(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 106549911 A
(43)申请公布日 2017.03.29

(21)申请号 201510595743.2

(22)申请日 2015.09.17

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦

(72)发明人 李燕

(74)专利代理机构 深圳鼎合诚知识产权代理有限公司 44281
代理人 薛祥辉 李发兵

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

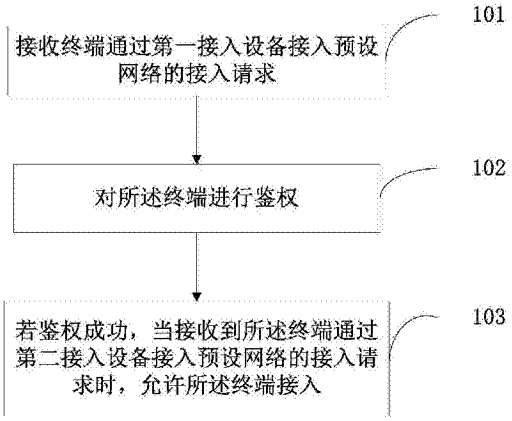
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种终端接入方法及装置

(57)摘要

本发明公开了一种终端接入方法及装置，包括：接收终端通过第一接入设备接入预设网络的接入请求，对所述终端进行鉴权；若鉴权成功，当接收到所述终端通过第二接入设备接入所述预设网络的接入请求时，允许所述终端接入。本发明提供的终端接入方法与装置，将证书鉴权与密钥协商的过程分离，使得终端只进行一次证书鉴权，鉴权通过后，当其从一个接入设备漫游到另一个接入设备时，不需要再次鉴权，就能直接接入网络，解决了终端漫游时业务受到影响的问题，提升了用户体验。



CN 106549911 A

1.一种终端接入方法,其特征在于,包括:

接收终端通过第一接入设备接入预设网络的接入请求,对所述终端进行鉴权;

若鉴权成功,当接收到所述终端通过第二接入设备接入所述预设网络的接入请求时,允许所述终端接入。

2.如权利要求1所述的终端接入方法,其特征在于,若鉴权成功,则还包括:将第一密钥或生成所述第一密钥所需的信息,传输给所述第一接入设备和所述终端,所述第一密钥为固定密钥;所述允许所述终端接入后,还包括:将所述第一密钥或生成所述第一密钥所需的信息传输给第二接入设备;

或者,若鉴权成功,则还包括:将第二密钥或生成所述第二密钥所需的信息,传输给所述第一接入设备和所述终端,所述第二密钥为周期性更新的密钥;所述允许所述终端接入后,还包括:将当前更新后的第二密钥或生成所述更新后的第二密钥所需的信息传输给所述第二接入设备和所述终端;

所述第一密钥或第二密钥用于所述终端与所述第一接入设备或所述第二接入设备生成两者之间进行数据传输的加解密密钥。

3.如权利要求2所述的终端接入方法,其特征在于,若鉴权成功,则还包括存储所述第一密钥或所述第二密钥、所述第一接入设备或所述第二接入设备的介质访问控制层地址、所述终端的介质访问控制层地址,所述第一密钥或所述第二密钥的生效时间,所述第一密钥或所述第二密钥的老化时间。

4.如权利要求1-3任一项所述的终端接入方法,其特征在于,对所述终端进行鉴权包括:获取所述终端的证书和所述第一接入设备的证书,根据所述终端的证书和所述第一接入设备的证书对所述接入终端进行鉴权。

5.如权利要求4所述的终端接入方法,其特征在于,获取所述第一接入设备的证书的方法具体为:从所述第一接入设备或从第三方服务器上进行获取。

6.一种终端接入系统,其特征在于,包括:

第一接受请求模块,用于接收终端通过第一接入设备接入预设网络的接入请求;

鉴权模块,用于当接收到终端通过第一接入设备接入预设网络的接入请求时,对所述终端进行鉴权;

第二接受请求模块,用于当鉴权成功后,接收所述终端通过第二接入设备接入预设网络的接入请求;

允许接入模块,用于当鉴权模块鉴权成功后,所述第二接受请求模块接收到终端通过第二接入设备接入所述预设网络的接入请求时,允许所述接入终端接入。

7.如权利要求6所述的终端接入系统,其特征在于,还包括:

第一传输模块,用于将第一密钥或生成所述第一密钥所需的信息,传输给所述第一接入设备和所述终端,所述第一密钥为固定密钥,或用于所述允许接入模块允许所述终端接入后,将所述第一密钥或生成所述第一密钥所需的信息传输给第二接入设备;

第二传输模块,用于将第二密钥或生成所述第二密钥所需的信息,传输给所述第一接入设备和所述终端,所述第二密钥为周期性更新的密钥;或用于所述允许接入模块允许所述终端接入后,将当前更新后的第二密钥或生成所述更新后的第二密钥所需的信息传输给所述第二接入设备和所述终端。

8.如权利要求7所述的终端接入系统，其特征在于，还包括存储模块，所述存储模块用于当所述鉴权模块鉴权成功后，存储所述第一密钥或所述第二密钥、所述第一接入设备或所述第二接入设备的介质访问控制层地址、所述终端的介质访问控制层地址，所述第一密钥或所述第二密钥的生效时间，所述第一密钥或所述第二密钥的老化时间。

9.如权利要求6-8任一项所述的终端接入系统，其特征在于，所述鉴权模块还包括证书存储单元，所述证书存储单元用于存储获取的所述第一接入设备的证书。

10.如权利要求9所述的终端接入系统，其特征在于，所述鉴权模块还包括第一接入设备证书获取单元，所述第一接入设备证书获取单元获取所述第一接入设备的证书的方法具体为：从所述第一接入设备或从第三方服务器上进行获取。

一种终端接入方法及装置

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种终端接入方法及装置。

背景技术

[0002] 随着无线保真(Wireless-Fidelity，Wifi)业务普及，人们对Wifi安全的关注也逐日提升。2003年年底，中国政府宣布了一项政策，要求在中国出售的无线设备必须支持无线局域网认证基础设施标准(WLAN Authentication and Privacy Infrastructure,WAPI)是中国自主研发的，拥有自主知识产权的无线局域网安全技术标准。是为了解决无线局域网国际标准中的安全漏洞而设计的安全增强协议，主要保护无线网络中数据传输的机密性、完整性、鉴别性，同时对请求接入网络的用户进行身份鉴别和访问控制，保障合法的用户安全接入并安全访问合法的网络。

[0003] WAPI由无线局域网鉴别基础架构(WLAN Authentication Infrastructure,WAI)和无线局域网保密基础架构(WLAN Privacy Infrastructure,WPI)组成。WAI和WPI分别实现对用户身份的鉴别和对传输的数据加密。其中WAI采用公钥密码技术，用于无线客户端(station,STA)与无线接入点(Access Point,AP)之间的身份认证。而WPI则采用国家密码管理委员会办公室批准的用于WLAN的对称密码算法实现数据保护，对介质访问控制(Medium Access Control，MAC)子层的MAC数据服务单元进行加密、解密处理。WAPI协议包含两种类型：1)基于证书的鉴别和密钥管理；2)基于预共享密钥的鉴别和密钥管理。

[0004] 针对基于证书的鉴别和密钥管理的WAPI协议的通信，现有技术中终端每次接入网络都需要进行证书鉴权与密钥协商的过程，即接入不同的接入点AP，就要进行不同的证书鉴权和密钥协商，这样使得WLAN接入终端用户在漫游时业务会受到影响，使用户的体验不佳。

发明内容

[0005] 本发明要解决的主要技术问题是，提供一种终端接入方法及装置，用于解决现有技术中终端每次接入网络都需要进行证书鉴权与密钥协商的过程，使得WLAN接入终端用户在漫游时业务会受到影响的技术问题。

[0006] 为解决上述技术问题，本发明提供一种终端接入方法，包括：接收终端通过第一接入设备接入预设网络的接入请求，对所述终端进行鉴权；若鉴权成功，当接收到所述终端通过第二接入设备接入所述预设网络的接入请求时，允许所述终端接入。

[0007] 在本发明一种实施例中，若鉴权成功，则还包括：将第一密钥或生成所述第一密钥所需的信息，传输给所述第一接入设备和所述终端，所述第一密钥为固定密钥；所述允许所述终端接入后，还包括：将所述第一密钥或生成所述第一密钥所需的信息传输给第二接入设备；

[0008] 或者，若鉴权成功，则还包括：将第二密钥或生成所述第二密钥所需的信息，传输给所述第一接入设备和所述终端，所述第二密钥为周期性更新的密钥；所述允许所述终端

接入后，还包括：将第二密钥或生成所述第二密钥所需的信息传输给所述第二接入设备和所述终端；

[0009] 所述第一密钥、第二密钥用于所述终端、所述第一接入设备、所述第二接入设备生成用于所述终端与所述第一接入设备或所述第二接入设备之间进行数据传输的加解密密钥。

[0010] 在本发明一种实施例中，若鉴权成功，则还包括：存储所述第一密钥或所述第二密钥，以及所述第一接入设备的介质访问控制层地址和所述终端的介质访问控制层地址。

[0011] 在本发明一种实施例中，对所述终端进行鉴权包括：获取所述终端的证书和所述第一接入设备的证书，根据所述终端的证书和所述第一接入设备的证书对所述接入终端进行鉴权。

[0012] 在本发明一种实施例中，获取所述第一接入设备的证书的方法具体为：从所述第一接入设备、接入控制器、交换机、云端或第三方服务器上进行获取。

[0013] 本发明还提供一种终端接入装置，包括：

[0014] 接收模块，用于接收终端通过第一接入设备接入预设网络的接入请求；以及当鉴权模块鉴权成功后，接收所述终端通过第二接入设备接入预设网络的接入请求；

[0015] 鉴权模块，用于所述接收模块接收到所述终端通过所述第一接入设备接入所述预设网络的接入请求时，对所述终端进行鉴权；

[0016] 接入模块，用于当所述接收模块接收到所述终端通过第二接入设备接入所述预设网络的接入请求时，允许所述终端接入。

[0017] 在本发明一种实施例中，还包括：

[0018] 第一传输模块，用于将第一密钥或生成所述第一密钥所需的信息，传输给所述第一接入设备和所述终端，所述第一密钥为固定密钥；

[0019] 第二传输模块，用于将所述第一密钥或生成所述第一密钥所需的信息传输给第二接入设备；

[0020] 第三传输模块，用于将第二密钥或生成所述第二密钥所需的信息，传输给所述第一接入设备和所述终端，所述第二密钥为周期性更新的密钥；

[0021] 第四传输模块，用于将第二密钥或生成所述第二密钥所需的信息传输给所述第二接入设备和所述终端。

[0022] 在本发明一种实施例中，还包括存储模块，所述存储模块用于存储所述第一密钥或所述第二密钥，以及所述第一接入设备的介质访问控制层地址和所述终端的介质访问控制层地址。

[0023] 在本发明一种实施例中，所述鉴权模块包括：

[0024] 获取子模块，用于获取所述终端的证书和所述第一接入设备的证书；

[0025] 鉴权子模块，用于根据所述终端的证书和所述第一接入设备的证书对所述接入终端进行鉴权。

[0026] 在本发明一种实施例中，所述获取子模块具体用于从所述第一接入设备、接入控制器、交换机、云端或第三方服务器上进行获取所述第一接入设备的证书。

[0027] 本发明的有益效果是：

[0028] 本发明提供的终端接入方法与装置，将证书鉴权与密钥协商的过程分离，使得终

端只进行一次证书鉴权，鉴权通过后，当其从一个接入设备漫游到另一个接入设备时，不需要再次鉴权，就能直接接入网络，提升了用户体验。

附图说明

[0029] 图 1 为本发明一种实施例的终端接入方法流程图；

[0030] 图 2 为本发明一种实施例的证书检验下载流程图；

[0031] 图 3 为本发明一种实施例的终端接入装置示意图；

[0032] 图 4 为图 3 终端接入装置中鉴权模块示意图；

[0033] 图 5 为实施例三中的终端接入流程图。

具体实施方式

[0034] 下面通过具体实施方式结合附图对本发明作进一步详细说明。

[0035] 实施例一：

[0036] 请参考图 1，图 1 为本发明一种实施例的终端接入方法流程图：

[0037] S101, 接收终端通过第一接入设备接入预设网络的接入请求；

[0038] 当接收到终端通过第一接入设备提出接入预设网络的请求后，终端与第一接入设备就进行了相互关联，收到第一接入设备发出的终端的信息后，会提起鉴权激活，通过第一接入设备转发给终端；终端收到鉴权激活后，提出接入鉴权请求。

[0039] 为了提高预设网络中接入点的安全性与可靠性，可以对接入点进行合法接入检验，这个检验过程可以是在终端请求接入预设网络之前，对该预设网络下全部或部分的接入设备进行合法接入检验，也可以是在接收到终端从某一个接入设备上发送的接入请求后，即对该接入设备进行合法接入验证。

[0040] S102, 对终端进行鉴权；

[0041] 收到终端提出的接入鉴权请求之后，需要获取第一接入设备与终端的证书。对于第一接入设备的证书，可以对其证书进行检验，请结合图 2：

[0042] S201，检验证书是否存在；

[0043] 若判断结果为否，则第一接入设备的证书不存在，执行 S202；

[0044] S202, 从第三方服务器上获取证书并安装；

[0045] 若判断结果为是，则第一接入设备的证书存在，执行 S203；

[0046] S203, 检验证书是否过期；

[0047] 若该证书已经过期，则执行 S202，从第三方服务器获取新的证书下载并安装，更新原有证书；

[0048] 若判断第一接入设备的证书并未过期，则继续使用该证书。进一步的，获取到最新的第一接入设备的证书之后，还可以存储该证书。

[0049] 由于在终端与预设网络进行相互关联之后，终端会通过第一接入设备转发出终端信息，终端信息中就包含从证书服务器上下载的终端证书。

[0050] 获取到第一接入设备与终端的证书后，将其封装成为证书鉴权报文，然后将该证书鉴权报文发送给第三方鉴权服务器进行鉴权，这里的第三方鉴权服务器可以是证书服务器，可以理解的是，证书服务器已经参与了第一接入设备与终端的证书生成，所以这里选

择证书服务器作为第三方鉴权服务器只是为了尽量减少终端接入预设网络时的交互参与者，提高终端接入预设网络过程的安全性，并不是必须的选择。

[0051] S103，若鉴权成功，当接收到所述终端通过第二接入设备接入所述预设网络的接入请求时，允许所述终端接入。

[0052] 证书服务器对第一接入设备与终端的证书进行证书鉴权后，会反馈证书鉴权结果，根据这个证书鉴权结果，判断鉴权是否成功；当判断结果为是，则允许终端通过第一接入设备接入预设网络，生成第一密钥；然后构建接入鉴权激活报文发送给第一接入设备和终端，发送给第一接入设备的接入鉴权报文可以包含生成的第一密钥，也可以包含生成第一密钥所需的信息；同样的，发送给终端的接入鉴权激活报文也可以包含第一密钥或生成第一密钥所需的信息，优选的，本实施例中，发送给终端的接入鉴权激活报文中包含生成第一密钥所需的信息，发送给第一接入设备的接入鉴权激活报文包含第一密钥；给终端发送的接入鉴权激活报文中包含生成第一密钥所需的信息是考虑到终端获取到接入鉴权激活报文需要通过第一接入终端进行转发，因此仅发送生成第一密钥所需的信息会更安全；而发送给第一接入设备的接入鉴权激活报文包含第一密钥是为了简化第一接入设备的工作。

[0053] 当终端获取到接入鉴权激活报文后，可以根据接入鉴权激活报文中的鉴权结果选择是否接入预设网络，当选择结果为是，终端还可以选择是否从第一接入设备接入预设的网络，若选择结果为否，终端可以选择从第二接入设备上接入预设网络；毫无疑义的是，终端可以再选择从第一接入设备接入预设网络，然后离开第一接入设备，选择从第二接入设备接入预设网络。在本实施例中，终端首先选择从第一接入设备接入预设网络，然后又离开第一接入设备，选择从第二接入设备接入预设网络。

[0054] 由于终端与预设网络已经通过第一接入设备进行了双向鉴权，所以，当终端选择从第二接入设备接入预设网络时，不需要再经历证书鉴权的过程，当接收到终端通过第二接入设备接入预设网络的接入请求时，可以直接允许终端接入；由于第一密钥是固定密钥，所以，当终端从第二接入设备接入预设网络时，只需要将第一密钥或生成第一密钥所需的信息发送给第二接入设备。

[0055] 终端与第一接入设备或第二接入设备可以通过获取到的第一密钥或者是根据相关信息生成的第一密钥，进行密钥协商，协商出用于终端与第一接入设备或第二接入设备之间进行数据传输加解密的密钥，这里的密钥可以是单播密钥，也可以是组播密钥。

[0056] 为了更进一步地提高用于密钥协商的密钥的安全性，因此，在本发明提供的另一优选实施例中，可以选择用第二密钥代替上述第一密钥，第二密钥是周期性更新的密钥，每更新第二密钥一次，就给终端以及当前终端关联的接入设备发送一次第二密钥或生成第二密钥所需的信息；终端与第一接入设备或第二接入设备可以通过获取到的第二密钥或者是根据相关信息生成的第二密钥，进行密钥协商，通过这种不断更新密钥的方式，使得第一接入设备与第二接入设备对第二密钥一次性利用，不用存储密钥，有效地提高了终端接入预设网络的安全性与可靠性。

[0057] 当根据证书服务器反馈的鉴权结果判断鉴权成功后，生成第一密钥或第二密钥，并将第一密钥或第二密钥及其相关信息进行存储，存储的内容包括第一密钥或第二密钥、第一接入设备的介质访问控制层（Medium Access Control，MAC）地址、终端的MAC地址。

[0058] 进一步地，储存的内容还包括第一密钥或第二密钥的老化时间，终端从第一接入

设备离开后，如果在第一密钥或第二密钥的老化时间内请求从第二接入设备上接入预设网络，则第二接入设备可以直接允许该终端接入，不需要进行证书鉴权的过程，但是，当终端是在第一密钥或第二密钥的老化时间之后请求接入，则需要重新进行证书鉴权。

[0059] 在本发明提供的另一实施例中，储存的第一密钥或第二密钥及其相关信息还包括第一密钥或第二密钥的生效时间。

[0060] 当终端从第一接入设备漫游到第二接入设备后，储存的第一密钥或第二密钥及其相关信息至少包括：第一密钥或第二密钥、第二接入设备的介质访问控制层(Medium Access Control，MAC)地址、终端的MAC地址。

[0061] 实施例二：

[0062] 本发明还提供一种终端接入装置，下面结合图3进行详细说明：

[0063] 终端接入装置包括：

[0064] 接收模块301，用于接收终端通过第一接入设备接入预设网络的接入请求；以及当鉴权模块鉴权成功后，接收终端通过第二接入设备接入预设网络的接入请求；

[0065] 当接收到终端通过第一接入设备提出接入预设网络的请求后，终端与第一接入设备就进行了相互关联，收到第一接入设备发出的终端的信息后，会提起鉴权激活，通过第一接入设备转发给终端；终端收到鉴权激活后，提出接入鉴权请求。

[0066] 为了提高预设网络中接入点的安全性与可靠性，可以对接入点进行合法接入检验，这个检验过程可以是在终端请求接入预设网络之前，对该预设网络下全部或部分的接入设备进行合法接入检验，也可以是在接收到终端从某一个接入设备上发送的接入请求后，即对该接入设备进行合法接入验证。

[0067] 鉴权模块302，用于接收模块接收到终端通过第一接入设备接入预设网络的接入请求时，对终端进行鉴权；

[0068] 请参考图4，鉴权模块302包括获取子模块3021和鉴权子模块3022。

[0069] 获取子模块3021用于获取终端的证书和第一接入设备的证书；对于第一接入设备的证书，可以对其证书进行检验，若终端接入装置中不存在第一接入设备的证书，则直接从第三方服务器上获取其证书并安装；若第一接入设备的证书已经存在，则检查该证书是否过期；若该证书已经过期，则从第三方服务器获取新的证书下载并安装，更新原有证书；若判断第一接入设备的证书并未过期，则终端接入装置继续使用该证书。进一步的，获取到最新的第一接入设备的证书之后，还可以由终端接入装置存储该证书。

[0070] 由于在终端与预设网络进行相互关联之后，终端会通过第一接入设备转发出终端信息，终端信息中就包含从证书服务器上下载的终端证书，所以获取子模块3022可以从上述终端信息中获取到终端的证书。

[0071] 鉴权子模块3022，用于根据终端的证书和第一接入设备的证书对接入终端进行鉴权。

[0072] 获取子模块3021获取到第一接入设备与终端的证书后，将其封装成为证书鉴权报文，然后将该证书鉴权报文发送给第三方鉴权服务器进行鉴权，这里的第三方鉴权服务器可以是证书服务器，可以理解的是，证书服务器已经参与了第一接入设备与终端的证书生成，所以这里选择证书服务器作为第三方鉴权服务器只是为了尽量减少终端接入预设网络时的交互参与者，提高终端接入预设网络过程的安全性，并不是必须的选择。

[0073] 接入模块303，用于当接收模块接收到终端通过第二接入设备接入预设网络的接入请求时，允许终端接入。

[0074] 第一传输模块304，用于将第一密钥或生成所述第一密钥所需的信息，传输给第一接入设备和终端，第一密钥为固定密钥。

[0075] 第二传输模块305，用于允许接入模块允许终端接入后，将第一密钥或生成第一密钥所需的信息传输给第二接入设备。

[0076] 第三传输模块306，用于将第二密钥或生成第二密钥所需的信息，传输给第一接入设备和终端，所述第二密钥为周期性更新的密钥。

[0077] 第四传输模块307，用于将第二密钥或生成第二密钥所需的信息传输给第二接入设备和终端。

[0078] 证书服务器对第一接入设备与终端的证书进行证书鉴权后，会反馈证书鉴权结果，根据这个证书鉴权结果，判断鉴权是否成功；当判断结果为是，则允许终端通过第一接入设备接入预设网络，生成第一密钥；然后构建接入鉴权激活报文由第一传输模块304发送给第一接入设备和终端，发送给第一接入设备的接入鉴权报文可以包含生成的第一密钥，也可以包含生成第一密钥所需的信息；同样的，发送给终端的接入鉴权激活报文也可以包含第一密钥或生成第一密钥所需的信息，优选的，本实施例中，发送给终端的接入鉴权激活报文中包含生成第一密钥所需的信息，发送给第一接入设备的接入鉴权激活报文包含第一密钥；给终端发送的接入鉴权激活报文中包含生成第一密钥所需的信息是考虑到终端获取到接入鉴权激活报文需要通过第一接入终端进行转发，因此仅发送生成第一密钥所需的信息会更安全；而发送给第一接入设备的接入鉴权激活报文包含第一密钥是为了简化第一接入设备的工作。

[0079] 当终端获取到接入鉴权激活报文后，可以根据接入鉴权激活报文中的鉴权结果选择是否接入预设网络，当选择结果为是，终端还可以选择是否从第一接入设备接入预设的网络，若选择结果为否，终端可以选择从第二接入设备上接入预设网络；毫无疑义的是，终端可以再选择从第一接入设备接入预设网络，然后离开第一接入设备，选择从第二接入设备接入预设网络。在本实施例中，终端首先选择从第一接入设备接入预设网络，然后又离开第一接入设备，选择从第二接入设备接入预设网络。

[0080] 由于终端与预设网络已经通过第一接入设备进行了双向鉴权，所以，当接收模块301接收到终端从第二接入设备接入预设网络的请求时，不需要再经历证书鉴权的过程；当接收模块301接收到终端通过第二接入设备接入预设网络的接入请求时，会通知接入模块303，接入模块303可以直接允许终端接入；由于第一密钥是固定密钥，所以，当终端从第二接入设备接入预设网络时，只需要由第二传输模块305将第一密钥或生成第一密钥所需的信息发送给第二接入设备。

[0081] 终端与第一接入设备或第二接入设备可以通过获取到的第一密钥或者是根据相关信息生成的第一密钥，进行密钥协商，协商出用于两者之间进行数据传输加解密的密钥，这里的密钥可以是单播密钥，也可以是组播密钥。

[0082] 为了更进一步地提高用于密钥协商的密钥的安全性，因此，在本发明提供的另一优选实施例中，可以选择用第二密钥代替上述第一密钥，第二密钥是周期性更新的密钥，每更新第二密钥一次，就由第三传输模块306给终端以及当前终端关联的第一接入设备发送

一次第二密钥或生成第二密钥所需的信息；或者由第四传输模块307给终端以及当前终端关联的第二接入设备发送一次第二密钥或生成第二密钥所需的信息；终端与第一接入设备或第二接入设备可以通过获取到的第二密钥或者是根据相关信息生成的第二密钥，进行密钥协商，通过这种不断更新密钥的方式，使得第一接入设备与第二接入设备对第二密钥一次性利用，不用存储密钥，有效地提高了终端接入预设网络的安全性与可靠性。

[0083] 本发明的终端接入装置还包括存储模块308，当根据证书服务器反馈的鉴权结果判断鉴权成功后，生成第一密钥或第二密钥，存储模块306会将第一密钥或第二密钥及其相关信息进行存储，存储的内容包括第一密钥或第二密钥、第一接入设备的MAC地址、终端的MAC地址。

[0084] 进一步地，储存的内容还包括第一密钥或第二密钥的老化时间，终端从第一接入设备离开后，如果在第一密钥或第二密钥的老化时间内请求从第二接入设备上接入预设网络，则第二接入设备可以直接允许该终端接入，不需要进行证书鉴权的过程，但是，当终端是在第一密钥或第二密钥的老化时间之后请求接入，则需要重新进行证书鉴权。

[0085] 在本发明提供的另一实施例中，储存的第一密钥或第二密钥及其相关信息还包括第一密钥或第二密钥的生效时间。

[0086] 当终端从第一接入设备漫游到第二接入设备后，储存的第一密钥或第二密钥及其相关信息至少包括：第一密钥或第二密钥、第二接入设备的MAC地址、终端的MAC地址。

[0087] 实施例三：

[0088] 本实施例在实施例二的基础上，可以由WAPI代理模块和第三方鉴权服务器一起作为终端接入装置。

[0089] 首先，将WAPI代理模块嵌入网络，对WLAN接入设备进行合法接入检验，通过一定的私有信息约定，确定WLAN接入设备是否能够接入网络；WAPI代理模块对WLAN接入设备的证书有效期进行检验、更新及安装；终端需要接入网络时，从证书服务器上下载一个证书。

[0090] 这里将结合图5对证书鉴权以及密钥协商做进一步说明：

[0091] S501，终端与WLAN接入设备进行关联；

[0092] 具体的，终端与WLAN接入设备关联后，WLAN接入设备将终端的信息通知给WAPI代理模块中的获取子模块，该信息中包含接入终端的证书；

[0093] S502，WAPI代理模块收到终端的信息后，发起鉴权激活；

[0094] S503，终端收到从WLAN接入设备转发过来的鉴权激活后发起接入鉴权请求；

[0095] S504，处理接入鉴权请求，发起证书鉴权请求；

[0096] 具体的，WAPI代理模块收到从WLAN接入设备转发过来的接入鉴权请求后，处理接入鉴权请求，封装终端与WLAN接入设备的证书的形成证书鉴权报文，并将证书鉴权报文发送给第三方鉴权服务器，以此发起证书鉴权请求；

[0097] S505，第三方鉴权服务器进行证书鉴权并发起证书鉴权响应；

[0098] 具体的，第三方鉴权服务器对终端的证书和WLAN接入设备的证书进行第三方鉴权，第三方鉴权服务器进行证书鉴权后，发起证书鉴权响应，同时将鉴权响应结果发给WAPI代理模块。

[0099] S506，WAPI代理模块根据收到证书鉴权响应产生基础密钥，并构建接入鉴权响应，

发送给终端；

[0100] 具体的，WAPI 代理模块收到证书鉴权响应结果后，根据该结果判断是否允许终端接入，如果允许终端接入，则产生基础密钥，这里的基础密钥可以是实施例二中的第一密钥也可以是第二密钥，优选地，本实施例还可以将基础密钥存储到 WPAI 代理模块中的基础密钥列表中，然后构建接入鉴权激活报文给终端，以此给终端接入鉴权响应。

[0101] S507，终端根据接入鉴权响应生成基础密钥；

[0102] 具体的，终端收到经 WLAN 接入设备转发来的接入鉴权激活报文后，根据鉴权结果判断是否接入 WLAN 接入设备，如果鉴权结果成功则接入，并生成基础密钥。

[0103] S508，WAPI 代理模块将产生的基础密钥通告给 WLAN 接入设备；

[0104] S509，WLAN 接入设备用获取的基础密钥与终端进行密钥协商；

[0105] 具体的，协商出用于两者之间进行数据传输加解密的密钥，这里的密钥可以是单播密钥，也可以是组播密钥。

[0106] 在本实施例中，终端接入装置可以放在AP、接入控制器 (Access Controller，AC)、交换机、云端上。

[0107] 以上内容是结合具体的实施方式对本发明所作的进一步详细说明，不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干简单推演或替换，都应当视为属于本发明的保护范围。

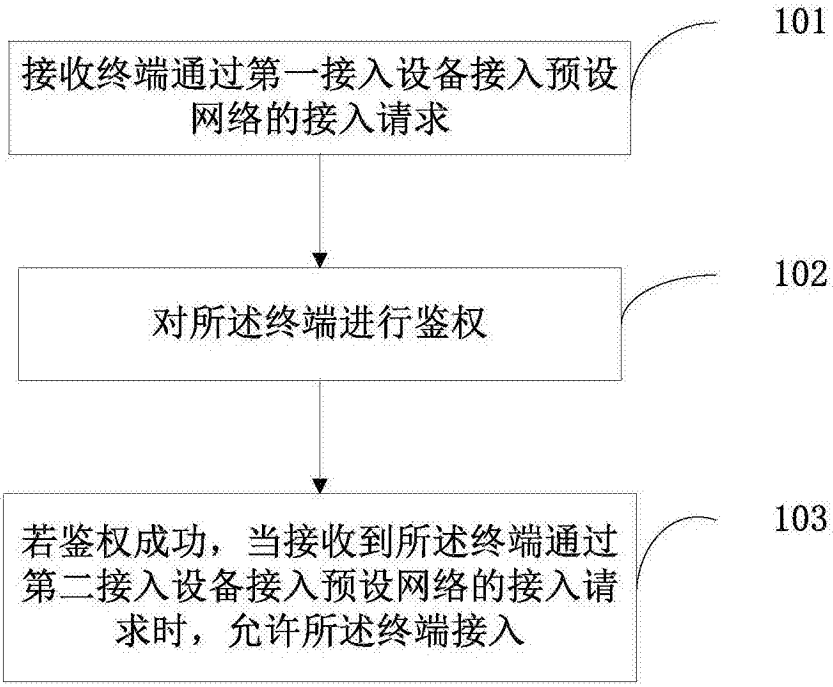

101
接收终端通过第一接入设备接入预设网络的接入请求
102
对所述终端进行鉴权
103
若鉴权成功，当接收到所述终端通过第二接入设备接入预设网络的接入请求时，允许所述终端接入

图 1

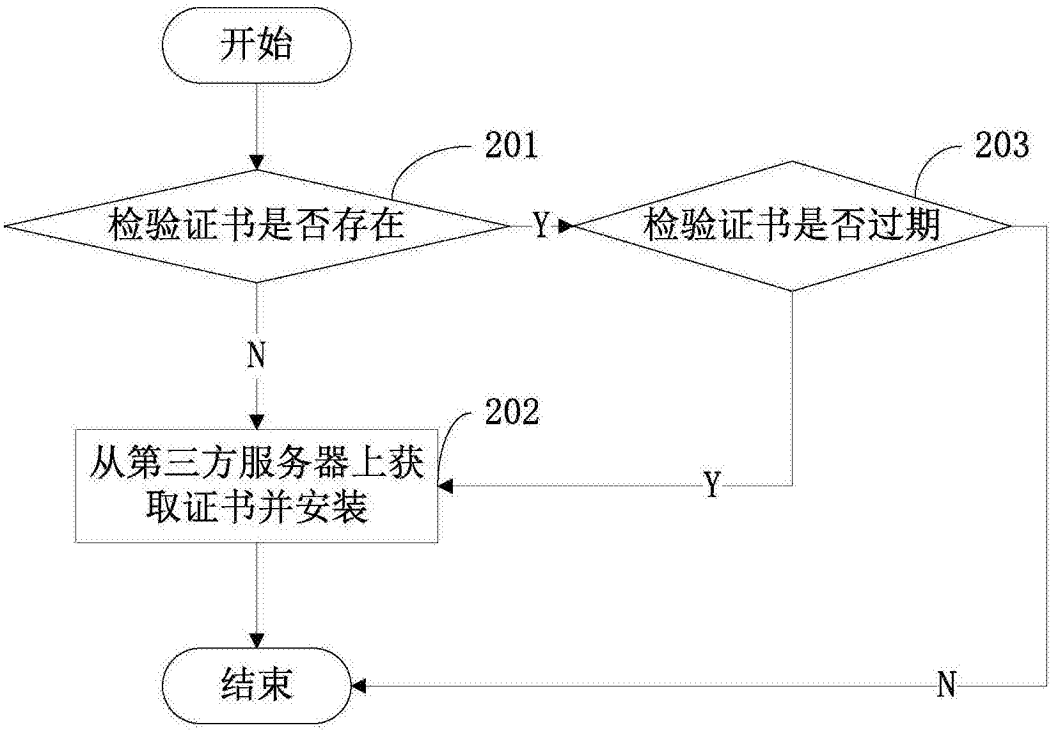

开始
201
检验证书是否存在
Y
203
检验证书是否过期
N
202
从第三方服务器上获取证书并安装
Y
结束
N

图 2

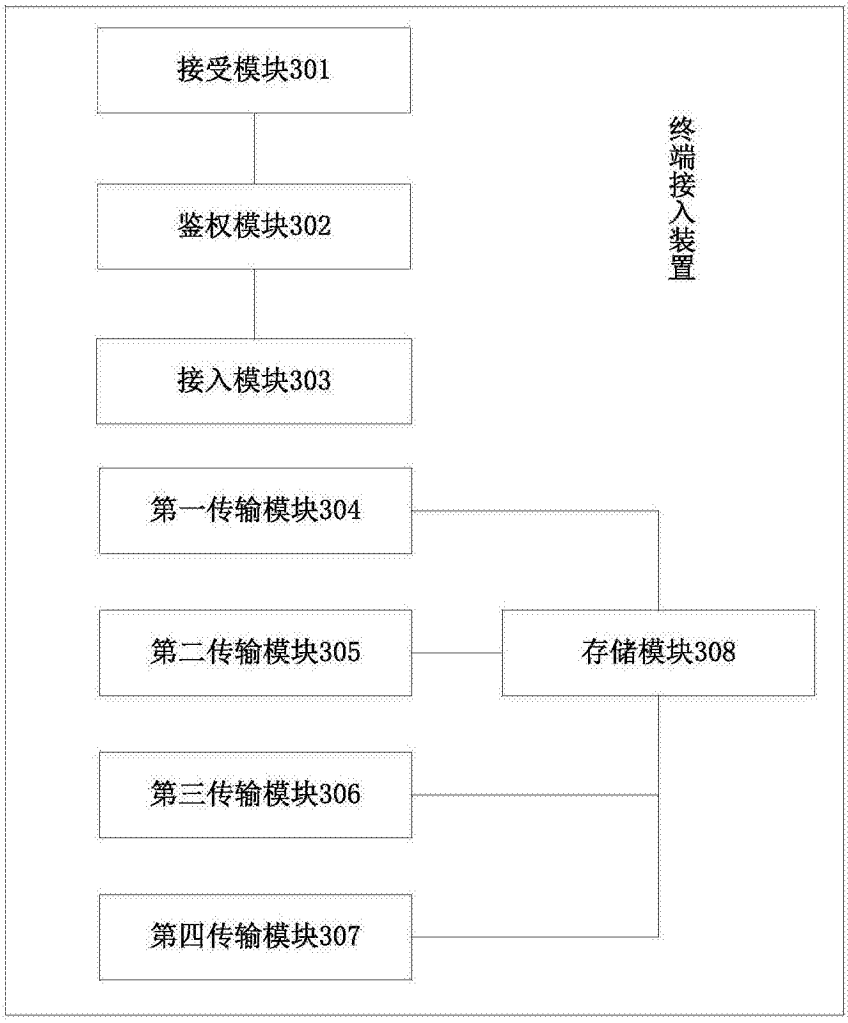

接受模块301
鉴权模块302
接入模块303
第一传输模块304
第二传输模块305
第三传输模块306
第四传输模块307
存储模块308
终端接入装置

图 3

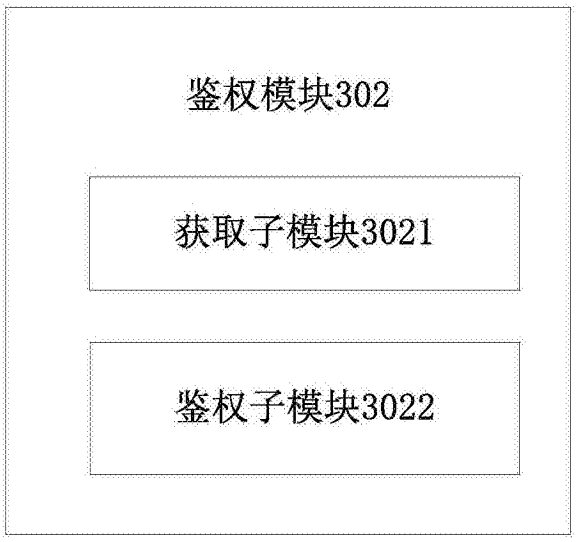

鉴权模块302
获取子模块3021
鉴权子模块3022

图 4

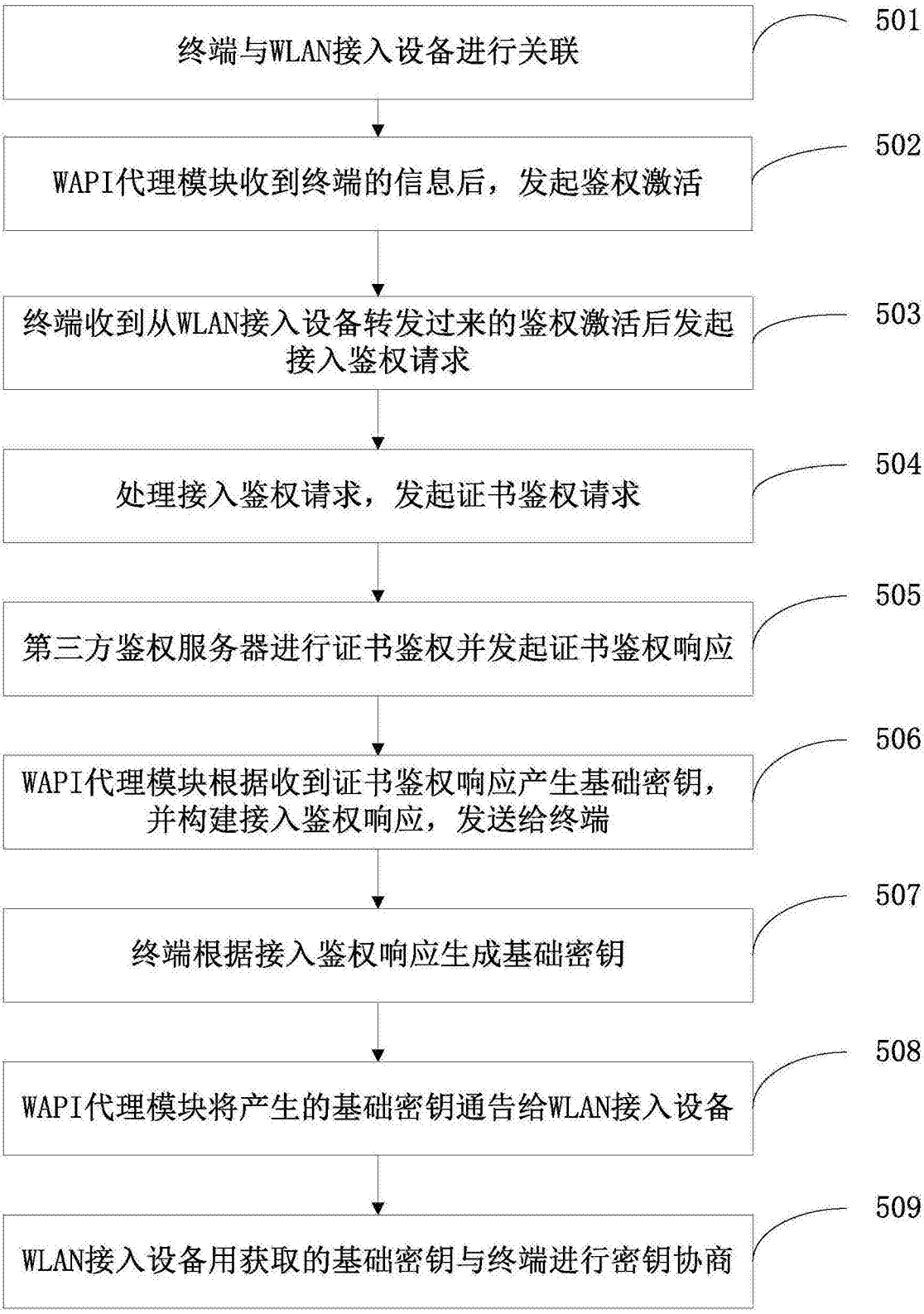

终端与WLAN接入设备进行关联
501
WAPI代理模块收到终端的信息后，发起鉴权激活
502
终端收到从WLAN接入设备转发过来的鉴权激活后发起接入鉴权请求
503
处理接入鉴权请求，发起证书鉴权请求
504
第三方鉴权服务器进行证书鉴权并发起证书鉴权响应
505
WAPI代理模块根据收到证书鉴权响应产生基础密钥，并构建接入鉴权响应，发送给终端
506
终端根据接入鉴权响应生成基础密钥
507
WAPI代理模块将产生的基础密钥通告给WLAN接入设备
508
WLAN接入设备用获取的基础密钥与终端进行密钥协商
509

图 5