,手机还可以包括摄像头、蓝牙模块等,在此不再赘述。

[0126] 在本发明实施例中,该终端所包括的处理器980还具有控制执行以上由终端设备执行的方法流程。

[0127] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0128] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统,装置和模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0129] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统,装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述模块的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个模块或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或模块的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0130] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的,作为模块显示的部件可以是或者也可以不是物理模块,即可以位于一个地方,或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0131] 另外,在本申请各个实施例中的各功能模块可以集成在一个处理模块中,也可以是各个模块单独物理存在,也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。

[0132] 所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。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或者该技术方案的全部或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)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(英文全称:Read-Only Memory,英文简称:ROM)、随机存取存储器(英文全称:Random Access Memory,英文简称:RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0133] 以上对本申请所提供的技术方案进行了详细介绍,本申请中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

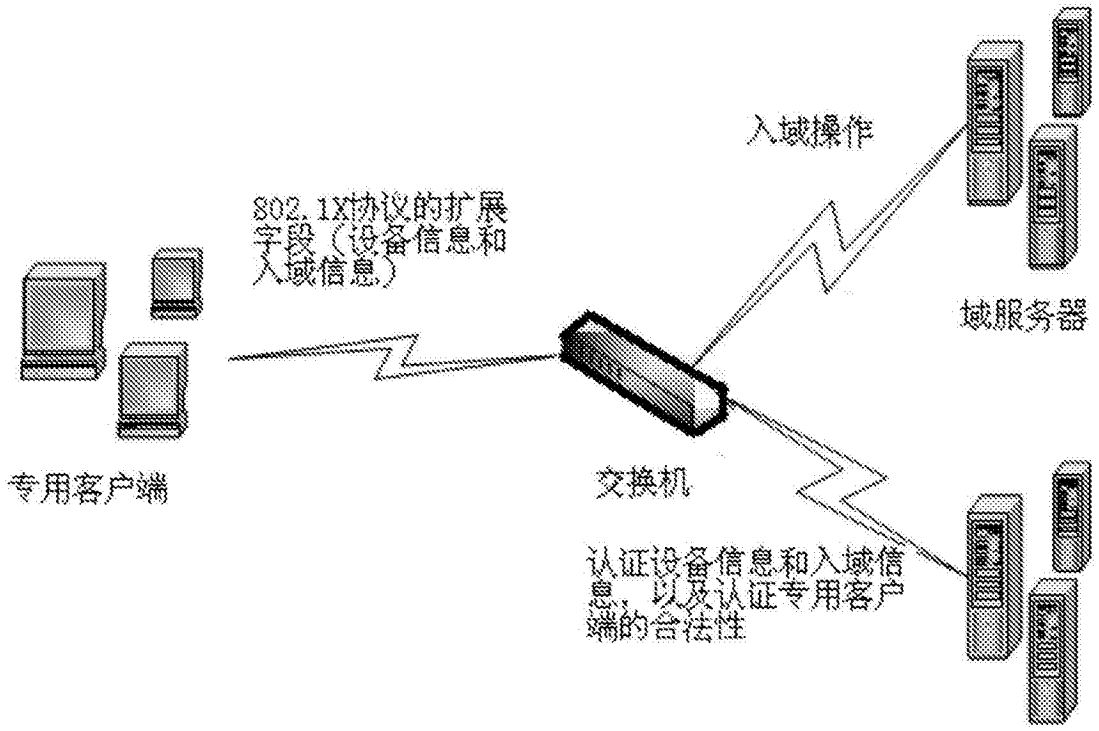

802.1X协议的扩展字段（设备信息和入域信息）
入域操作
域服务器
专用客户端
交换机
认证设备信息和入域信息，以及认证专用客户端的合法性

图1


终端设备
网络认证服务器
域服务器
201、终端设备获取所述终端设备的设备信息和入域信息
202、发送接入认证请求
203、接收送接入认证请求
204、解析接入认证请求中的扩展字段，得到设备信息和入域信息
206、认证通过后，网络认证服务器开通终端设备接入目标网络的临时权限
205、对解析得到的设备信息和所述入域信息分别进行认证
入域请求
208、接收接入确认响应
207、发送接入确认响应
209、通过域服务器入目标网络对应的域后，接入目标网络

图2

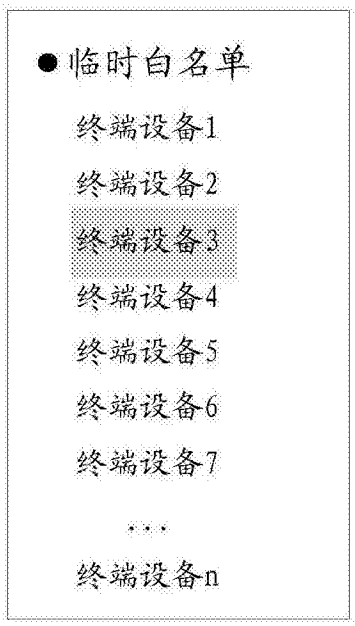

●临时白名单
终端设备1
终端设备2
终端设备3
终端设备4
终端设备5
终端设备6
终端设备7
...
终端设备n

图3

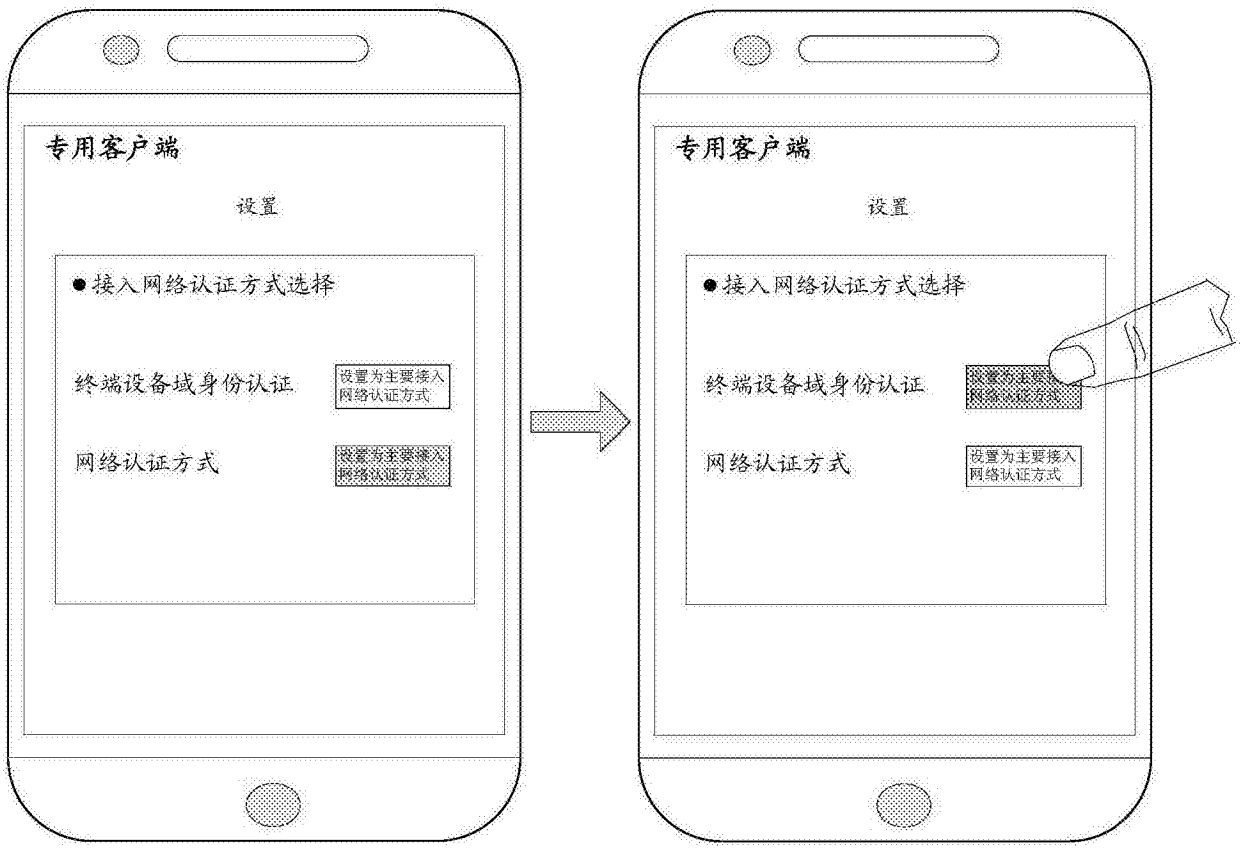

专用客户端
设置
●接入网络认证方式选择
终端设备域身份认证
设置为主要接入网络认证方式
网络认证方式
设置为主要接入网络认证方式
专用客户端
设置
●接入网络认证方式选择
终端设备域身份认证
网络认证方式
设置为主要接入网络认证方式

图4

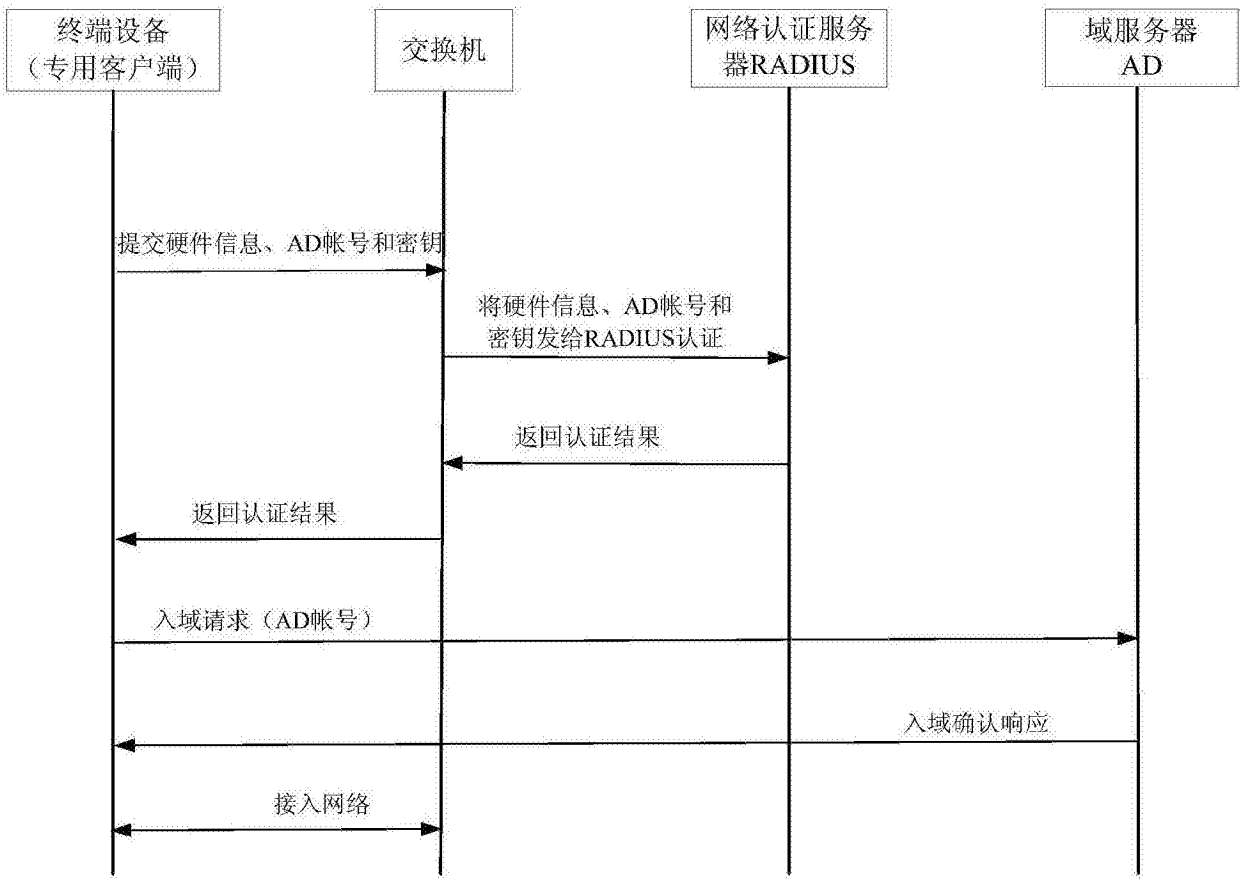

终端设备
（专用客户端）
交换机
网络认证服务
器RADIUS
域服务器
AD
提交硬件信息、AD帐号和密钥
将硬件信息、AD帐号和
密钥发给RADIUS认证
返回认证结果
返回认证结果
入域请求（AD帐号）
入域确认响应
接入网络

图5

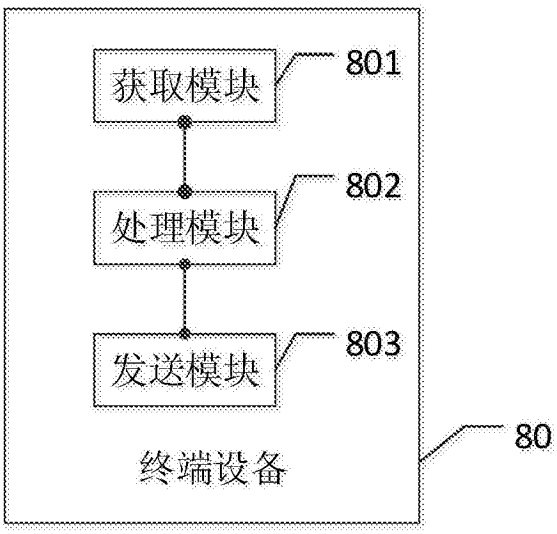

获取模块
801
处理模块
802
发送模块
803
终端设备
80

图6

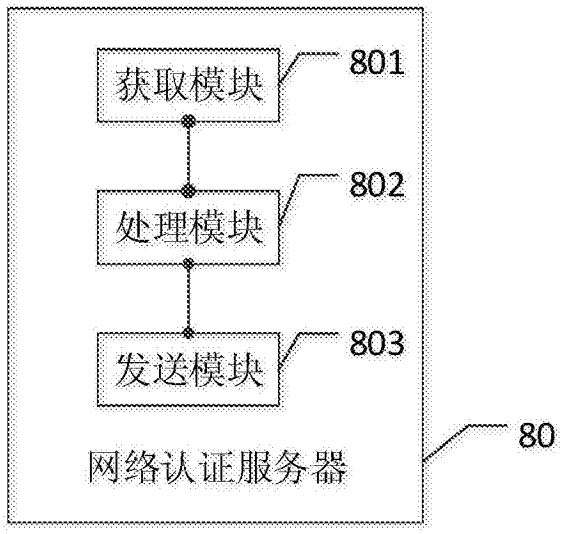

获取模块
801
处理模块
802
发送模块
803
网络认证服务器
80

图7

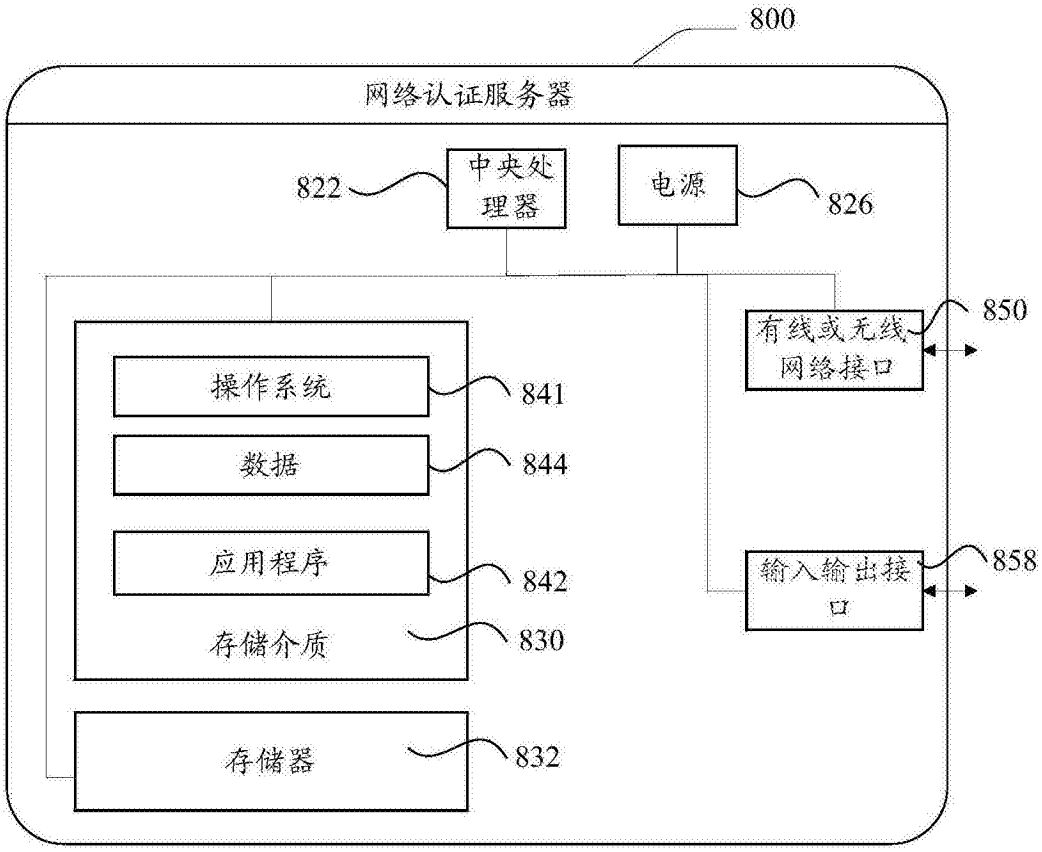

800
网络认证服务器
822
中央处理器
电源
826
有线或无线网络接口
850
操作系统
841
数据
844
应用程序
842
存储介质
830
输入输出接口
858
存储器
832

图8

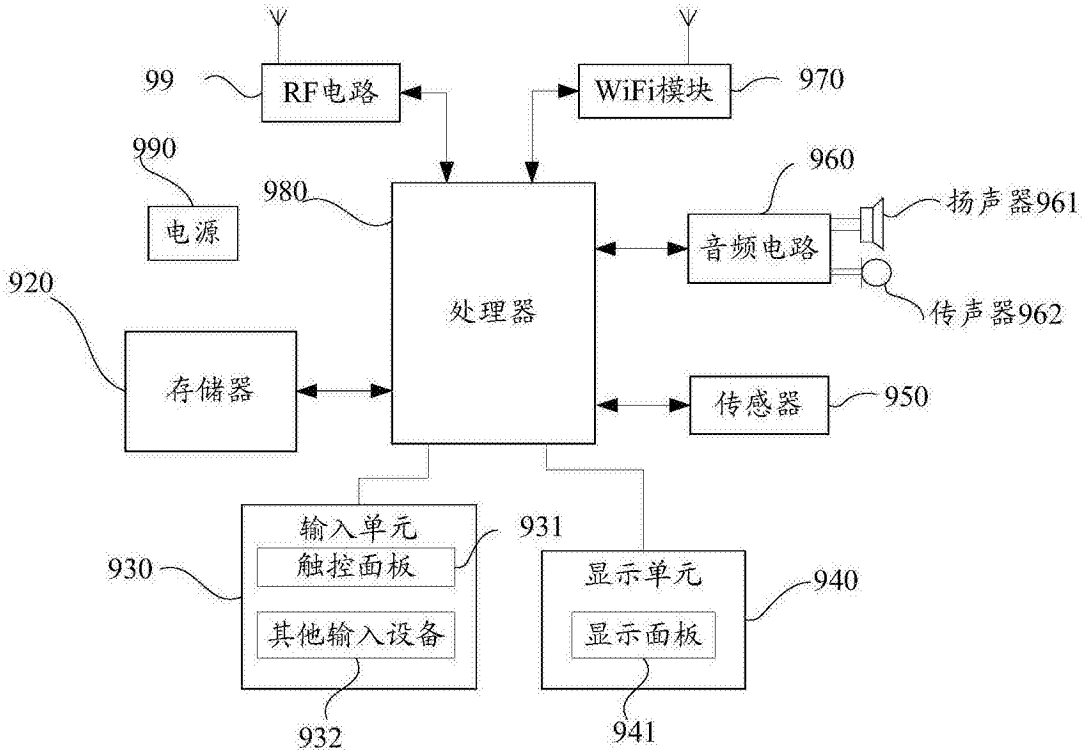

99
RF电路
WiFi模块
970
990
电源
980
处理器
960
音频电路
扬声器961
传声器962
920
存储器
传感器
950
输入单元
触控面板
931
930
其他输入设备
显示单元
显示面板
940
932
941

图9