(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102761940 B
(45)授权公告日 2016.06.08

(21)申请号 201210211976.4

(22)申请日 2012.06.26

(73)专利权人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路310号华为杭州生产基地

(72)发明人 徐勇刚 卢宇

(74)专利代理机构 北京鑫媛睿博知识产权代理有限公司 11297
代理人 龚家骅

(51)Int.Cl.
H04L 12/28(2006.01)

(56)对比文件
CN 102137401 A,2011.07.27,
CN 1567868 A,2005.01.19,

审查员 刘娟

权利要求书3页 说明书6页 附图3页

(54)发明名称

一种802.1X认证方法和设备

(57)摘要

本发明公开了一种802.1X认证方法和设备，该方法包括：接入设备接收来自AP设备的EAPOL-Start报文，且所述EAPOL-Start报文中携带AP设备的MAC地址、客户端对应的SSID、以及所述客户端的MAC地址；所述接入设备向认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。本发明中，使得接入设备可以精确获取客户端的接入AP设备。

CN 102761940 B

1.一种802.1X认证方法，应用于包括客户端、接入点AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，其特征在于，该方法包括以下步骤：

所述接入设备接收来自所述AP设备的局域网上的可扩展认证协议开始EAPOL-Start报文，且所述EAPOL-Start报文中携带所述AP设备的介质访问控制MAC地址、所述客户端对应的服务集标识SSID、以及所述客户端的MAC地址；

所述接入设备向所述认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证；

其中，所述接入设备为二层交换机。

2.如权利要求1所述的方法，其特征在于，

所述接入设备接收来自所述AP设备的EAPOL-Start报文，之后还包括：所述接入设备通过所述AP设备向所述客户端发送用于触发所述客户端进行认证的局域网上的可扩展认证协议请求EAPOL-Request报文，并接收来自所述客户端的局域网上的可扩展认证协议响应EAPOL-Response报文，且所述EAPOL-Response报文中携带所述客户端的认证信息；

所述接入设备向所述认证服务器发送认证请求报文，具体包括：所述接入设备向所述认证服务器发送携带所述客户端的认证信息的认证请求报文。

3.如权利要求2所述的方法，其特征在于，所述方法进一步包括：

所述接入设备接收来自所述AP设备的EAPOL-Start报文之后，所述接入设备在用户表项中记录所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址之间的对应关系；

所述接入设备接收来自所述客户端的EAPOL-Response报文之后，所述接入设备通过所述EAPOL-Response报文中携带的所述客户端的MAC地址查询所述用户表项，并利用查询结果得到所述客户端对应的AP设备的MAC地址以及所述客户端对应的SSID。

4.一种802.1X认证方法，应用于包括客户端、接入点AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，其特征在于，该方法包括以下步骤：

所述AP设备接收来自所述客户端的局域网上的可扩展认证协议开始EAPOL-Start报文，且所述EAPOL-Start报文中携带所述客户端的介质访问控制MAC地址；

所述AP设备在所述EAPOL-Start报文中添加所述AP设备本身的MAC地址以及所述客户端对应的服务集标识SSID；

所述AP设备将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备；

由所述接入设备利用收到的EAPOL-Start报文中携带的信息向所述认证服务器发送认证请求报文，并由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证；

其中，所述接入设备为二层交换机。

5.如权利要求4所述的方法，其特征在于，所述AP设备将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设

备，之后还包括：

所述AP设备接收来自所述接入设备的用于触发所述客户端进行认证的局域网上的可扩展认证协议请求EAPOL-Request报文，并将所述EAPOL-Request报文发送给所述客户端；以及，接收来自所述客户端的局域网上的可扩展认证协议响应EAPOL-Response报文，并将所述EAPOL-Response报文发送给所述接入设备，且所述EAPOL-Response报文中携带所述客户端的认证信息。

6.一种接入设备，应用于包括客户端、接入点AP设备、所述接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，其特征在于，该接入设备包括：

接收模块，用于接收来自所述AP设备的局域网上的可扩展认证协议开始EAPOL-Start报文，且所述EAPOL-Start报文中携带所述AP设备的介质访问控制MAC地址、所述客户端对应的服务集标识SSID、以及所述客户端的MAC地址；

发送模块，用于向所述认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证；

其中，所述接入设备为二层交换机。

7.如权利要求6所述的接入设备，其特征在于，

所述发送模块，还用于在接收到来自所述AP设备的EAPOL-Start报文之后，通过所述AP设备向所述客户端发送用于触发所述客户端进行认证的局域网上的可扩展认证协议请求EAPOL-Request报文；

所述接收模块，还用于接收来自所述客户端的局域网上的可扩展认证协议响应EAPOL-Response报文，且所述EAPOL-Response报文中携带所述客户端的认证信息；

且所述认证请求报文中还携带所述客户端的认证信息。

8.如权利要求7所述的接入设备，其特征在于，还包括：

处理模块，用于在接收到来自所述AP设备的EAPOL-Start报文之后，在用户表项中记录所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址之间的对应关系；

在接收到来自所述客户端的EAPOL-Response报文之后，通过所述EAPOL-Response报文中携带的所述客户端的MAC地址查询所述用户表项，并利用查询结果得到所述客户端对应的AP设备的MAC地址以及所述客户端对应的SSID。

9.一种接入点AP设备，应用于包括客户端、所述AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，其特征在于，该AP设备包括：

接收模块，用于接收来自所述客户端的局域网上的可扩展认证协议开始EAPOL-Start报文，且所述EAPOL-Start报文中携带所述客户端的介质访问控制MAC地址；

处理模块，用于在所述EAPOL-Start报文中添加所述AP设备本身的MAC地址以及所述客户端对应的服务集标识SSID；

发送模块，用于将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备；

由所述接入设备利用收到的EAPOL-Start报文中携带的信息向所述认证服务器发送认证请求报文，并由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证；

其中，所述接入设备为二层交换机。

10.如权利要求9所述的AP设备，其特征在于，

所述接收模块，还用于接收来自所述接入设备的用于触发所述客户端进行认证的局域网上的可扩展认证协议请求EAPOL-Request报文；以及，

接收来自所述客户端的局域网上的可扩展认证协议响应EAPOL-Response报文，所述EAPOL-Response报文中携带所述客户端的认证信息；所述发送模块，还用于将所述EAPOL-Request报文发送给所述客户端；以及，将所述EAPOL-Response报文发送给所述接入设备。

一种802.1X认证方法和设备

技术领域

[0001] 本发明涉及通信技术领域，特别是涉及一种802.1X认证方法和设备。

背景技术

[0002] 为了解决无线局域网的网络安全问题，提出了802.1X协议，该802.1X协议作为局域网端口的接入控制机制在以太网中被广泛应用，其用于解决以太网内认证和安全方面的问题；802.1X协议是一种基于端口的网络接入控制协议，且基于端口的网络接入控制是指：在局域网接入设备的端口对所接入的客户端进行认证和控制，如果连接在端口上的客户端能通过认证，则可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

[0003] 如图1所示，为802.1X认证系统的结构示意图，包括：客户端(Client)、接入设备(Device)和认证服务器(Server)；该客户端需要支持EAPOL(Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议)，且客户端可以通过启动客户端软件发起802.1X认证；接入设备为支持802.1X协议的网络设备，用于为客户端提供接入局域网的端口，该端口为物理端口或者逻辑端口；认证服务器是提供认证服务的实体，用于对客户端进行认证、授权和计费，其可以为RADIUS(Remote Authentication Dial-In User Service，远程认证拨号用户服务)服务器。

[0004] 随着无线技术的发展，802.1X认证系统可以应用在无线局域网中，如图2所示，为基于无线局域网的802.1X认证系统，图2中的二层交换机为接入设备，在该应用场景下，AP(Access Point，接入点)设备是无线连接的媒介，AP设备本身并不进行接入控制；且对于支持802.1X认证的二层交换机来说，由于无线接入空口传输的特殊性，二层交换机并不能感知到客户端是从哪个AP设备接入的，从而造成对客户端管理上的困难。

发明内容

[0005] 本发明提供一种802.1X认证方法和设备，以实现对客户端的精确管理和控制。

[0006] 为了达到上述目的，本发明提供一种802.1X认证方法，应用于包括客户端、接入点AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，该方法包括以下步骤：

[0007] 所述接入设备接收来自所述AP设备的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述AP设备的介质访问控制MAC地址、所述客户端对应的服务集标识SSID、以及所述客户端的MAC地址；

[0008] 所述接入设备向所述认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0009] 所述接入设备接收来自所述AP设备的EAPOL-Start报文，之后还包括：所述接入设备通过所述AP设备向所述客户端发送用于触发所述客户端进行认证的EAPOL-请求Request

报文，并接收来自所述客户端的EAPOL-响应Response报文，且所述EAPOL-Response报文中携带所述客户端的认证信息；

[0010] 所述接入设备向所述认证服务器发送认证请求报文，具体包括：所述接入设备向所述认证服务器发送携带所述客户端的认证信息的认证请求报文。

[0011] 所述方法进一步包括：接入设备接收来自所述AP设备的EAPOL-Start报文之后，所述接入设备在用户表项中记录所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址之间的对应关系；

[0012] 所述接入设备接收来自所述客户端的EAPOL-Response报文之后，所述接入设备通过所述EAPOL-Response报文中携带的所述客户端的MAC地址查询所述用户表项，并利用查询结果得到所述客户端对应的AP设备的MAC地址以及所述客户端对应的SSID。

[0013] 本发明提供一种802.1X认证方法，应用于包括客户端、接入点AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，该方法包括以下步骤：

[0014] 所述AP设备接收来自所述客户端的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述客户端的介质访问控制MAC地址；

[0015] 所述AP设备在所述EAPOL-Start报文中添加所述AP设备本身的MAC地址以及所述客户端对应的服务集标识SSID；

[0016] 所述AP设备将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备；

[0017] 由所述接入设备利用收到的EAPOL-Start报文中携带的信息向所述认证服务器发送认证请求报文，并由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0018] 所述AP设备将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备，之后还包括：所述AP设备接收来自所述接入设备的用于触发所述客户端进行认证的EAPOL-请求Request报文，并将所述EAPOL-Request报文发送给所述客户端；以及，接收来自所述客户端的EAPOL-响应Response报文，并将所述EAPOL-Response报文发送给所述接入设备，且所述EAPOL-Response报文中携带所述客户端的认证信息。

[0019] 本发明提供一种接入设备，应用于包括客户端、接入点AP设备、所述接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，该接入设备包括：

[0020] 接收模块，用于接收来自所述AP设备的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述AP设备的介质访问控制MAC地址、所述客户端对应的服务集标识SSID、以及所述客户端的MAC地址；

[0021] 发送模块，用于向所述认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0022] 所述发送模块，还用于在接收到来自所述AP设备的EAPOL-Start报文之后，通过所述AP设备向所述客户端发送用于触发所述客户端进行认证的EAPOL-请求Request报文；

[0023] 所述接收模块，还用于接收来自所述客户端的EAPOL-响应Response报文，且所述EAPOL-Response报文中携带所述客户端的认证信息；

[0024] 且所述认证请求报文中还携带所述客户端的认证信息。

[0025] 还包括：处理模块，用于在接收到来自所述AP设备的EAPOL-Start报文之后，在用户表项中记录所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址之间的对应关系；

[0026] 在接收到来自所述客户端的EAPOL-Response报文之后，通过所述EAPOL-Response报文中携带的所述客户端的MAC地址查询所述用户表项，并利用查询结果得到所述客户端对应的AP设备的MAC地址以及所述客户端对应的SSID。

[0027] 本发明提供一种接入点AP设备，应用于包括客户端、所述AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，该AP设备包括：

[0028] 接收模块，用于接收来自所述客户端的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述客户端的介质访问控制MAC地址；

[0029] 处理模块，用于在所述EAPOL-Start报文中添加所述AP设备本身的MAC地址以及所述客户端对应的服务集标识SSID；

[0030] 发送模块，用于将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备；

[0031] 由所述接入设备利用收到的EAPOL-Start报文中携带的信息向所述认证服务器发送认证请求报文，并由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0032] 所述接收模块，还用于接收来自所述接入设备的用于触发所述客户端进行认证的EAPOL-请求Request报文；以及，

[0033] 接收来自所述客户端的EAPOL-响应Response报文，所述EAPOL-Response报文中携带所述客户端的认证信息；

[0034] 所述发送模块，还用于将所述EAPOL-Request报文发送给所述客户端；以及，将所述EAPOL-Response报文发送给所述接入设备。

[0035] 与现有技术相比，本发明至少具有以下优点：本发明中，AP设备通过在EAPOL-Start(开始)报文中携带自身的MAC(Medium Access Control，介质访问控制)地址以及客户端对应的SSID(Service Set Identifier，服务集标识)，使得接入设备可以获知客户端是从哪个AP设备接入的，即接入设备可以精确获取客户端的接入AP设备，从而可以实现对客户端的精确管理和控制。

附图说明

[0036] 图1是现有技术中的802.1X认证系统的结构示意图；

[0037] 图2是现有技术中的基于无线局域网的802.1X认证系统的结构示意图；

[0038] 图3是本发明提出的一种802.1X认证方法流程图；

[0039] 图4是本发明提出的一种接入设备的结构示意图；

[0040] 图5是本发明提出的一种AP设备的结构示意图。

具体实施方式

[0041] 以图2为本发明应用场景示意图，当在接入设备(即二层交换机)上配置了802.1X认证功能时，会下发802.1X协议报文上报未知源MAC地址丢弃规则，客户端在未认证通过时，只有802.1X协议报文送到上层802.1X模块，其他报文会被丢弃；在客户端认证通过后，会下发MAC转发表项，当后续收到报文时，检查MAC转发表项是否存在，如果已经存在，则正常转发报文。

[0042] 在上述图2所示的应用场景下，客户端和AP设备连接成功之后，AP设备只进行报文的转发，因此当认证报文到达接入设备时，接入设备无法确切知道客户端是以无线方式接入还是以有线方式接入，且在以无线方式接入时无法确切知道客户端的具体接入AP设备。

[0043] 针对上述问题，本发明提出一种802.1X认证方法，如图2所示的应用场景示意图，该方法应用于包括客户端、AP设备、接入设备(即二层交换机)和认证服务器的802.1X认证系统中，如图3所示，该方法包括以下步骤：

[0044] 步骤301，客户端向AP设备发送EAPOL-Start报文，且该EAPOL-Start报文中携带客户端的MAC地址。其中，在客户端需要发起802.1X认证时，则客户端会通过AP设备向接入设备发送EAPOL-Start报文。

[0045] 步骤302，AP设备接收来自客户端的EAPOL-Start报文，并在EAPOL-Start报文中添加AP设备本身的MAC地址以及客户端对应的SSID。

[0046] 本发明中，AP设备在接收到基于802.1X协议的EAPOL-Start报文后，可以将AP设备本身的MAC地址以及客户端对应的SSID(即客户端连接的SSID)通过RADIUS格式属性封装到EAPOL-Start报文的载荷中。

[0047] 步骤303，AP设备将携带AP设备的MAC地址、客户端对应的SSID、以及客户端的MAC地址的EAPOL-Start报文发送给接入设备。

[0048] 步骤304，接入设备接收来自AP设备的EAPOL-Start报文，该EAPOL-Start报文中携带AP设备的MAC地址、客户端对应的SSID、客户端的MAC地址。

[0049] 本发明中，接入设备在接收到EAPOL-Start报文之后，可以按照RADIUS属性TLV(Type Length Value，类型长度值)格式对EAPOL-Start报文的载荷内容进行解析，得到AP设备的MAC地址和客户端对应的SSID，以及从该EAPOL-Start报文的报文头中获得客户端的MAC地址，并根据该客户端的MAC地址建立用户表项，以及在用户表项中记录AP设备的MAC地址、客户端对应的SSID、以及客户端的MAC地址之间的对应关系；如表1所示，为用户表项的一种具体实例。

[0050] 表1

[0051]

客户端的MAC	客户端对应的SSID	AP设备的MAC地址
MAC地址1	SSID A	MAC地址B

[0052] 步骤305，接入设备向AP设备发送EAPOL-Request(请求)报文，且该EAPOL-Request报文用于触发客户端进行认证。

[0053] 步骤306，AP设备接收来自接入设备的EAPOL-Request报文，并将该EAPOL-Request报文发送给客户端。

[0054] 步骤307，客户端接收来自AP设备的EAPOL-Request报文，并向AP设备发送EAPOL-Response(响应)报文，且该EAPOL-Response报文中携带客户端的认证信息(如客户端的用户名以及密码等信息)。

[0055] 步骤308，AP设备接收来自客户端的EAPOL-Response报文，并将该EAPOL-Response报文发送给接入设备。

[0056] 步骤309，接入设备接收来自AP设备的EAPOL-Response报文，并向认证服务器发送认证请求报文，且该认证请求报文中携带了AP设备的MAC地址、客户端对应的SSID、以及客户端的MAC地址；此外，在该认证请求报文中还需要携带客户端的认证信息。

[0057] 具体的，接入设备在接收到EAPOL-Response报文之后，可以通过EAPOL-Response报文中携带的客户端的MAC地址查询用户表项，并利用查询结果得到客户端对应的AP设备的MAC地址以及客户端对应的SSID，继而可以通过认证请求报文将AP设备的MAC地址、客户端对应的SSID、客户端的MAC地址、以及客户端的认证信息发送给认证服务器。

[0058] 需要注意的是，在实际应用中，上述认证请求报文可以为RADIUS认证请求报文，且接入设备可以将AP设备的MAC地址以及客户端对应的SSID添加到RADIUS认证请求报文的30号属性的Data(数据)域中。

[0059] 本发明中，在将认证请求报文发送给认证服务器之后，该认证服务器可以利用认证请求报文中携带的信息(AP设备的MAC地址、客户端对应的SSID、客户端的MAC地址、客户端的认证信息)对客户端进行802.1X认证。

[0060] 进一步的，由于认证请求报文中携带了AP设备的MAC地址以及客户端对应的SSID，因此认证服务器可精确知道客户端连接的AP设备以及对应的SSID，且管理员可在认证服务器上配置能够允许接入的AP设备以及SSID，并且可以针对不同AP设备和SSID下发不同的用户权限，比如流量限速，会话时长等，从而可以实现对客户端的精确管理和控制。

[0061] 基于与上述方法同样的发明构思，本发明还提出了一种接入设备，应用于包括客户端、接入点AP设备、所述接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，如图4所示，该接入设备包括：

[0062] 接收模块11，用于接收来自所述AP设备的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述AP设备的介质访问控制MAC地址、所述客户端对应的服务集标识SSID、以及所述客户端的MAC地址；

[0063] 发送模块12，用于向所述认证服务器发送认证请求报文，且所述认证请求报文中携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址；由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0064] 所述发送模块12，还用于在接收到来自所述AP设备的EAPOL-Start报文之后，通过所述AP设备向所述客户端发送用于触发所述客户端进行认证的EAPOL-请求Request报文；

[0065] 所述接收模块11，还用于接收来自所述客户端的EAPOL-响应Response报文，且所述EAPOL-Response报文中携带所述客户端的认证信息；

[0066] 且所述认证请求报文中还携带所述客户端的认证信息。

[0067] 该接入设备还包括：处理模块13，用于在接收到来自所述AP设备的EAPOL-Start报文之后，在用户表项中记录所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址之间的对应关系；

[0068] 在接收到来自所述客户端的EAPOL-Response报文之后，通过所述EAPOL-Response报文中携带的所述客户端的MAC地址查询所述用户表项，并利用查询结果得到所述客户端对应的AP设备的MAC地址以及所述客户端对应的SSID。

[0069] 其中，本发明装置的各个模块可以集成于一体，也可以分离部署。上述模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0070] 基于与上述方法同样的发明构思，本发明还提出了一种接点AP设备，应用于包括客户端、所述AP设备、接入设备和认证服务器的802.1X认证系统中，在所述客户端通过所述AP设备发起802.1X认证时，如图5所示，该AP设备包括：

[0071] 接收模块21，用于接收来自所述客户端的局域网上的可扩展认证协议EAPOL-开始Start报文，且所述EAPOL-Start报文中携带所述客户端的介质访问控制MAC地址；

[0072] 处理模块22，用于在所述EAPOL-Start报文中添加所述AP设备本身的MAC地址以及所述客户端对应的服务集标识SSID；

[0073] 发送模块23，用于将携带所述AP设备的MAC地址、所述客户端对应的SSID、以及所述客户端的MAC地址的EAPOL-Start报文发送给所述接入设备；

[0074] 由所述接入设备利用收到的EAPOL-Start报文中携带的信息向所述认证服务器发送认证请求报文，并由所述认证服务器利用所述认证请求报文中携带的信息对所述客户端进行802.1X认证。

[0075] 所述接收模块21，还用于接收来自所述接入设备的用于触发所述客户端进行认证的EAPOL-请求Request报文；以及，

[0076] 接收来自所述客户端的EAPOL-响应Response报文，所述EAPOL-Response报文中携带所述客户端的认证信息；

[0077] 所述发送模块23，还用于将所述EAPOL-Request报文发送给所述客户端；以及，将所述EAPOL-Response报文发送给所述接入设备。

[0078] 其中，本发明装置的各个模块可以集成于一体，也可以分离部署。上述模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0079] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM，U盘，移动硬盘等)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的方法。

[0080] 本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

[0081] 本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0082] 上述本发明序号仅仅为了描述，不代表实施例的优劣。

[0083] 以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

图1

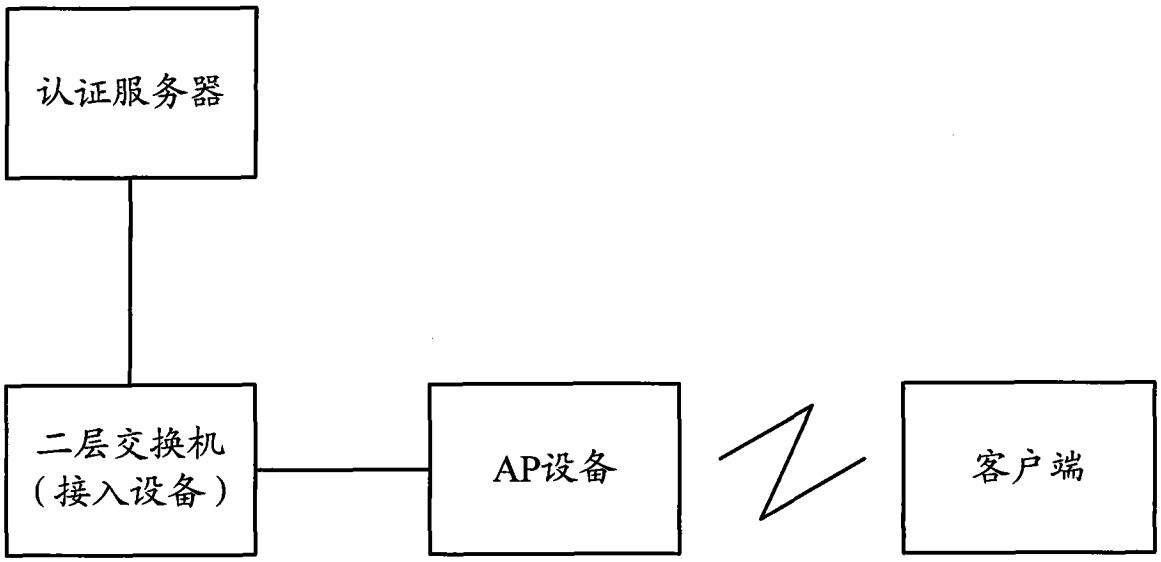

图2

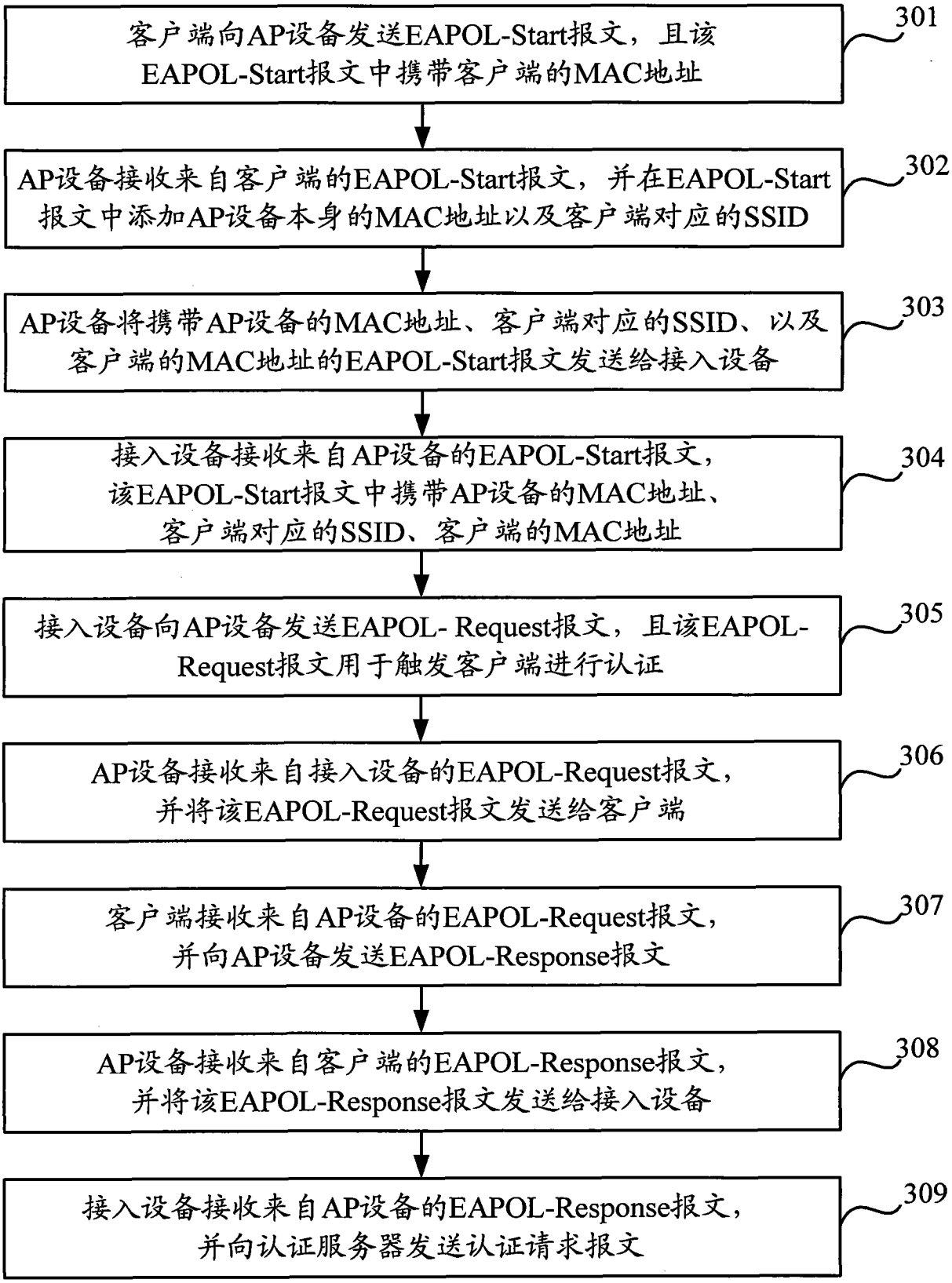
客户端向AP设备发送EAPOL-Start报文，且该EAPOL-Start报文中携带客户端的MAC地址
301
AP设备接收来自客户端的EAPOL-Start报文，并在EAPOL-Start报文中添加AP设备本身的MAC地址以及客户端对应的SSID
302
AP设备将携带AP设备的MAC地址、客户端对应的SSID、以及客户端的MAC地址的EAPOL-Start报文发送给接入设备
303
接入设备接收来自AP设备的EAPOL-Start报文，该EAPOL-Start报文中携带AP设备的MAC地址、客户端对应的SSID、客户端的MAC地址
304
接入设备向AP设备发送EAPOL- Request报文，且该EAPOL-Request报文用于触发客户端进行认证
305
AP设备接收来自接入设备的EAPOL-Request报文，并将该EAPOL-Request报文发送给客户端
306
客户端接收来自AP设备的EAPOL-Request报文，并向AP设备发送EAPOL-Response报文
307
AP设备接收来自客户端的EAPOL-Response报文，并将该EAPOL-Response报文发送给接入设备
308
接入设备接收来自AP设备的EAPOL-Response报文，并向认证服务器发送认证请求报文
309

图3

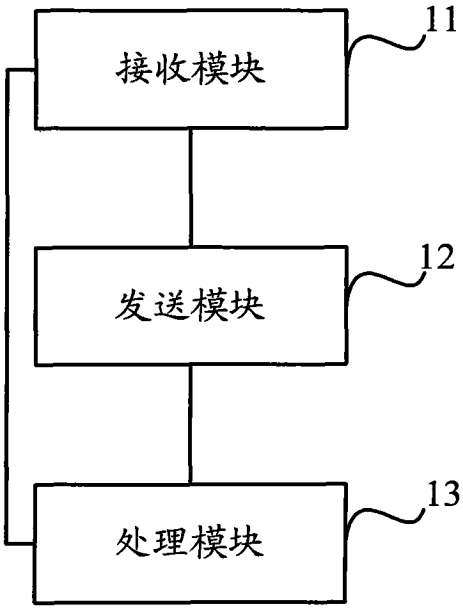

图4

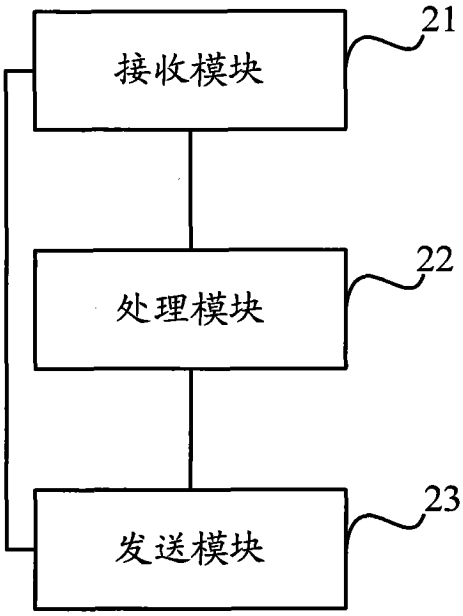

图5