(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 106134143 B
(45)授权公告日 2019.05.21

(21)申请号 201580006463.1

(22)申请日 2015.01.27

(65)同一申请的已公布的文献号
申请公布号 CN 106134143 A

(43)申请公布日 2016.11.16

(30)优先权数据
14/170,474 2014.01.31 US

(85)PCT国际申请进入国家阶段日
2016.07.29

(86)PCT国际申请的申请数据
PCT/US2015/013102 2015.01.27

(87)PCT国际申请的公布数据
WO2015/116593 EN 2015.08.06

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 C·O·特伦 T·R·古丁 R·S·戴利

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/28(2006.01)
H04W 12/06(2006.01)
H04W 12/08(2006.01)
H04W 84/12(2006.01)

(56)对比文件
US 2012317619 A1,2012.12.13,
CN 103441984 A,2013.12.11,
CN 102461272 A,2012.05.16,
US 2008155685 A1,2008.06.26,
US 2006165103 A1,2006.07.27,
CN 102415072 A,2012.04.11,
US 2013318587 A1,2013.11.28,
CN 101931954 A,2010.12.29,
CN 101453409 A,2009.06.10,
US 2013034046 A1,2013.02.07,

审查员 彭帜

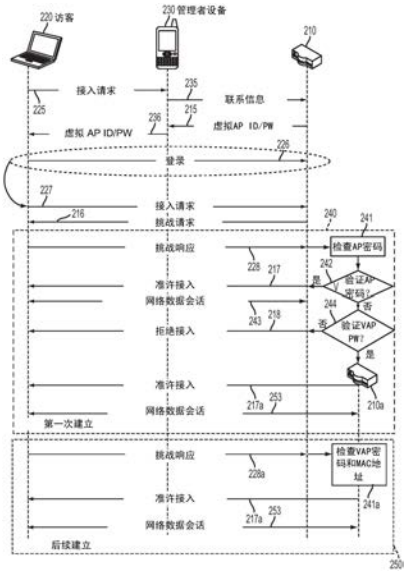
权利要求书8页 说明书21页 附图11页

(54)发明名称

用于动态网络接入管理的方法、设备和系统

(57)摘要

用于通过利用网络密码提供安全的网络接入点来提供针对无线网络的接入的方法和设备可以包括:接收对于在该网络接入点上向设备提供针对无线网络的接入的请求。响应于接收到对于在该网络接入点上向设备提供接入的请求,可以建立虚拟接入点来向该设备提供针对该无线网络的接入。可以为该设备建立虚拟接入点密码,并将其与该设备的唯一标识符进行关联。该虚拟接入点密码可以与网络密码不同。当输入的密码与虚拟接入点密码匹配,并且设备标识符与和该虚拟接入点密码相关联的设备的唯一标识符相匹配时,向该设备提供针对该网络的接入。



CN 106134143 B

1.一种通过利用网络密码提供安全保护的网络接入点来提供到无线网络的接入的方法,所述方法包括:

在所述网络接入点中接收为访客设备提供到所述无线网络的接入的请求;

响应于接收到为所述访客设备提供接入的所述请求,由所述网络接入点建立虚拟接入点来为所述访客设备提供到所述无线网络的接入;

由所述网络接入点为所述访客设备生成与所述访客设备的唯一设备标识符相关联的虚拟接入点密码,其中,所述虚拟接入点密码与所述网络密码不同,其中所述虚拟接入点密码和所述唯一设备标识符各自仅对所述访客设备和所述网络接入点的所述虚拟接入点唯一;

通过在所述虚拟接入点能够访问的数据库中将所述虚拟接入点密码与所述访客设备的所述唯一设备标识符绑定,由所述网络接入点将所述虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述访客设备;以及

当输入的密码与所述虚拟接入点密码匹配,并且所述访客设备的访客设备标识符与所述访客设备的所述唯一设备标识符匹配时,向所述访客设备提供到所述无线网络的接入。

2.根据权利要求1所述的方法,其中,所述访客设备的所述唯一设备标识符包括所述访客设备的媒体访问控制(MAC)地址。

3.根据权利要求1所述的方法,其中,建立所述虚拟接入点包括:

确定是否已达到可用虚拟接入点的限度;以及

响应于确定没有达到可用虚拟接入点的所述限度,建立具有虚拟接入点标识符的所述虚拟接入点。

4.根据权利要求1所述的方法,其中:

所接收的请求包括与所述访客设备相关联的信息;

为所述访客设备生成所述虚拟接入点密码包括:基于与所述访客设备相关联的所述信息,为所述访客设备生成所述虚拟接入点密码并将所述虚拟接入点密码与所述访客设备的虚拟标识符相关联;以及

向所述访客设备提供到所述无线网络的接入包括:在当所输入的密码与所述虚拟接入点密码匹配,并且与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时的第一次接入尝试期间,提供到所述无线网络的临时接入。

5.根据权利要求4所述的方法,还包括:

在所述网络接入点中,从没有请求进行接入的第二访客设备接收第二密码,并在第二访客设备接入尝试中获得与所述第二访客设备相关联的信息;

确定从所述第二访客设备接收的所述第二密码是否与所述网络接入点的所述网络密码或者所述虚拟接入点密码匹配;

响应于识别出从所述第二访客设备接收的所述第二密码与所述网络接入点的所述网络密码或者所述虚拟接入点密码不匹配,向所述无线网络的管理者通知所述第二访客设备接入尝试;

在所述网络接入点中,从所述管理者接收请求所述网络接入点向所述第二访客设备提供到所述无线网络的接入的消息;

由所述网络接入点基于与所述第二访客设备相关联的所述信息,为所述第二访客设备

生成与所述第二访客设备的第二虚拟标识符相关联的第二虚拟接入点密码，其中，所述第二虚拟接入点密码与所述网络密码和所述访客设备的所述虚拟接入点密码不同，其中所述第二虚拟接入点密码和所述第二虚拟标识符各自仅对所述第二访客设备唯一；以及

通过在所述数据库中将所述第二虚拟接入点密码与所述第二访客设备的所述第二虚拟标识符绑定，由所述网络接入点将所述第二虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述第二访客设备。

6.根据权利要求4所述的方法，还包括：

建立与所述虚拟接入点相关联的虚拟接入点标识符；

向所述访客设备提供所述虚拟接入点标识符和所述虚拟接入点密码；

在所述虚拟接入点可访问的所述数据库中，存储所述虚拟接入点标识符和所述虚拟接入点密码；

在所述访客设备使用所述虚拟接入点标识符和所述虚拟接入点密码进行的所述第一次接入尝试期间，获得所述访客设备的所述唯一设备标识符；以及

在所述虚拟接入点可访问的所述数据库中，关联于所述虚拟接入点标识符和所述虚拟接入点密码来存储所述访客设备的所述唯一设备标识符，

其中，当获得所述唯一设备标识符时，向所述访客设备提供到所述无线网络的接入包括：在以下情形的后续接入尝试中，向所述访客设备提供到所述无线网络的接入：当所述访客设备使用所述虚拟接入点标识符来接入所述虚拟接入点时，当所输入的密码与所述虚拟接入点密码匹配时，以及当所述访客设备的所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时。

7.根据权利要求6所述的方法，其中，响应于接收到为所述访客设备提供接入的所述请求，建立所述虚拟接入点来为所述访客设备提供到所述无线网络的接入包括：

当在所述第一次接入尝试期间，与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时，建立所述虚拟接入点；以及

当在所述第一次接入尝试之后的后续接入尝试期间，所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时，建立所述虚拟接入点。

8.根据权利要求6所述的方法，其中：

建立所述虚拟接入点包括：建立关于所述访客设备对所述无线网络的接入的限制；以及

在当所输入的密码与所述虚拟接入点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时的后续接入尝试中，向所述访客设备提供到所述无线网络的接入包括：当所输入的密码与所述虚拟接入点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络受到所述限制的接入。

9.一种用于提供到利用网络密码提供安全保护的无线网络的接入的网络接入点，所述网络接入点包括：

配置为访问在非暂时性计算机可读介质上存储的处理器可读指令，以执行包括以下各

项的操作的处理器：

接收为访客设备提供到所述无线网络的接入的请求；

响应于接收到为所述访客设备提供接入的所述请求，建立虚拟接入点来为所述访客设备提供到所述无线网络的接入；

为所述访客设备生成与所述访客设备的唯一设备标识符相关联的虚拟接入点密码，其中，所述虚拟接入点密码与所述网络密码不同，其中所述虚拟接入点密码和所述唯一设备标识符各自仅对所述访客设备和所述网络接入点的所述虚拟接入点唯一；

通过在所述虚拟接入点能够访问的数据库中将所述虚拟接入点密码与所述访客设备的所述唯一设备标识符绑定，将所述虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述访客设备；以及

当输入的密码与所述虚拟接入点密码匹配，并且所述访客设备的访客设备标识符与所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络的接入。

10.根据权利要求9所述的网络接入点，其中，所述处理器配置有处理器可执行指令来执行操作，使得所述访客设备的所述唯一设备标识符包括所述访客设备的媒体访问控制(MAC)地址。

11.根据权利要求9所述的网络接入点，其中，所述处理器配置有处理器可执行指令来执行操作，使得建立所述虚拟接入点包括：

确定是否已达到可用虚拟接入点的限度；以及

响应于确定没有达到可用虚拟接入点的所述限度，建立具有虚拟接入点标识符的所述虚拟接入点。

12.根据权利要求9所述的网络接入点，其中：

所接收的请求包括与所述访客设备相关联的信息；

所述处理器配置有处理器可执行指令来执行操作，使得：

为所述访客设备生成所述虚拟接入点密码包括：基于与所述访客设备相关联的所述信息，为所述访客设备生成所述虚拟接入点密码并将所述虚拟接入点密码与所述访客设备的虚拟标识符相关联；以及

向所述访客设备提供到所述无线网络的接入包括：在当所输入的密码与所述虚拟接入点密码匹配，并且与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时的第一次接入尝试期间，提供到所述无线网络的临时接入。

13.根据权利要求12所述的网络接入点，其中，所述处理器配置有处理器可执行指令来执行操作，所述操作还包括：

在所述网络接入点中，从没有请求进行接入的第二访客设备接收第二密码，并在第二访客设备接入尝试中获得与所述第二访客设备相关联的信息；

确定从所述第二访客设备接收的所述第二密码是否与所述网络接入点的所述网络密码或者所述虚拟接入点密码匹配；

响应于识别出从所述第二访客设备接收的所述第二密码与所述网络接入点的所述网络密码或者所述虚拟接入点密码不匹配，向所述无线网络的管理者通知所述第二访客设备接入尝试；

在所述网络接入点中，从所述管理者接收请求所述网络接入点向所述第二访客设备提

供到所述无线网络的接入的消息；

由所述网络接入点基于与所述第二访客设备相关联的所述信息，为所述第二访客设备生成与所述第二访客设备的第二虚拟标识符相关联的第二虚拟接入点密码，其中，所述第二虚拟接入点密码与所述网络密码和所述访客设备的所述虚拟接入点密码不同，其中所述第二虚拟接入点密码和所述第二虚拟标识符各自仅对所述第二访客设备唯一；以及

通过在所述数据库中将所述第二虚拟接入点密码与所述第二访客设备的所述第二虚拟标识符绑定，将所述第二虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述第二访客设备。

14.根据权利要求12所述的网络接入点，其中，所述处理器配置有处理器可执行指令，以执行还包括以下各项的操作：

建立与所述虚拟接入点相关联的虚拟接入点标识符；

向所述访客设备提供所述虚拟接入点标识符和所述虚拟接入点密码；

在所述虚拟接入点可访问的所述数据库中，存储所述虚拟接入点标识符和所述虚拟接入点密码；

在所述访客设备使用所述虚拟接入点标识符和所述虚拟接入点密码进行的所述第一次接入尝试期间，获得所述访客设备的所述唯一设备标识符；以及

在所述虚拟接入点可访问的所述数据库中，关联于所述虚拟接入点标识符和所述虚拟接入点密码来存储所述访客设备的所述唯一设备标识符，

其中，所述处理器配置有处理器可执行指令来执行操作，使得当获得所述唯一设备标识符时，向所述访客设备提供到所述无线网络的接入包括：在以下情形的后续接入尝试中，向所述访客设备提供到所述无线网络的接入：当所述访客设备使用所述虚拟接入点标识符来接入所述虚拟接入点时，当所输入的密码与所述虚拟接入点密码匹配时，以及当所述访客设备的所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时。

15.根据权利要求14所述的网络接入点，其中，所述处理器配置有处理器可执行指令来执行操作，使得响应于接收到为所述访客设备提供接入的所述请求，建立所述虚拟接入点来为所述访客设备提供到所述无线网络的接入包括：

当在所述第一次接入尝试期间，与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时，建立所述虚拟接入点；以及

当在所述第一次接入尝试之后的后续接入尝试期间，所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时，建立所述虚拟接入点。

16.根据权利要求14所述的网络接入点，其中，所述处理器配置有处理器可执行指令来执行操作，使得：

建立所述虚拟接入点包括：建立关于所述访客设备到所述无线网络的接入的限制；以及

在当所输入的密码与所述虚拟接入点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时的后续接入尝试中，向所述访客设备提供到所述无线网络的接入包括：当所输入的密码与所述虚拟接入

点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络受到所述限制的接入。

17.一种用于通过利用网络密码提供安全保护的网络接入点来提供到无线网络的接入的装置，所述装置包括：

用于在所述网络接入点中接收为访客设备提供到所述无线网络的接入的请求的单元；

用于响应于接收到为所述访客设备提供接入的所述请求，由所述网络接入点建立虚拟接入点来为所述访客设备提供到所述无线网络的接入的单元；

用于由所述网络接入点为所述访客设备生成与所述访客设备的唯一设备标识符相关联的虚拟接入点密码的单元，其中，所述虚拟接入点密码与所述网络密码不同，其中所述虚拟接入点密码和所述唯一设备标识符各自仅对所述访客设备和所述网络接入点的所述虚拟接入点唯一；

用于通过在所述虚拟接入点能够访问的数据库中将所述虚拟接入点密码与所述访客设备的所述唯一设备标识符绑定，由所述网络接入点将所述虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述访客设备的单元；以及

用于当输入的密码与所述虚拟接入点密码匹配，并且访客设备标识符与所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络的接入的单元。

18.根据权利要求17所述的装置，其中，所述访客设备的所述唯一设备标识符包括所述访客设备的媒体访问控制(MAC)地址。

19.根据权利要求17所述的装置，其中，用于建立所述虚拟接入点的单元包括：

用于确定是否已达到可用虚拟接入点的限度的单元；以及

用于响应于确定没有达到可用虚拟接入点的所述限度，建立具有虚拟接入点标识符的所述虚拟接入点的单元。

20.根据权利要求17所述的装置，其中：

所接收的请求包括与所述访客设备相关联的信息；

用于为所述访客设备生成所述虚拟接入点密码的单元包括：用于基于与所述访客设备相关联的所述信息，为所述访客设备生成所述虚拟接入点密码并将所述虚拟接入点密码与所述访客设备的虚拟标识符相关联的单元；以及

用于向所述访客设备提供到所述无线网络的接入的单元包括：用于在当所输入的密码与所述虚拟接入点密码匹配，并且与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时的第一次接入尝试期间，提供到所述无线网络的临时接入的单元。

21.根据权利要求20所述的装置，还包括：

用于在所述网络接入点中，从没有请求进行接入的第二访客设备接收第二密码，并在第二访客设备接入尝试中获得与所述第二访客设备相关联的信息的单元；

用于确定从所述第二访客设备接收的所述第二密码是否与所述网络接入点的所述网络密码或者所述虚拟接入点密码匹配的单元；

用于响应于识别出从所述第二访客设备接收的所述第二密码与所述网络接入点的所述网络密码或者所述虚拟接入点密码不匹配，向所述无线网络的管理者通知所述第二访客设备接入尝试的单元；

用于在所述网络接入点中，从所述管理者接收请求所述网络接入点向所述第二访客设备提供到所述无线网络的接入的消息的单元；

用于由所述网络接入点基于与所述第二访客设备相关联的所述信息，为所述第二访客设备生成与所述第二访客设备的第二虚拟标识符相关联的第二虚拟接入点密码的单元，其中，所述第二虚拟接入点密码与所述网络密码和所述访客设备的所述虚拟接入点密码不同，其中所述第二虚拟接入点密码和所述第二虚拟标识符各自仅对所述第二访客设备唯一；以及

用于通过在所述数据库中将所述第二虚拟接入点密码与所述第二访客设备的所述第二虚拟标识符绑定，将所述第二虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述第二访客设备的单元。

22.根据权利要求20所述的装置，还包括：

用于建立与所述虚拟接入点相关联的虚拟接入点标识符的单元；

用于向所述访客设备提供所述虚拟接入点标识符和所述虚拟接入点密码的单元；

用于在所述虚拟接入点可访问的所述数据库中，存储所述虚拟接入点标识符和所述虚拟接入点密码的单元；

用于在所述访客设备使用所述虚拟接入点标识符和所述虚拟接入点密码进行的所述第一次接入尝试期间，获得所述访客设备的唯一设备标识符的单元；以及

用于在所述虚拟接入点可访问的所述数据库中，关联于所述虚拟接入点标识符和所述虚拟接入点密码来存储所述访客设备的所述唯一设备标识符的单元，

其中，用于向所述访客设备提供到所述无线网络的接入的单元包括：用于在以下情形时，向所述访客设备提供到所述无线网络的接入的单元：当所述访客设备使用所述虚拟接入点标识符来接入所述虚拟接入点时，当所输入的密码与所述虚拟接入点密码匹配时，以及当所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时。

23.根据权利要求22所述的装置，其中，用于响应于接收到提供到所述无线网络的接入的所述请求，建立所述虚拟接入点为向所述访客设备提供到所述无线网络的接入的单元包括：

用于当在所述第一次接入尝试期间，与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时，建立所述虚拟接入点的单元；以及

用于当在所述第一次接入尝试之后的后续接入尝试期间，所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时，建立所述虚拟接入点的单元。

24.根据权利要求22所述的装置，其中：

用于建立所述虚拟接入点的单元包括：用于建立关于所述访客设备到所述无线网络的接入的限制的单元；以及

用于在当所输入的密码与所述虚拟接入点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时的后续接入尝试中，向所述访客设备提供到所述无线网络的接入的单元包括：用于当所输入的密码与所述虚拟接入点密码匹配，并且所述访客设备标识符与关联于所述虚拟接入点密码进行

存储的所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络受到所述限制的接入的单元。

25.一种其上存储有处理器可执行指令的非临时性计算机可读介质，其中，所述处理器可执行指令被配置为使处理器执行包括以下各项的操作：

在网络接入点中，接收为访客设备提供到无线网络的接入的请求；

响应于接收到为所述访客设备提供接入的所述请求，由所述网络接入点建立虚拟接入点来为所述访客设备提供到所述无线网络的接入；

由所述网络接入点为所述访客设备生成与所述访客设备的唯一设备标识符相关联的虚拟接入点密码，其中，所述虚拟接入点密码与所述网络密码不同，其中所述虚拟接入点密码和所述唯一设备标识符各自仅对所述访客设备和所述网络接入点的所述虚拟接入点唯一；

通过在所述虚拟接入点能够访问的数据库中将所述虚拟接入点密码与所述访客设备的所述唯一设备标识符绑定，由所述网络接入点将所述虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述访客设备；以及

当输入的密码与所述虚拟接入点密码匹配，并且所述访客设备的访客设备标识符与所述访客设备的所述唯一设备标识符匹配时，向所述访客设备提供到所述无线网络的接入。

26.根据权利要求25所述的非临时性计算机可读介质，其中：

所接收的请求包括与所述访客设备相关联的信息；

所存储的处理器可执行指令被配置为使所述处理器执行操作，使得：

为所述访客设备生成所述虚拟接入点密码包括：基于与所述访客设备相关联的所述信息，为所述访客设备生成所述虚拟接入点密码并将所述虚拟接入点密码与所述访客设备的虚拟标识符相关联；以及

向所述访客设备提供到所述无线网络的接入包括：在当所输入的密码与所述虚拟接入点密码匹配，并且与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时的第一次接入尝试期间，提供到所述无线网络的临时接入。

27.根据权利要求26所述的非临时性计算机可读介质，其中，所存储的处理器可执行指令被配置为使所述处理器执行操作，所述操作还包括：

在所述网络接入点中，从没有请求进行接入的第二访客设备接收第二密码，并在第二访客设备接入尝试中获得与所述第二访客设备相关联的信息；

确定从所述第二访客设备接收的所述第二密码是否与所述网络接入点的所述网络密码或者所述虚拟接入点密码匹配；

响应于识别出从所述第二访客设备接收的所述第二密码与所述网络接入点的所述网络密码或者所述虚拟接入点密码不匹配，向所述无线网络的管理者通知所述第二访客设备接入尝试；

在所述网络接入点中，从所述管理者接收请求所述网络接入点向所述第二访客设备提供到所述无线网络的接入的消息；

由所述网络接入点基于与所述第二访客设备相关联的所述信息，为所述第二访客设备生成与所述第二访客设备的第二虚拟标识符相关联的第二虚拟接入点密码，其中，所述第二虚拟接入点密码与所述网络密码和所述访客设备的所述虚拟接入点密码不同，其中所述

第二虚拟接入点密码和所述第二虚拟标识符各自仅对所述第二访客设备唯一;以及

通过在所述数据库中将所述第二虚拟接入点密码与所述第二访客设备的所述第二虚拟标识符绑定,由所述网络接入点将所述第二虚拟接入点密码为了获得经由所述虚拟接入点到所述无线网络的接入的使用限制到仅仅所述第二访客设备。

28.根据权利要求26所述的非临时性计算机可读介质,其中,所存储的处理器可执行指令被配置为使所述处理器执行还包括以下各项的操作:

建立与所述虚拟接入点相关联的虚拟接入点标识符;

向所述访客设备提供所述虚拟接入点标识符和所述虚拟接入点密码;

在所述虚拟接入点可访问的所述数据库中,存储所述虚拟接入点标识符和所述虚拟接入点密码;

在所述访客设备使用所述虚拟接入点标识符和所述虚拟接入点密码进行的所述第一次接入尝试期间,获得所述访客设备的所述唯一设备标识符;以及

在所述虚拟接入点可访问的所述数据库中,关联于所述虚拟接入点标识符和所述虚拟接入点密码来存储所述访客设备的所述唯一设备标识符,

其中,所存储的处理器可执行指令被配置为使处理器执行操作,使得当获得所述唯一设备标识符时,向所述访客设备提供到所述无线网络的接入包括:在以下情形的后续接入尝试中,向所述访客设备提供到所述无线网络的接入:当所述访客设备使用所述虚拟接入点标识符来接入所述虚拟接入点时,当所输入的密码与所述虚拟接入点密码匹配时,以及当所述访客设备的访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时。

29.根据权利要求28所述的非临时性计算机可读介质,其中,所存储的处理器可执行指令被配置为使所述处理器执行操作,使得响应于接收到为所述访客设备提供接入的所述请求,建立所述虚拟接入点来向所述访客设备提供到所述无线网络的接入包括:

当在所述第一次接入尝试期间,与所述访客设备相关联的所述信息与所述访客设备的所述虚拟标识符匹配时,建立所述虚拟接入点;以及

当在所述第一次接入尝试之后的后续接入尝试期间,所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时,建立所述虚拟接入点。

30.根据权利要求28所述的非临时性计算机可读介质,其中,所存储的处理器可执行指令被配置为使所述处理器执行操作,使得:

建立所述虚拟接入点包括:建立关于所述访客设备到所述无线网络的接入的限制;以及

在当所输入的密码与所述虚拟接入点密码匹配,并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时的后续接入尝试中,向所述访客设备提供到所述无线网络的接入包括:当所输入的密码与所述虚拟接入点密码匹配,并且所述访客设备标识符与关联于所述虚拟接入点密码进行存储的所述访客设备的所述唯一设备标识符匹配时,向所述访客设备提供到所述无线网络受到所述限制的接入。

用于动态网络接入管理的方法、设备和系统

[0001] 相关申请的交叉引用

[0002] 本申请要求享受2014年1月31日向美国专利商标局提交的美国非临时专利申请No.14/170,474的优先权和利益，故以引用方式将该申请的全部内容并入本文。

背景技术

[0003] 常规的无线网络接入点(AP)、路由器、网桥或者类似的接入设备向一个或多个客户端提供针对根据各种标准或协议(例如，802.11a、802.11g等等)配置的无线网络(例如，WiFi网络)的接入。网络接入点可以向计算设备提供针对该网络上的其它节点(例如，连接到家庭网络的计算设备和外围设备)的接入。网络接入点还可以例如通过与该网络接入点相关联的服务提供商，向通信设备提供针对互联网的接入。

[0004] 网络接入点可以被配置为进行开放接入或者共享密钥接入。对于开放接入网络而言，通信设备可以通过发现或者了解网络的名称或者服务集标识符(SSID)，经由网络接入点来自由地获得针对网络的接入。在开放接入网络中，通信设备可以与网络接入点进行关联，并在无需输入密码的情况下直接接入网络。对于被配置为进行开放接入的网络接入点而言，位于无线范围之内的任何客户端可以通过向该网络接入点发送连接请求(例如，使用用于该网络接入点或者网络的SSID)，获得针对该网络的接入。通常，该网络接入点允许以开放接入操作模式来与网络进行关联。

[0005] 在共享密钥网络中，仅仅在通信设备成功地提交共享密钥或者密码之后，其才可以通过网络接入点来获得针对该网络的接入。如果网络接入点确认该提交的密钥或者密码是正确的，则同意该通信设备接入该网络。对于被配置为进行共享密钥接入的接入点而言，可以利用密码或者加密密钥，对网络接入点和通信设备之间的无线通信链路进行加密，在客户端初始连接到网络接入点和网络时，可以输入该密码或者加密密钥，或者在稍后的时间使用该密钥的存储版本。在共享密钥接入配置模式下，可以使用共享密钥，对网络接入点和通信设备之间发送的分组或者帧进行加密和解密。因此，为了使网络接入点能够对从通信设备接收的分组或者帧进行处理，该通信设备必须使用正确的加密密钥。

[0006] 当安装新的网络接入点设备时，其可以被配置为通过设置密码来进行共享密钥接入，其中该密码通常是用于表示该共享密钥的单一密码。分配该密码的人员可以充当为该网络接入点以及因此该网络的“管理者”。由于仅仅使用单一密钥来进行接入，因此尝试使用该单一密钥通过网络接入点来获得针对该网络的接入的任何设备可以被同意接入。由于该密码并不与任何特定的接入设备相关联，因此能够潜在地接入该网络的设备的数量仅仅受限于用于对该共享密钥或者密码的分发进行控制的能力。因此，知道密码的任何人员都可以通过在设备和网络接入点之间的接入过程期间正确地输入密码，来获得针对该网络的接入，而不管他们正在使用的是什么通信设备。

[0007] 但是，当向需要网络接入的访客分发密码时，可能出现安全漏洞。目前，用于提供访客接入的唯一选项之一是向访客提供网络密码。因此，根据设计方案，在密码和任何特定设备之间不存在关联，访客可以将密码给予其他人，这些人随后可以使用他们的设备来接

入网络。因此，当向不同于管理者的甚至一个人分发密码时，存在着无意透露该密码的风险。当该密码变得广泛分布时，接入控制和网络安全可能受到影响。

[0008] 为了解决该安全风险，系统管理者可以定期地改变密码。但是，必须将新密码重新分发给合法的或者期望的访客，故可能会重复发生密码的无意分发和潜在的安全受损的循环。用于避免泄漏主接入点密码的其它选项可以涉及建立具有访客密码的访客帐户或者多个帐户。这种处理是高成本的、复杂的、耗时且不可靠的，这是由于配置网络接入点硬件来支持另外的服务集标识符(SSID)或者使用另外的网络接入点可能是必须的。即使建立单独的访客接入，也会出现关于该访客帐户的相同问题，这是由于该访客密码可能要分发给其他随后获得对该网络的接入的人员。

发明内容

[0009] 各个实施例包括针对经由利用网络密码提供安全的网络接入点，来提供针对无线网络的接入的方法和设备。一种实施例方法可以包括：接收对于在网络接入点上向访客设备提供针对该无线网络的接入的请求；响应于接收到对于在该网络接入点上向该访客设备提供接入的请求，建立虚拟接入点来向该访客设备提供针对该无线网络的接入；为该访客设备建立与该访客设备的唯一设备标识符相关联的与所述网络密码不同的虚拟接入点密码；以及当输入的密码与虚拟接入点密码匹配，并且该访客设备的访客设备标识符与和该虚拟接入点密码相关联的访客设备的唯一标识符相匹配时，向该访客设备提供针对该网络的接入。

[0010] 在一种实施例方法中，所接收的请求包括与访客设备相关联的信息。一种实施例方法还可以包括：通过基于与该访客设备相关联的信息，为该访客设备建立与该访客设备的虚拟标识符相关联的虚拟接入点密码，来为访客设备建立虚拟接入点密码。一种实施例方法还可以包括：通过在输入的密码与虚拟接入点密码匹配，并且与该访客设备相关联的信息与和该虚拟接入点密码相关联的访客设备的虚拟标识符相匹配时的第一次接入尝试期间提供针对该网络的接入，来向访客设备提供针对该网络的接入。

[0011] 一种实施例方法还可以包括：建立与虚拟接入点相关联的虚拟接入点标识符；向访客设备提供该虚拟接入点标识符和虚拟接入点密码；在虚拟接入点可访问的数据库中，存储该虚拟接入点标识符和虚拟接入点密码；在访客设备使用该虚拟接入点标识符和虚拟接入点密码进行的第一次接入尝试期间，获得该访客设备的唯一设备标识符；在虚拟接入点可访问的数据库中，关联于该虚拟接入点标识符和虚拟接入点密码来存储该访客设备的唯一设备标识符。在另外的实施例方法中，当已获得该唯一标识符时，向访客设备提供针对网络的接入可以包括：在以下情形的后续接入尝试中，向访客设备提供针对该网络的接入：当访客设备使用该虚拟接入点标识符来接入虚拟接入点时，当输入的密码与该虚拟接入点密码匹配时，以及当该访客设备的访客设备标识符与关联于该虚拟接入点密码而存储的访客设备的唯一设备标识符相匹配时。在另外的实施例方法中，访客设备的唯一标识符可以包括访客设备的媒体访问控制(MAC)地址。

[0012] 在另外的实施例方法中，为访客设备建立与该访客设备的虚拟标识符相关联的虚拟接入点密码可以包括：在网络接入点中，从没有请求进行接入的第二访客设备接收密码，并在接入尝试中获得与第二访客设备相关联的信息；确定从第二访客设备接收的所接收密

码是否与该网络接入点的网络密码和虚拟接入点密码中的一个相匹配;响应于识别出从第二访客设备接收的密码与该网络接入点的网络密码和虚拟接入点密码中的一个不匹配,向网络的管理者通知第二访客设备接入尝试;在网络接入点中,从网络管理者接收用于请求该网络接入点向第二访客设备提供针对该网络的接入的消息;基于与第二访客设备相关联的信息,为第二访客设备建立与第二访客设备的第二虚拟标识符相关联的第二虚拟接入点密码,其中,第二虚拟接入点密码与所述网络密码不同;以及在包括第二访客设备的第二虚拟标识符的数据记录中,存储所建立的针对第二访客设备的第二虚拟接入点密码。在另外的实施例方法中,响应于接收到对于在网络接入点上向访客设备提供接入的请求,建立虚拟接入点来向该访客设备提供针对无线网络的接入可以包括:当在第一次接入尝试期间,与访客设备相关联的信息与该访客设备的虚拟标识符相匹配时,建立虚拟接入点;当在第一次接入尝试之后的后续接入尝试期间,访客设备标识符与关联于所述虚拟接入点密码而存储的访客设备的唯一设备标识符相匹配时,建立虚拟接入点。

[0013] 在另外的实施例方法中,建立虚拟接入点可以包括:确定是否已达到可用虚拟接入点的限度;以及建立虚拟接入点可以包括:响应于确定没有达到可用虚拟接入点的限度,建立具有虚拟接入点标识符的虚拟接入点。在另外的实施例方法中,建立虚拟接入点可以包括:建立关于该访客设备针对该无线网络的接入的限制;在输入的密码与虚拟接入点密码匹配,并且访客设备标识符与关联于所述虚拟接入点密码而存储的访客设备的唯一设备标识符相匹配时的后续接入尝试中向访客设备提供针对所述网络的接入可以包括:当输入的密码与虚拟接入点密码匹配,并且访客设备标识符与关联于该虚拟接入点密码而存储的访客设备的唯一设备标识符相匹配时,向访客设备提供受到(subject to)限制的、针对所述网络的接入。

[0014] 另外的实施例包括具有处理器或者一些处理器的装置,其中该处理器配置有处理器可执行指令以执行上面所描述的方法的操作。另外的实施例包括一种装置,该装置具有用于执行上面所描述的方法的功能的单元。另外的实施例包括一种非临时性处理器可读存储介质,其中,在该非临时性处理器可读存储介质上存储有被配置为使处理器执行上面所描述的方法的操作的处理器可执行指令。

附图说明

[0015] 被并入本文并且构成本说明书一部分的附图示出了本发明的示例性实施例,并且连同上面给出的概括描述以及下面给出的详细描述一起来解释本发明的特征。

[0016] 图1A是示出包括网络、接入点和接入设备的示例性通信网络的通信系统框图。

[0017] 图1B是示出接入设备、接入点和一个或多个网络之间与接入有关的消息传送的消息流图。

[0018] 图1C是具有另外的处理流程框图和用户界面图的消息流图,其示出了在示例性接入尝试期间,与接入有关的消息流、过程和示例性用户界面消息和密码或者密钥输入屏幕。

[0019] 图2A是示出一种示例性通信网络的通信系统框图,其中该示例性通信网络包括适合于结合各个实施例使用的网络、接入点、管理者设备和访客设备。

[0020] 图2B是根据一个实施例,示出访客设备、网络管理者设备和接入点之间的示例性消息交换,以便使用虚拟接入点来提供访客接入的消息流图。

[0021] 图3A是用于示出适合于结合各个实施例使用的虚拟接入点表参数的表。

[0022] 图3B是用于示出适合于结合各个实施例使用的媒体访问控制(MAC)地址用户表参数的表。

[0023] 图3C是用于示出虚拟接入点表参数和MAC地址用户表参数之间的关联的表。

[0024] 图4A是用于示出对访客接入的请求进行处理,并建立虚拟接入点的实施例方法的处理流程图。

[0025] 图4B是用于示出使用虚拟接入点来提供访客接入的实施例方法的处理流程图。

[0026] 图5是用于示出适合于实现各个实施例的示例性移动设备的框图。

[0027] 图6是用于示出适合于实现各个实施例的示例性移动计算设备的框图。

具体实施方式

[0028] 现在参照附图来详细地描述各个实施例。在可以的地方,贯穿附图使用相同的附图标记来指代相同或者类似的部件。对于特定示例和实现方式的引用只是用于说明目的,而不是旨在限制本发明或者权利要求的保护范围。

[0029] 如本文所使用的术语“设备”、“计算设备”、“访客设备”、“网络管理者设备”可以指代下面中的任何一项或者全部:蜂窝电话、智能电话、个人或移动多媒体播放器、个人数据助理(PDA)、膝上型计算机、桌面型计算机、平板计算机、智能本、掌上计算机、无线电子邮件接收机、具备多媒体互联网功能的蜂窝电话、电视、智能TV、智能TV机顶(buddy)盒、集成智能TV、流媒体播放器、智能有线电视盒、机顶盒、数字录像机(DVR)、数字媒体播放器、以及包括可编程处理器的类似个人电子设备、特别是包括SoC的那些电子设备。

[0030] 本文所使用的术语“接入点”(附图中的“AP”)指代下面中的任何一个或者全部:无线接入点、无线路由器、无线接入点中继器、无线接入点距离扩展器、网桥、这些设备的组合、或者用于向客户端提供针对于网络的接入的其它设备,其中该网络根据诸如WiFi协议(例如,在802.11协议的各种版本之下)之类的无线协议进行操作,包括基于密码的安全认证配置。接入点还可以提供针对私人网络和/或服务提供商的进一步接入,以接入诸如互联网之类的公共网络或者公共网络和私人网络的组合。本文将接入点描述成无线的,以及提供针对诸如家庭网络或者私人局域网之类的局域网(LAN)或无线LAN(WLAN)的无线接入。但是,接入点还可以支持与网络的有线连接。

[0031] 如本文所使用的,术语“通信设备”和“设备”指代具有诸如无线网络收发机(例如,WiFi收发机)之类的网络接入电路的任何类型的计算或者通信设备,其中无线网络收发机被配置为与接入点进行通信。通信设备的一些非限制性例子包括智能电话、膝上型计算机、平板计算机、具备网络能力的电视、以及具备无线能力的电器。如本文所使用的,术语“访客设备”指代在没有适当的密码的情况下,连接或者尝试连接到接入点的通信设备,该计算设备的用户不知道该网络接入点密码。如本文所使用的,术语“网络管理者设备”指代接入点的管理者或者所有者可以使用的通信设备。

[0032] 当通信设备尝试在没有适当的密码的情况下,通过接入点来接入常规的安全的无线网络时,网络接入点将拒绝针对该网络的接入。网络管理者(其可以是无线网络的所有者)可以向该网络管理者希望向其提供接入的访客提供网络密钥或者密码。但是,如上面所提及的,向访客提供密码增加了网络受到损害的风险。

[0033] 这些问题可以通过各个实施例来克服,其中这些实施例通过虚拟接入点(其使用访客输入的虚拟接入点密码)和批准的访客设备的设备特定标识符的方式,来向管理者批准的访客设备提供针对安全的无线网络的接入。例如,网络接入点可以基于管理者发送的请求,来建立或者实例化虚拟接入点。该虚拟接入点可以使访客能够获得针对无线网络(其使用被配置为通过共享密钥或者密码进行安全接入的网络接入点来实现安全)的接入,而无需向访客透露该密钥或者密码。替代地,虚拟接入点的标识符和专用虚拟接入点密码可以是基于下面内容来针对访客设备所建立的:限制该虚拟接入点密码的使用的信息,以及经由其MAC或者其它唯一标识符来向访客设备说明通过虚拟接入点标识符标识的虚拟接入点。用此方式,由于访客使用的虚拟接入点密码对于其它通信设备来说是无用的,从而消除了该虚拟接入点密码的广泛分发的风险,因此维持了网络安全。

[0034] 在一个实施例中,访客设备可以在网络管理者先前没有进行请求的情况下,尝试进行接入。在该情形下,当访客设备通过输入与该网络的正确密码不匹配的密码,或者与虚拟接入点密码不匹配的密码来尝试接入该网络接入点时,该访客接入尝试可以充当为请求或者使得网络管理者进行请求。关于访客设备的接入尝试的信息(其包括关于该访客设备能够帮助网络管理者来识别该设备或者设备用户的信息)可以被网络接入点进行捕获,并被转发给网络管理者。替代地,该信息可以由访客设备基于来自网络接入点的查询来提供或者补充,并随后被转发给网络管理者。

[0035] 当网络管理者批准该请求时,可以将该批准发送给网络接入点。该批准可以使得如本文所描述地建立虚拟接入点和虚拟接入点密码,或者稍后在发现期间来建立该虚拟接入点。换言之,在访客设备尝试使用非匹配的密码来接入本网络的第一时间,网络接入点将不能识别该密码,因此可以通知网络管理者,并查询是否应当允许该访客设备接入。

[0036] 如果网络管理者批准接入(例如,通过按下在网络管理者的设备上显示的用户界面上的虚拟键),则将该批准传输给网络接入点(可能与关于该访客设备的另外信息一起传输)。用此方式,访客接入尝试作用为使得进行所述请求。响应于该请求,网络接入点可以基于该请求和该访客设备的标识信息,来生成虚拟接入点和虚拟接入点密码。当访客在后续的消息中接收到虚拟接入点密码和虚拟接入点标识符时,可以使用所建立的虚拟接入点密码来进行后续的接入尝试。当使用正确的虚拟接入点密码和关于该访客设备的信息来进行后续的接入尝试时,可以获得该访客设备的唯一标识符,该唯一标识符与虚拟接入点密码绑定在一起,如本文所进一步描述的。

[0037] 与访客设备唯一地相关联的设备标识符的非限制性例子包括:MAC地址、IMEI号、IMSI号或者其它唯一性基于硬件的标识符。换言之,在虚拟接入点可访问的数据库中,可以将设备标识符与虚拟接入点密码绑定在一起。其后,访客可以通过从相同的通信设备中输入该虚拟接入点密码,来接入该网络。当虚拟接入点接收到与虚拟接入点密码相匹配的密码时,其确定该访问的通信设备(即,访客设备)的设备ID是否与和该虚拟接入点密码相关联的设备ID相匹配;如果相匹配,则允许该访客设备接入该网络,如果不匹配,则拒绝网络接入。

[0038] 通过将网络接入限制于从访客设备(其中该访客设备具有所批准的访客设备所独有的设备标识符)输入批准的虚拟接入点密码的访客,仅仅与该设备标识符相关联并且使用正确的虚拟接入点密码的特定访客设备才可以被给予对该虚拟接入点的接入。即使该虚

拟接入点密码被暴露给第三方，第三方也不能够使用第三方通信设备来获得对该网络的接入，这是由于第三方通信设备的设备标识符与可以使用该虚拟接入点密码的访客设备的设备标识符不匹配。因此，虚拟接入点密码的无意或者有意分发将不会导致非授权的通信设备进行不受控的网络接入。这降低了通常伴随着密码的广泛分发而导致的潜在网络安全和性能下降风险。

[0039] 在各个实施例中，网络管理者可以管理对虚拟接入点密码的授权。可以通过网络管理者与其具有连接的网络接入点，来进行针对无线网络的接入。该连接可以是通过与网络接入点的本地无线连接，例如，当网络管理者设备位于该网络接入点的范围之内时。网络管理者设备和网络接入点之间的连接也可以通过与互联网的远程连接来进行，例如，通过网络管理者设备之间的连接和与互联网的蜂窝数据连接，或者通过从远程Wi-Fi网络到互联网的接入点连接。网络管理者设备可以通过连接到与网络接入点相关联的URL(例如，通过浏览器或者其它软件)，来获得针对该网络接入点的接入。通过连接到该网络接入点对应的URL，可以在网络管理者设备上呈现允许对该网络接入点进行控制和配置的界面。网络管理者设备和网络接入点之间的连接可以允许网络管理者设备利用各种各样的方式，对网络接入点进行配置。替代地或另外地，可以使用允许对网络接入点进行配置的软件，来修改网络接入点，如本文所进一步描述的。

[0040] 在另一个实施例中，网络接入点可以生成虚拟接入点密码，并将其提供给网络管理者以便中继给访客。另外，虚拟接入点可以具有其自己的标识符(例如，未公布的SSID或者索引的SSID)，其中，当访客设备使用虚拟接入点密码来接入该网络时，其必须使用该标识符。在该虚拟接入点可访问的数据库中，该虚拟接入点标识符可以与虚拟接入点密码和唯一性访客设备ID相关联。要求访客设备连同虚拟接入点密码来使用虚拟接入点标识符，可以提供进一步的安全层。在该实施例中，可以通过各种各样的机制(例如，通过从访客设备到网络管理者设备的文本消息，或者通过提前讨论的安排)，来实现访客接入该网络的请求。网络管理者设备可以将该请求转发给网络接入点，或者单方面地“推送”给网络接入点。当网络接入点接收到接入请求时，可以实例化或者以其它方式建立虚拟接入点。作为该实例化的一部分，可以建立该虚拟接入点的虚拟接入点标识符和虚拟接入点密码。该虚拟接入点密码与网络接入点的共享密钥或者密码不同。通过向虚拟接入点提供与网络接入点的共享密钥不同的密码，网络管理者可以维持关于该共享密钥的分发的控制，并在不披露该共享密钥的情况下向访客提供接入。

[0041] 当实例化或者建立虚拟接入点时，网络接入点可以将虚拟接入点标识符和虚拟接入点密码转发给网络管理者设备。网络管理者设备可以利用诸如文本消息，将该虚拟接入点标识符和虚拟接入点密码转发给访客设备。此外，网络管理者设备还可以使得虚拟接入点标识符和虚拟接入点密码被显示在访客设备上，使得访客随后可以使用该信息来获得对无线网络的接入。在登录或者与网络接入点的接入过程期间(例如，当访客设备位于网络接入点的范围之内时)，访客设备可以输入该虚拟接入点标识符和虚拟接入点密码。在第一次登录过程期间，虚拟接入点可以获得访客设备ID，并在用于存储该虚拟接入点密码和相应的虚拟接入点标识符的数据库记录中关联性地增加或者存储该访客设备ID。其后，当访客设备使用虚拟接入点标识符来连接到允许该访客设备进行接入的虚拟接入点时，访客设备在登录过程期间，将虚拟接入点密码连同其设备ID进行一起发送。如果虚拟接入点密码和

设备ID与和该虚拟接入点标识符相关联的记录相匹配，则在虚拟接入点和访客设备之间建立安全连接。

[0042] 因此，各个实施例使得能够在无需向访客提供网络接入点密码的情况下，实现访客接入到安全网络的规定和控制。可以向访客提供用于虚拟接入点的专用密码，例如，该专用密码还可以是专门基于虚拟接入点标识符的。在各个实施例中，可以将用于虚拟接入点的密码与和该访客设备相关联的设备标识符(例如，媒体访问控制(MAC)地址)绑定在一起。可以将MAC地址和虚拟接入点密码的组合增加到网络接入点的接入列表中。因此，即使将该密码披露给别人，该密码也不能够与不同通信设备的用户进行共享，这是由于任何其它通信设备也必须通过远程管理者来请求虚拟接入点标识符和虚拟接入点密码。

[0043] 为了便于引用起见，下面参照图1A-图1C来描述被配置用于共享密钥安全的传统无线网络与接入点。

[0044] 图1A示出了诸如局域网(LAN)、无线局域网(WLAN)或者其它网络之类的无线网络103的例子100。无线网络103可以是私人网络(如，家庭网络)。无线网络103可以包括用于通过天线111提供无线接入的网络接入点110。网络接入点110还可以向位于该无线网络103的环境之内的通信设备提供有线接入。网络接入点110可以通过连接102来耦合到互联网101，例如通过服务提供商(没有示出)。无线网络103还可以包括服务器130，其可以通过连接130a来耦合到网络接入点110。连接130a可以是有线连接，也可以是无线连接。服务器130可以耦合到其它计算机133、耦合到诸如网络打印机132之类的设备、或者耦合到与该无线网络103相连接的计算机可以共享的其它设备。通信设备134(例如，具有无线能力的电视)也可以例如通过无线连接134a，无线地连接到网络接入点110。

[0045] 在网络接入点110的操作期间，一个或多个访客设备120可以通过连接121，经由网络接入点110来获得针对无线网络103的接入，其中连接121可以是有线连接，也可以是无线连接。如上面所提及的，访客设备120可以是各种各样的通信设备中的任何一种，例如，智能电话、膝上型计算设备102a、或者能够与网络接入点110进行有线或无线连接的其它便携式计算设备。

[0046] 为了获得针对网络接入点110的接入，访客设备120可以进行接入过程，在图1B中示出了该接入过程的至少一部分。虽然一种示例性接入过程可以与WiFi接入相关联(例如，根据802.11标准中的一种标准)，但在各个实施例中，也可以使用其它接入过程。在诸如访客设备120之类的通信设备在网络接入点110的无线环境之下发送探测请求帧，并且网络接入点110利用探测响应帧进行响应之后，访客设备可以通过向网络接入点110发送接入请求消息125来请求接入。在一种开放接入环境中，知道网络接入点的服务集标识符(SSID)的任何通信设备可以获得针对该网络的接入。但是，在安全网络中，访客设备120还必须输入密码，以便获得针对无线网络103的接入。因此，网络接入点110可以使用挑战请求消息(challenge request message)115来响应接入请求消息125，其中挑战请求消息115可以被发送回访客设备120。挑战请求消息115的接收可以例如导致：用于访客设备120提示访客输入网络密码的对话框或者数据输入屏幕的显示。可以向网络接入点110发送包括网络密码的挑战响应消息126。当网络密码正确时，网络接入点可以向访客设备120发送授权响应消息116，在该时间点，可以通过网络接入点110，在访客设备120和网络之间建立安全连接。为了便于描述起见，示出了上面的过程和消息流，并省略了某些细节，其中这些细节根据与网

络接入点110和访客设备120相关联的接入协议和特定硬件而不同。当在访客设备120和网络接入点110之间建立安全连接或者关联时，可以例如通过网络接入点110与用于该无线网络的网络服务器130来建立数据连接127。数据连接127可以允许访客设备120接入服务器130和耦合到该服务器130的设备。此外，可以通过网络接入点110来建立与互联网101的数据连接128。数据连接128可以允许访客设备接入互联网101以及通过互联网101可访问的任何资源，其包括网站、基于web的电子邮件、以及例如通过通用资源定位符(URL)可访问的其它资源。

[0047] 结合图1C示出了更详细的消息流交换。在给出的例子中，访客设备120可以是具有显示器120b的膝上型计算设备。当访客设备120发送探测帧，并通过从接入点发送的探测响应消息来发现附近的网络时，可以获得可用网络的列表来进行选择。访客设备120的用户可以使用SSID来在输入窗口120c中选择用于接入的网络(例如，“JOHNS NET”)。授权请求消息125可以包含用于所选网络的SSID，并将其发送给与“JOHNS NET”SSID相关联的网络接入点110。基于被配置为实现安全接入，响应于授权请求消息125，网络接入点110可以向访客设备120发送挑战请求115，其可以导致在显示器120b上显示对话框，其提示输入共享密钥(例如，“w@3nf”)以接入到网络接入点110，其中该共享密钥可以在输入窗口120d中进行输入。可以从访客设备120向网络接入点110发送包含共享密钥126a“w@3nf”的挑战响应消息126。在方框117中，网络接入点110可以对该共享密钥126a进行解码。当该共享密钥正确时(例如，判断框118＝“是”)，可以向访客设备120发送授权响应消息116a，其使得在显示器120b上显示用于指示成功地授权或认证的消息120f，故可以建立数据连接。当该共享密钥不正确时(例如，判断框118＝“否”)，可以向访客设备120发送授权响应消息116b，其使得在显示器120b上显示用于指示授权或认证失败的消息120g，故拒绝数据连接。因此，为了使访客设备120能够接入该网络，必须向访客提供网络密码或者共享密钥。如上面所讨论的，这种实现增加了损害网络的风险。

[0048] 各个实施例通过消除分发共享密钥126a的需求，以通过建立虚拟接入点来提供访客接入，来克服传统的接入点的限制，其中虚拟接入点识别与共享密钥或网络密码不同的虚拟接入点密码，虚拟接入点密码的使用被限制于具有与该虚拟接入点密码相关联的设备ID的通信设备。在图2A中，示出了用于实现各个实施例的示例性通信网络200。在该系统中，当网络管理者设备230授权时，可以通过网络接入点210来向访客设备200提供针对网络的接入。访客设备220可以通过无线接口221，与网络接入点210建立无线通信链路。

[0049] 网络管理者设备230可以利用各种各样的方式来与网络接入点210进行连接，使得即使当网络管理者设备230位于远离网络接入点210的位置时，也可以提供访客接入。例如，当网络管理者设备230位于网络接入点210的无线范围之内时，网络管理者设备230可以通过无线连接230a与网络接入点210进行连接。在其它例子中，网络管理者设备230可以通过与公众交换电话网络(PSTN)101a的连接230b，与网络接入点210进行连接，其中PSTN 101a可以使用调制解调器连接或者其它用户线连接来提供针对互联网101的接入。在另外的例子中，网络管理者设备230可以通过与蜂窝塔101b的无线连接230c，与网络接入点210进行连接，其中蜂窝塔101b也提供针对互联网101的接入。在另外的例子中，网络管理者设备230可以通过与另一个接入点101c(其也可以提供针对互联网101的接入)的连接230d，与网络接入点210进行连接。

[0050] 网络接入点210可以通过服务提供商211和与该网络接入点210所支持的通信设备的连接102，来提供互联网101接入。通过服务提供商211的连接102还可以允许通信设备通过输入与网络接入点210相关联的URL，来接入网络接入点210。网络接入点210可以通过需要管理者密码，来保护能够接入与该网络接入点210相关联的URL的通信设备。因此，通过本地地经由连接230a或者远程地经由连接230b、230c、230d(或者经由其它远程连接)来接入网络接入点210，网络管理者设备230可以输入管理者密码来配置网络接入点210。网络管理者设备230还可以进行用于向访客设备220提供接入的通信，如图2B中所示。

[0051] 访客设备220可以发起对于接入到无线网络的请求225，其中网络接入点210控制针对该无线网络的接入。该请求225可以包括利用文本消息来向网络管理者设备230的用户进行的请求，或者是利用使用访客设备220和网络管理者设备230建立的会话来进行。该请求可以是预先安排的协定的一部分，以便提供在访客设备220的用户和网络管理者设备230的用户之间进行的接入。

[0052] 响应于请求225，网络管理者设备230可以向网络接入点210提供诸如联系信息之类的信息235。信息235可以充当为虚拟设备标识符，其使网络接入点210能够在接入列表中生成一个条目，以便在无需知道该访客设备220的唯一设备标识符的情况下，建立访客设备220针对该无线网络的接入。还可以使用信息235来生成虚拟设备标识符。在获得所述唯一标识符之前的第一次接入尝试期间，可以使用该虚拟设备标识符，并将其与虚拟接入点密码绑定在一起。如本文所讨论的，网络接入点210可以实例化或者以其它方式建立虚拟接入点和虚拟接入点密码。替代地，可以在发现过程期间可选地实例化虚拟接入点密码。该发现过程可以是网络接入点在第一次接入尝试期间，确定访客设备220的虚拟标识符的过程。该发现过程还可以是网络接入点在第一次接入尝试之后的后续接入中，确定访客设备220的唯一设备标识符与所存储的访客设备220的标识符相匹配的过程。如本文所进一步详细描述的唯一标识符可以是在第一次接入尝试期间获得的，以及在后续的接入尝试中使用其来验证访客设备220的身份。

[0053] 可以将虚拟接入点标识符和虚拟接入点密码连同在信息235中传送的联系信息一起存储在网络接入点210的接入列表中。在后续的接入尝试期间，可以使用虚拟接入点标识符和虚拟接入点密码来向访客设备220提供接入。可以将虚拟接入点标识符和虚拟接入点密码转发给访客设备220，使得当输入转发的虚拟接入点标识符和虚拟接入点密码时，访客设备220可以获得针对无线网络的接入。

[0054] 可以在动作236中，将虚拟接入点标识符和虚拟接入点密码转发给访客设备220，其中动作236可以包括：在访客设备220的用户可以读取的文本消息中，发送虚拟接入点标识符和虚拟接入点密码。动作236还可以包括：使用不同于文本消息传送的消息传送软件应用，显示虚拟接入点标识符和虚拟接入点密码。该消息传送软件应用可以允许在包括访客设备220和网络管理者设备230的通信设备之间传送消息。当向访客设备220的用户或者访客设备220提供虚拟接入标识符和虚拟接入点密码时，访客设备220可以尝试登录(226)到网络接入点210。根据与该无线网络和网络接入点210相关联的协议的类型，登录226过程可以包括没有示出的例行程序步骤，例如，发送探测请求和从位于范围之内的任何接入点(其包括如上所述的网络接入点210)接收探测响应。

[0055] 在典型的例子中，当访客设备220“发现”网络接入点210时，访客设备220可以基于

根据SSID对网络接入点的识别，向网络接入点210发送接入请求消息227。在其它例子中，虚拟接入点可以通过虚拟接入点标识符(其可以充当为SSID)来独立地可发现。网络接入点210或者通过网络接入点210进行工作的虚拟接入点可以接收接入请求消息227，生成向访客设备220发送的挑战请求消息216。挑战请求消息216可以使得在与访客设备220相关联的显示器上显示对话框或者视窗，其请求输入网络接入点210或者虚拟接入点的密码(如果该访客设备识别出的话)。访客设备220的用户可以在该对话框或者视窗中的网络的正常密码位置中输入虚拟接入点密码，以便获得针对虚拟接入点的接入，其中该虚拟接入点可以在网络接入点210上进行实例化。在一些实施例中，挑战请求消息216可以使得显示定制的对话框或者视窗，其专门请求网络密码和与该接入请求相关联的虚拟接入点标识符。可以在作为初始虚拟接入点建立序列240中的第一消息的挑战响应消息228中，将输入的信息从访客设备220发送给网络接入点210。在方框241中，网络接入点210可以对所接收的信息进行检查。

[0056] 在访客设备的用户选择了网络接入点210的SSID的例子中，当从该访客设备接收的信息包括诸如共享网络密钥之类的正确的网络密码时(即，判断框242＝“是”)，网络接入点210可以发送接入准许消息217，并准许根据普通的接入过程，通过网络接入点210来接入到该无线网络，从而建立网络数据会话243。当从访客设备接收的信息不包括正确的网络密码时(即，判断框242＝“否”)，网络接入点210可以执行几种动作。举一个例子，网络接入点210可以被配置为将输入的密码传送给虚拟接入点，使得虚拟接入点可以确定输入的密码和设备标识符信息是否对应于有效的访客。在其它例子中，网络接入点210可以将来自于访客设备220的信息传送给虚拟接入点，以确定所接收的信息是否对应于该网络接入点210所支持的虚拟接入点，或者被虚拟接入点进行识别。当从访客设备接收的信息与虚拟接入点或者虚拟接入点知道的信息不对应时(即，判断框244＝“否”)，可以拒绝访客设备220的接入，网络接入点210可以发送接入拒绝消息218。当从访客设备接收的信息与虚拟接入点相对应或者与授权的访客设备的数据库记录中的信息相匹配时(例如，与设备ID相关的正确的虚拟接入点密码)(即，判断框244＝“是”)，则可以通过发送接入准许消息217a，准许访客设备220接入到虚拟接入点210a，其中虚拟接入点210a可以是在网络接入点210上建立或者实例化的。随后，可以在访客设备220和虚拟接入点210a之间建立网络数据会话253。

[0057] 在访客设备220进行的初始接入尝试期间，可以基于在上面所描述的消息235中发送的联系信息，来准许接入到虚拟接入点210a，其中虚拟接入点210a可以是网络接入点210使用先前指定的虚拟接入点标识符在先前建立或者实例化的。这种临时接入可能是必需的，这是由于虽然访客设备220的设备标识符是可获得的，但直到将访客设备220识别成具有正确的虚拟接入点标识符和正确的虚拟接入点密码(例如，或者正确的联系信息)的设备为止，该设备标识符没有与虚拟接入点密码和/或虚拟接入点标识符进行绑定或者关联。

[0058] 当与网络接入点210进行通信时，在从准许接入之前在访客设备220向网络接入点210传送的通信帧中可获得访客设备220的设备标识符。访客设备220的设备标识符可以包括媒体访问控制(MAC)地址或者标识符，也可以包括不同的标识符，例如IMEI标识符，或者对于与访客设备220相关联的硬件来说唯一的其它标识符。在初始接入尝试期间，当确定虚拟接入点密码、虚拟接入点标识符、联系信息或者其它识别信息是正确的时，可以将设备标识符和虚拟接入点密码与虚拟接入点标识符绑定在一起，或者一起存储在网络接入点210

和/或虚拟接入点210a可获得的接入列表或者接入数据库中(例如,存储在网络接入点210/虚拟接入点210a的存储器中,或者存储在网络接入点210/虚拟接入点210a连接到的网络上的服务器中)。

[0059] 在图2B中通过接入顺序250所表示的访客设备220进行的后续接入尝试期间(即,在初始或者第一次尝试之后),访客设备220可以发送挑战响应消息228a。在虚拟接入点标识符包括在挑战响应消息218a的例子中,在虚拟接入点210a中,对虚拟接入点密码和设备标识符进行接收和处理。在另一个例子中(其中,没有提供虚拟接入点标识符),当网络接入点210没有识别出虚拟接入点密码(由于其不是网络密码)时,可以将该接入尝试和输入的信息(其包括访客设备标识符)传送给虚拟接入点210a。虚拟接入点210a可以检查虚拟接入点密码和访客设备220的设备标识符(例如,MAC地址),例如通过在方框241a中,将该虚拟接入点密码和设备标识符与接入列表或者接入数据库中的数据进行比较。倘若该虚拟接入点密码和设备标识符与接入列表/数据库中的条目相匹配,则可以准许网络接入。当准许接入时,可以将接入准许消息217a发送给访客设备220并建立网络数据会话253。替代地,虚拟接入点210a可以识别与访客设备220相关联的设备标识符,可以发生自动关联或者接入准许过程,以准许访客设备220的接入和该虚拟接入点密码的存储版本。在替代的例子中,网络接入点210可以被配置为识别访客设备220的设备标识符。网络接入点210可以使用接入请求消息227,将该设备标识符连同访客设备220所提供的存储的虚拟接入点密码一起传送给虚拟接入点210a。当虚拟接入点210a识别该设备标识符和虚拟接入点密码时,可以向访客设备220自动地准许进行接入。

[0060] 当与访客设备220相关联的联系信息被发送给网络接入点210,并建立或者实例化虚拟接入点时(如上所述),网络接入点210可以在虚拟接入点表301中生成一个条目,图3A中示出了其一个例子。虚拟接入点表301可以包含:与为了提供访客接入而建立或者实例化的任何建立的虚拟接入点相关联的信息。虚拟接入点表301的列的非限制性和非详尽示例包括:虚拟接入点索引(例如,标识符)列310、虚拟接入点名称列320、虚拟接入点活动列330、虚拟接入点状态列340、时间限制列350、接入限制列360a和带宽限制列360b。在各个实施例中,可以实现另外的或者较少的列。

[0061] 虚拟接入点索引列310可以包括:当网络接入点接收到对于访客接入的请求时,其可以建立或者实例化的虚拟接入点的条目。在一些实施例中,可以对于与给定的网络或者网络接入点相关联的虚拟接入点的数量进行限制,当达到该限制时,可以拒绝新的访客接入。在所给出的例子中,基于针对访客接入的五个请求,建立五个虚拟接入点。可以建立诸如索引1 311、索引2 312、索引3 313、索引4 314和索引5 315之类的虚拟接入点索引,并将其与相应的虚拟接入点进行关联。可以将这些虚拟接入点索引提供给访客设备,使得可以指引到用于特定的访客的虚拟接入点。

[0062] 在虚拟接入点名称列320中,还可以向虚拟接入点分配名称(例如,SSID),其可以用于在例如挑战响应过程期间获得接入。可以分配诸如“NEIGHBORS”名称321、“JOHNSNET”名称322、“PARENTS”名称323、“KIDS”名称324和“JANESNET”名称325之类的虚拟接入点名称,并将其与相应的虚拟接入点进行关联,以及针对给定的虚拟接入点,与用于该给定的虚拟接入点的其它行条目(例如,相应的虚拟接入点索引)进行关联。

[0063] 在虚拟接入点活动列330中,还可以向虚拟接入点分配活动状态,其可以用于确定

和更新相关联的虚拟接入点的状态活动。虚拟接入点活动状态可以包括活动状态331、空闲状态332、活动状态333、活动状态334和空闲状态335，以及相应的虚拟接入点的活动的其它指示符。该活动状态可以指示访客设备已登录到虚拟接入点并与其相关联，或者在网络接入点和访客设备之间发生了活动数据传输。

[0064] 在虚拟接入点状态列340中，还可以跟踪和维持虚拟接入点的状态，其可以用于确定该虚拟接入点的接入状态。可以列出虚拟接入点的虚拟接入点状态，例如，具有索引1 311的虚拟接入点的开放状态341、具有索引2 312的虚拟接入点的绑定状态342、具有索引3 313的虚拟接入点的绑定状态343、具有索引4 314的虚拟接入点的绑定状态344、以及具有索引5 315的虚拟接入点的绑定状态345。具有索引1 311的虚拟接入点的开放状态341可以指代已进行了接入请求、建立了虚拟接入点、但访客设备还没有接入的状态。具有索引2 312到5 315的虚拟接入点的绑定状态342-345可以指代具有设备特定标识符的访客设备已进行了接入的状态。该访客设备标识符可以是例如MAC地址、IMEI号、或者该通信设备的其它设备特定标识符。可以将该设备标识符绑定到虚拟接入点密码。当建立或者实例化了虚拟接入点，并且建立了索引、标识符和/或名称时，可以建立虚拟接入点密码。可以将虚拟接入点的密码和索引和/或名称转发给访客设备，使得可以在该访客设备的第一次接入尝试期间，就得知该访客设备的设备标识符。因此，在后续的接入期间，可以使用相关联的虚拟接入点和虚拟接入点密码来识别该访客设备。仅仅该访客设备可以接入该虚拟接入点，这是由于接入取决于从通信设备输入了正确的虚拟接入点密码，其中该通信设备具有绑定到该虚拟接入点密码的设备标识符。

[0065] 可以在虚拟接入点时间限制列350中指定时间限制，其可以用于指定该访客设备能够接入该虚拟接入点的可允许时间或者时间窗。可以针对每一个虚拟接入点来指定虚拟接入点可允许接入时间，例如，具有索引1 311的虚拟接入点的早8点到下午11点的接入时间351、具有索引2 312的虚拟接入点的早8点到下午11点的接入时间352、具有索引3 313的虚拟接入点的无限制接入时间353、具有索引4 314的虚拟接入点的下午3点到下午8点的接入时间354、以及具有索引5 315的虚拟接入点的无限制接入时间355。当被指派通过特定的虚拟接入点索引、标识符和/或名称来接入特定的虚拟接入点的访客设备尝试进行接入时，如果从具有绑定标识符的访客设备输入了正确的密码，则可以对接入时间进行检查，并且当在可允许的时间窗期间尝试进行接入时，准许进行接入。当没有指定限制时(例如，无限制)，则倘若从具有绑定标识符的访客设备输入了正确的密码，就可以在任何时间尝试并准许进行接入。如果在时间限制指示的时间之外来尝试进行接入，则可以拒绝接入。在一些实施例中，网络管理者可以批准位于指定的时间之外的接入。

[0066] 可以在虚拟接入点接入限制列360a中，指定关于针对虚拟接入点的接入的另外限制。可以使用这些接入限制来确定与该虚拟接入点服务的无线网络相关联的网络资源的可允许接入。可以针对每一个虚拟接入点来指定虚拟接入点接入限制，例如，具有索引 1 311的虚拟接入点的仅外部(EXTERNAL ONLY)接入限制361a、具有索引2 312的虚拟接入点的仅外部(EXTERNAL ONLY)接入限制362a、具有索引3 313的虚拟接入点的无限制接入限制363a、具有索引4 314的虚拟接入点的无限制接入限制364a、以及具有索引 5 315的虚拟接入点的无限制接入限制365a。仅外部(EXTERNAL ONLY)接入限制361a和362a可以将访客设备的接入限制于外部网络连接，以便防止接入该网络“内部”的网络资源，例如，打印机、计

算机以及可以形成与该无线网络正在操作的场地相关联的私人网络的其它设备。例如，仅外部(EXTERNAL ONLY)接入限制361a和362a可以将访客设备的接入限制于互联网接入，其中互联网接入可用成服务提供商针对网络接入点的外部资源。当被指派通过特定的虚拟接入点索引、标识符和/或名称来接入特定的虚拟接入点的访客设备尝试进行接入时，可以对接入限制进行检查，并根据相应的限制来准许对网络资源的接入。可以拒绝对位于所指示的接入限制之外的接入资源进行的尝试。在一些实施例中，网络管理者可以批准针对受限制资源的尝试。无限制接入限制363a-365a可以允许访客设备接入所有的网络资源。在仅外部和无限制的情况下，或者在其它限制级别下，系统管理者可以例如基于用户、设备或者特定于文件的限制(其根据安全和秘密性目的的需求，限制接入或者限制读取/写入能力)，来提供另外的或者特殊限制。

[0067] 可以在虚拟接入点带宽限制列360b中指定关于针对虚拟接入点的接入的另外限制。可以使用带宽限制来扼制或者限制被分配给与该无线网络相关联并由该虚拟接入点服务的访客设备的带宽。可以针对每一个虚拟接入点来指定虚拟接入点带宽限制，以及虚拟接入点带宽限制可以是基于与访客设备的类型相关联的优先级，或者是根据该访客的身份或者该访客与该无线网络的所有者或管理者的关系。还可以在动态基础上实现带宽限制。动态带宽限制将尝试向所有访客提供最大可能带宽。在动态限制示例中，如果需要的话，则基于访客的当前数量和访客的优先级，或者基于预先设置的带宽分配机制，来实现针对访客的带宽限制。换言之，当有多余的带宽可用时，可以向访客分配最大带宽。也就是说，直到访客的数量增加到多余的带宽不再可用的时间点为止，或者针对该系统的带宽限制开始接近或者超过为止。当多余的带宽不再可用时，虚拟接入点可以基于访客设备的优先级，开始对带宽进行限制，其中首先对低优先级访客设备进行限制。在其它例子中，当访客设备连接到虚拟接入点时，可以按照预先指定的级别来分配带宽。

[0068] 由于所有的虚拟接入点是在网络接入点硬件上建立和实例化的，并且可以使用相同的无线电模块，因此关于分配给访客设备的带宽的限制可以防止网络和网络接入点变得过度负载。对于诸如所有者或管理者之类的高优先级用户来说，网络过载是特别不利的。因此，当访客与虚拟接入点进行连接时，可以基于虚拟接入点标识符来应用特定于访客的带宽限制。例如，诸如具有索引1 311的虚拟接入点(例如，其对应于虚拟接入点名称NEIGHBORS 321)的BW LVL 5带宽限制361b、具有索引2 312的虚拟接入点(例如，其对应于虚拟接入点名称JOHNSNET 322)的BW LVL 1带宽限制362b、具有索引3 313的虚拟接入点(例如，其对应于虚拟接入点名称PARENTS 323)的全BW LVL 10带宽限制363b、具有索引4 314的虚拟接入点(例如，其对应于虚拟接入点名称KIDS 324)的BW LVL 8带宽限制364b、以及具有索引5 315的虚拟接入点(例如，其对应于虚拟接入点名称JANESNET 325)的BW LVL 7带宽限制365b之类的带宽限制。带宽限制361b-365b可以限制被分配给访客设备的带宽，以便防止网络接入点和网络过载。例如，带宽限制361b-365b可以根据“级别”、优先级或者其它因素来限制带宽。在所给出的例子中，BW LVL 10表示全带宽，BW LVL 1表示更受限制的带宽。

[0069] 可以基于各种各样的因素(其包括活动级别、可用带宽或者多余的带宽、带宽升级或者其它因素)，来动态地改变带宽级别。在所给出的例子中，可以基于空闲状态332，为具有索引2 312的虚拟接入点的虚拟接入点名称JOHNSNET 322分配BW LVL 1，其是最低带宽

分配。当与JOHNSNET 322相关联的访客再次变成活动时，可以将带宽级别增加或者升级到适当的级别。当访客设备的连接状态改变时(例如，发展到多余的带宽状况)，可以根据需要来动态地增加或者升级带宽级别。

[0070] 为了跟踪连接到虚拟接入点的访客设备，可以提供另外的列(例如，设备ID列370a)。设备ID列370a可以用于维持虚拟接入点和绑定到该虚拟接入点的访客设备之间的关联或者对应关系。例如，对于具有索引1 311的虚拟接入点(例如，对应于虚拟接入点名称NEIGHBORS 321)而言，设备ID 371a可以包含未知地址“??:??:??:??:??:??”，这是由于针对该虚拟接入点和访客设备的绑定状态341被指示成“开放”。开放状态341意味着该访客设备还没有执行到该虚拟接入点的第一次登录。对于具有索引2 312的虚拟接入点(例如，对应于虚拟接入点名称JOHNSNET 322)而言，设备ID 372a可以包含已知地址“12:34:56:78:9A:02”，这是由于针对该虚拟接入点和访客设备的绑定状态342被指示成“绑定”。绑定状态342和其它绑定指示意味着该访客设备执行了到该虚拟接入点的第一次登录，该虚拟接入点已记录了该访客设备的设备标识符(例如，MAC地址)。对于具有索引3 313的虚拟接入点(例如，对应于虚拟接入点名称PARENTS 323)而言，两个设备ID 373a可以包含已知地址“12:34:56:78:9A:00”和“12:34:56:78:9A:01”，这是由于针对该虚拟接入点和访客设备的绑定状态343被指示成“绑定”。对于具有索引4 314的虚拟接入点(例如，对应于虚拟接入点名称KIDS 324)而言，两个设备ID 374a可以包含已知地址“12:34:56:78:9A:04”和“12:34:56:78:9A:05”，这是由于针对该虚拟接入点和访客设备的绑定状态344被指示成“绑定”。对于具有索引5 315的虚拟接入点(例如，对应于虚拟接入点名称JOHNSNET 325)而言，设备ID 375a可以包含已知地址“12:34:56:78:9A:03”，这是由于针对该虚拟接入点和访客设备的绑定状态345被指示成“绑定”。

[0071] 当如上所述地建立或者实例化虚拟接入点，并且访客设备随后尝试接入时，网络接入点210可以指代MAC地址用户表302，如图3B中所示。MAC地址用户表302可以包含与虚拟接入点相对应的针对访客设备标识符的条目、以及与这些访客设备相关联的访客的名称信息。设备ID列370b可以包含地址“12:34:56:78:9A:00”373b、地址“12:34:56:78:9A:01”373c、地址“12:34:56:78:9A:02”372b、地址“12:34:56:78:9A:04”374b、地址“12:34:56:78:9A:05”374c、地址“??:??:??:??:??:??”371b和地址“12:34:56:78:9A:03”375b。MAC地址用户表302的设备ID列370b中的地址可以与图3A的虚拟接入点表301中的设备ID列370a具有某种对应关系。在MAC地址用户表302中，具有有效MAC地址值的MAC地址列370b中的条目可以指代已尝试进行接入的访客设备的MAC地址值，并且它们的虚拟接入点密码与该访客设备的MAC地址或者特定于设备的标识符和例如通过虚拟接入点索引所识别的虚拟接入点进行了绑定。地址??:??:??:??:??:??371b可以指代已被分配了虚拟接入点和虚拟接入点密码，但还没有尝试接入该虚拟接入点的访客的未知设备标识符。

[0072] 虚拟接入点索引列380可以包含与地址12:34:56:78:9A:00 373b相对应的虚拟接入点索引3 381、与地址12:34:56:78:9A:01 373c相对应的虚拟接入点索引3 382、与地址12:34:56:78:9A:02 372b相对应的虚拟接入点索引2 383、与地址12:34:56:78:9A:04 374b相对应的虚拟接入点索引4 384、与地址12:34:56:78:9A:05 374c相对应的虚拟接入点索引4 385、与地址??:??:??:??:??:??371b相对应的虚拟接入点索引1 386、以及与地址12:34:56:78:9A:03 375b相对应的虚拟接入点索引5 387。在所给出的例子中，如通过虚拟

接入点表301和MAC地址用户表302所观察的，可能几个访客设备与同一个虚拟接入点相关联。

[0073] 在各个实施例中，访客名称列390可以包含名称标识符，其可以是例如基于在请求建立访客接入期间发送的联系信息，而在虚拟接入点的建立期间分配的。还可以以其它方式来设置或者重新设置这些名称标识符(例如，当访客已获得接入时由访客执行，或者由网络管理者执行)。访客名称列390可以包括访客名称“MOM”391、访客名称“DAD”391、访客名称“JOHN DOE”393、访客名称“BOBBY PHONE”394、访客名称“BOBBY LAPTOP”395、访客名称“DALE NEIGHBOR”396和访客名称“JANE”397。访客名称DALE NEIGHBOR 396可以与无效的或者未分配的地址(例如，地址??:??:??:??:??:??371b)相关联。地址371b(通过不包含有效地址)可以指示与访客名称DALE NEIGHBOR 396相关联的访客还没有尝试进行接入。其它地址373b、373c、372b、374b、374c和375b与已尝试进行了接入从而使得设备标识符或者MAC地址已知的访客设备相关联。

[0074] 当访客设备进行了针对接入的请求并尝试进行接入时，网络接入点可以例如基于虚拟接入点表301和MAC地址用户表302之间的关联，引用和更新虚拟接入点表301和MAC地址用户表302中的各个条目。在图3C中示出了虚拟接入点表301和MAC地址用户表302之间的关联。MAC地址用户表302和虚拟接入点表301之间的关联303示出了：与MAC地址用户表302中的MOM名称条目391、索引3 381和地址12:34:56:78:9A:00 371相关联的访客设备可以与虚拟接入点表301中对应于索引3 313、虚拟接入点名称PARENTS 323、活动状态ACTIVE 333、状态BOUND(绑定)343、时间限制NO RESTRICTIONS(无限制)353和接入限制NO RESTRICTIONS(无限制)363的相应条目相关联。类似地，MAC地址用户表302和虚拟接入点表301之间的关联304示出了：与MAC地址用户表302中的DAD名称条目392、索引3 382和地址12:34:56:78:9A:01 372相关联的访客设备可以与虚拟接入点表301中对应于索引3 313、虚拟接入点名称PARENTS 323、活动状态ACTIVE 333、状态BOUND(绑定)343、时间限制NO RESTRICTIONS(无限制)353和接入限制NO RESTRICTIONS(无限制)363的相应条目相关联。

[0075] MAC地址用户表302和虚拟接入点表301之间的关联305示出了：与MAC地址用户表302中的JOHN DOE名称条目393、索引2 383和地址12:34:56:78:9A:02 372b相关联的访客设备可以与虚拟接入点表301中对应于索引2 312、虚拟接入点名称JOHNSNET 322、活动状态IDLE(空闲)332、状态BOUND(绑定)342、时间限制早8点到下午11点353、接入限制EXTERNAL ONLY(仅外部)362a、带宽限制BW LVL 1 362b和设备ID 12:34:56:78:9A:02 372a的相应条目相关联。

[0076] MAC地址用户表302和虚拟接入点表301之间的关联306示出了：与MAC地址用户表302中的BOBBY PHONE名称条目394、索引4 384和地址12:34:56:78:9A:04 374b相关联的访客设备可以与虚拟接入点表301中对应于索引4 314、虚拟接入点名称KIDS 324、活动状态ACTIVE(活动)334、状态BOUND(绑定)344、时间限制下午3点到下午8点354、接入限制NO RESTRICTIONS(无限制)364a、带宽限制BW LVL 8 364b、以及所列出的设备ID 374a中的一个(例如，12:34:56:78:9A:04)的相应条目相关联。在“Bobby”具有另外的通信设备来获得对该网络的接入的实施例中，该另外的通信设备也与针对所建立的虚拟接入点的条目进行关联。例如，MAC地址用户表302和虚拟接入点表301之间的关联307示出了：与MAC地址用户表302中的BOBBY LAPTOP名称条目395、索引4 385和地址12:34:56:78:9A:05 374c相关联

的访客设备可以与虚拟接入点表301中对应于索引4 314、虚拟接入点名称KIDS 324、活动状态ACTIVE(活动)334、状态BOUND(绑定)344、时间限制下午3点到下午8点354、接入限制NO RESTRICTIONS(无限制)364a、带宽限制BW LVL 8 364b、以及所列出的设备ID 374a中的另一个(例如,12:34:56:78:9A:05)的相应条目相关联。

[0077] 当网络接入点接收到接入请求时,可以确定是否建立或者实例化新的虚拟接入点。该确定可以是基于现有的虚拟接入点和其它因素的使用。网络接入点还可以确定是否向现有的虚拟接入点分配与该请求相关联的访客设备。条目398a可以指示:与MOM名称条目391和DAD名称条目392相关联的访客设备以及与BOBBY PHONE名称条目394和BOBBY LAPTOP名称条目395相关联的访客设备具有活动的活动状态(以及绑定的状态)。根据活动的活动状态,例如网络接入点可以决定限制针对索引3 313和索引4 314所标识的虚拟接入点的另外的访客接入,这是由于这些绑定访客设备是活动的。

[0078] 条目398b可以指示:与JOHN DOE名称条目393相关联的访客设备和与JANE名称条目397相关联的访客设备被绑定至已建立的虚拟接入点(例如,索引2 312和索引5 315),并具有空闲的活动状态。根据空闲的活动状态(例如,以及绑定的状态),例如网络接入点可以决定允许针对索引2 312和索引5 315所标识的虚拟接入点的另外的访客接入,这是由于这些绑定访客设备是空闲的。

[0079] 条目398c可以指示:与DALE NEIGHBOR名称条目396相关联的访客设备正在接入具有开放状态的已建立的虚拟接入点(例如,索引1 311)。通过指示开放状态,网络接入点和/或相应的虚拟接入点将尝试获得与DALE NEIGHBOR名称条目396相关联的访客设备的设备标识符371a/371b。当获得该设备标识符371a/371b(例如,与DALE NEIGHBOR名称条目396相关联的访客设备的MAC地址)时,可以将设备标识符371a/371b与针对与索引1 311相关联的已建立的虚拟接入点的虚拟接入点密码绑定在一起。当对访客设备的设备标识符和虚拟接入点密码进行绑定时,在输入或者以其它方式提供了正确的虚拟接入点密码时,仅仅具有该绑定设备标识符的访客设备才可以获得接入。即使具有不同的设备标识符的访客设备输入了正确的虚拟接入点密码,也拒绝该访客设备进行接入,这是由于其设备标识符与和该虚拟接入点密码绑定在一起的设备标识符不匹配。

[0080] 绑定可以是将一个值与另一个值进行关联的过程,其使得一个绑定值的引用可以是第一值所捆绑到的另一个值的引用。在一个实施例中,在所给出的例子中,设备标识符可以是针对虚拟接入点密码的引用。在该例子中,例如在捆绑之后发生的接入尝试期间,当网络接入点和/或虚拟接入点获得访客设备的设备标识符时,可以使用该设备标识符来引用虚拟接入点密码(例如,其是该设备先前成功输入的),故可以立即准许进行接入。在其它实施例中,可以将绑定设备标识符和虚拟接入点密码存储在一个表中。当访客设备提供虚拟接入点密码时,在该表中执行查询以验证是否是具有正确设备标识符的设备正在尝试进行连接。可以将该设备标识符和虚拟接入点密码与该查询获得的绑定值进行比较,故当这些值匹配时,可以允许该访客设备接入该虚拟接入点。

[0081] 在图4A中示出了用于通过建立虚拟接入点,向访客设备提供针对无线网络的接入的实施例方法。在方框401中,访客可以请求接入到无线网络。该请求可以涉及针对网络管理者设备的消息或者其它通信。在方框402中,网络管理者设备可以从访客设备接收对于接入到该无线网络的请求。在方框403中,网络管理者可以向网络接入点发送与接入到该无线

网络相关联的信息。例如，该信息可以是来自于与网络管理者设备相关联的联系列表的联系信息。如果不存在与该访客或者该访客设备的所有者相关联的联系信息，则可以将该信息作为网络管理者设备中的联系人进行增加，并随后进行发送。

[0082] 在方框404中，网络接入点可以接收该访客或者该访客设备的所有者的联系信息。当网络接入点确定已建立了一个或多个虚拟接入点，并且在现有的虚拟接入点中有资源可用时(即，判断框405＝“是”)，则在方框408中，网络接入点可以返回虚拟接入点索引或者标识符和虚拟接入点密码。当网络接入点确定现有的虚拟接入点没有生成时，或者现有的虚拟接入点的资源不足够用于支持与访客设备的另外连接时(即，判断框405＝“否”)，进行进一步的确定。例如，当网络接入点检查已建立的虚拟接入点的表，并确定关于可以建立的虚拟接入点的数量的限制还没有满足时(即，判断框406＝“否”)，则在方框407中，网络接入点可以生成、实例化或者以其它方式建立具有虚拟接入点索引或者标识符和唯一密码的虚拟接入点。用于该虚拟接入点的唯一密码可以与网络密码或者共享密钥不同。

[0083] 生成或者实例化虚拟接入点可以涉及：开始具有接入点的逻辑和功能属性的进程。该虚拟接入点进程可以访问硬件资源，或者可以通过网络接入点的主进程与硬件进行通信，或者处于网络接入点的主进程的控制之下。当生成、实例化或者以其它方式建立虚拟接入点时，在方框408中，网络接入点可以返回虚拟接入点索引或者标识符和虚拟接入点密码。

[0084] 当生成虚拟接入点时和/或当向网络管理者设备返回标识符和密码时，在方框409中，网络管理者设备可以向访客或者访客设备转发该虚拟接入点索引或者标识符和虚拟接入点密码。随后，访客设备可以通过使用该虚拟接入点标识符和虚拟接入点密码与该虚拟接入点进行关联，来尝试获得针对该网络的接入。

[0085] 当达到生成虚拟接入点的限度时(即，判断框406＝“是”)，则在方框411中，网络接入点可以拒绝该接入请求。响应于在方框403中进行的请求，网络管理者设备可以转发或者以其它方式接收该拒绝。在方框412中，网络管理者设备可以将该接入拒绝转发给访客或者访客设备。

[0086] 该接入拒绝可以是临时的，直到在现有的虚拟接入点上有可用的另外资源为止。在某些环境下，网络接入点可以终止虚拟接入点。例如，当与一个虚拟接入点相关联的所有访客都空闲一段时间时，网络接入点可以终止该虚拟接入点。

[0087] 在各个实施例中，网络接入点还可以监测与虚拟接入点相关联的登录活动，以及当与一个虚拟接入点相关联的访客在一段时间都没有进行登录时，其可以终止该虚拟接入点。在替代的实施例中，虚拟接入点自身可以监测活动，并在类似的状况下终止自身。当虚拟接入点资源变得可用时，或者当虚拟接入点已被终止时，可以准许另外的请求。因此，访客或者访客设备可以接收用于说明已拒绝进行接入的指示(例如，消息)。该消息可以包含当资源可用时，可以再次尝试请求的另外通知。在各个实施例中，该消息甚至可以包含重新进行接入尝试的建议时间。在其它实施例中，网络管理者可以在某个稍后的时间自动地再次尝试接入，并且当接入最终可行时，转发虚拟接入点标识符和密码。

[0088] 当访客设备接收到虚拟接入点索引或者标识符和虚拟接入点密码时，访客设备可以尝试通过图4B中所示出的实施例方法420来尝试接入。在方框421中，访客设备可以使用虚拟接入点标识符和虚拟接入点密码来尝试接入。如上所述，可以从网络管理者接收虚拟

接入点索引或标识符和虚拟接入点密码。当访客设备进行网络接入点的初始发现时，其可以使设备标识符让网络接入点知道。如上面所提及的，该设备标识符可以是MAC地址、IMEI号或者该通信设备的其它唯一标识符。通过当访客设备进入网络接入点的信号范围之内时发生的初始通信，可以使该访客设备的设备标识符变得可获得。

[0089] 当访客设备响应从网络接入点发送的用于通知通信设备位于该网络接入点的现有无线通信范围之内以及该网络接入点的能力的信号时，可以发生初始通信。替代地，当访客设备尝试与网络接入点进行有线连接时(例如，当访客设备使用电缆(如，RJ45网络电缆或者类似的电缆)来耦合到网络接入点硬件时)，可以发生类似的通信。这种初始通信可以包括：从访客设备到网络接入点的通信，其在与关联于连接请求的初始通信相关联的协议分组中包含设备标识符。作为连接请求过程的一部分，例如响应于网络接入点的挑战或者密码请求，访客设备可以输入虚拟接入点标识符和虚拟接入点密码。当输入正确的虚拟接入点密码时，虚拟接入点可以准许针对该网络的接入。如在上面的例子中，在第一次接入尝试期间，访客设备可以输入联系信息以验证访客身份，此时可以确定访客设备的设备标识符，并将其捆绑到虚拟接入点密码。在后续的有线或者无线接入尝试期间，虚拟接入点可以基于设备标识符来识别访客设备。为了便于描述起见，上面所描述的连接过程在本质上是通用的，故省略了一些细节。

[0090] 在示例性实施例中，在方框422中，网络接入点可以获得访客设备的MAC地址。在方框423中，网络接入点可以针对与该访客设备相关联的条目，对虚拟接入点表和/或MAC地址表进行检查。在各个实施例中，网络接入点进行的该检查可以通过MAC地址查询操作来完成。替代地或另外地，可以通过MAC地址查询以及在虚拟接入点表或MAC地址表中可获得的访客名称和/或其它信息，来进行该检查。当针对该访客联系人(例如，访客设备)的表条目是不可获得的时(即，判断框424＝“否”)，则在方框425中，可选地生成一个表条目。但是，在通常环境下，诸如当由例如网络管理者进行请求时(如本文所描述的)，表条目应当是可用的，并分配有虚拟接入点标识符。表条目的确定可以基于访客联系名称、虚拟接入点标识符和/或该访客设备的MAC地址。该表条目可以至少包含：足够用于识别该访客的访客联系信息、以及虚拟接入点索引或标识符和虚拟接入点密码。

[0091] 当表条目是可获得的时(即，判断框424＝“是”)，则网络接入点可以确定该访客设备是否是第一次尝试进行接入。例如，当MAC地址表不包含对应于该访客设备的设备标识符或者MAC地址的任何条目时，该确定是可行的。当访客设备是第一次尝试接入该网络时(即，判断框426＝“是”)，例如在该访客设备可以连接的可用网络列表中，与该虚拟接入点相对应的网络是可见的。虽然在虚拟接入点标识符的用户表中，存在未绑定的访客用户(例如，还没有进行第一次登录的访客)，但虚拟接入点可以被配置为出现在位于本网络接入点的范围之内的设备的可用网络列表之中。当所有指定的访客用户都进行了捆绑时，其后，当该访客设备下一次进入到本网络接入点的范围之内时，虚拟接入点可以自动地进行连接。

[0092] 在方框427中，网络接入点可以将联系信息和虚拟接入点密码转发给适当的虚拟接入点(例如，根据访客设备所提供的虚拟接入点索引或者标识符)。在各个实施例中，例如，基于网络管理者的请求，先前已经实例化或者建立了具有该虚拟接入点索引或标识符的虚拟接入点。当虚拟接入点从进行第一次接入的访客接收到联系信息和虚拟接入点密码时，在方框428中，网络接入点可以将该访客设备的MAC地址至少与该虚拟接入点进行绑定，

并可选地与虚拟接入点索引或者标识符进行绑定。网络接入点可以使用该访客设备的MAC地址，来更新MAC地址用户表中与该访客设备相对应的条目。随后，在方框430中，访客设备可以关联或者以其它方式连接到与该虚拟接入点索引或者标识符相关联的虚拟接入点。在方框431中，可以对虚拟接入点表或者一些表进行更新，以反映诸如访客设备与该虚拟接入点的连接状态、状态和其它信息之类的信息。在各个实施例中，虚拟接入点可以查询虚拟接入点表，以确定是否列出了可能影响该访客设备的网络连接和接入范围的任何时间或接入限制或者其它参数。

[0093] 在后续的接入尝试中，也就是当访客设备不是第一次尝试接入该网络时(即，判断框426＝“否”)，则在方框432中，该访客设备所指示的虚拟接入点可以查询该访客设备的MAC地址，并对虚拟接入点密码进行验证。例如，可以通过将输入的虚拟接入点密码和该访客设备的MAC地址与表格中存储的绑定设备标识符和虚拟接入点密码进行比较，来完成验证。当对MAC地址和虚拟接入点密码的验证没有通过时(即，判断框433＝“否”)，则在方框434中，拒绝该连接。当对MAC地址和虚拟接入点密码进行了验证时(即，判断框433＝“是”)，则在方框430中，可以允许该访客设备与该虚拟接入点进行关联。在另一个例子中，假定在与设备标识符相关联的设备的第一次接入尝试期间，输入了正确的虚拟接入点密码，则虚拟接入点仅仅基于设备标识符就准许进行接入。在另外的例子中，对于后续的连接而言，当网络接入点识别出绑定访客设备的设备标识符时，可以实例化完全绑定的但不具有关联的当前访客的指定的虚拟接入点。例如，可以根据当访客设备进入网络接入点的范围之内时，该网络接入点接收的分组传输来识别访客设备标识符。在认识到该设备位于范围之内时，可以实例化与该设备标识符相对应的虚拟接入点，并自动地准许进行接入。

[0094] 各种实施例可以在各种各样的计算设备中的任何一种(例如，图5中所示出的移动计算设备500)之中实现，和/或使用各种各样的计算设备中的任何一种来实现。图5中所示出的移动计算设备500只是可结合各种实施例使用的计算设备的一个例子，下面所描述的部件在本质上只是示例性的，其可以表示任何移动计算设备的通用部件。典型的移动计算设备500通常具有图5中所示出的部件。例如，移动计算设备500可以包括耦合到用于存储信息的内部存储器504和506的处理器501。内部存储器504和506可以是易失性存储器或非易失性存储器，还可以是安全和/或加密存储器，或者非安全和/或非加密存储器、或者其任意组合。处理器501还可以耦合到触摸屏显示器512，例如，电阻式感应触摸屏、电容感应触摸屏红外线感测触摸屏等等。在一些实施例中，移动计算设备500的显示器不需要具有触摸屏能力。

[0095] 移动计算设备500可以具有用于发送和接收无线信号的一个或多个无线信号收发机508(例如，Peanut®、Bluetooth®、Zigbee®、Wi-Fi、RF无线电装置)和天线510、或者耦合到天线设备的天线模块。无线信号收发机508可以彼此之间相耦合和/或耦合到处理器501。移动计算设备500可以包括蜂窝网络无线调制解调器芯片516，其经由蜂窝数据网络(例如，CDMA、TDMA、GSM、PCS、3G、4G、LTE、或者任何其它类型的蜂窝数据网络)来实现通信并耦合到处理器501。移动计算设备500可以包括耦合到处理器501的外围设备连接接口518。外围设备连接接口518可以被单独地配置为接受一种类型的连接，或者被多重地配置为接受多种类型的物理和通信连接、共同或专有连接(例如，USB、火线、Thunderbolt或PCIe)。外围设备连接接口518还可以耦合到类似配置的外围设备连接端口。移动计算设备500还可以

包括扬声器514或者用于提供音频输出的扬声器。移动计算设备500还可以包括使用塑料、金属、或材料组合构成的壳体520，以包含本文所讨论的所有部件或者一些部件。在一些实施例中，物理天线结构可以合并到壳体520中，并耦合到天线模块510。移动计算设备500可以包括耦合到处理器501的电源522，例如一次性或可充电电池。该可充电电池还可以耦合到外围设备连接端口，以便从移动计算设备500之外的源接收充电电流。移动计算设备500还可以包括耦合到处理器501的GPS接收机，以确定该设备的位置。移动计算设备500还可以包括用于接收用户输入的物理按键512b。

[0096] 上面所描述的各个实施例还可以实现在各种各样的个人计算设备(例如，如图6中所示的膝上型计算机600)中，和/或使用各种各样的个人计算设备来实现。很多膝上型计算机包括触摸板触摸接口607，其用作该计算机的指向设备，故可以接收拖动、滚动和滑动手势(其类似于上面所描述的在装备有触摸屏显示器的移动计算设备上所实现的那些)。通常，膝上型计算机600包括耦合到易失性存储器和大容量非易失性存储器(例如，闪存设备602)的处理器601。膝上型计算机600还可以包括耦合到处理器601的软盘驱动器和紧致碟(CD)驱动器。膝上型计算机600还可以包括耦合到处理器601的多个网络收发机或者网络连接器端口606，其配置为使处理器602能够通过一个或多个有线或无线网络来与其它计算设备进行通信。举一个特定的例子，膝上型计算机600的网络收发机可以包括耦合到用于发送和接收电磁辐射的一个或多个天线的以太网、USB或FireWire®连接器插座/收发机、诸如Wi-Fi之类的一个或多个无线调制解调器收发机和/或蜂窝数据网络收发机。膝上型计算机600还可以包括用于将处理器601耦合到可能在未来开发的网络的其它类型的网络连接电路。在笔记本配置中，计算机壳体605包括全部都耦合到处理器601的触摸板607、键盘608和显示器609。该计算设备的其它配置可以包括(例如，经由USB输入)耦合到处理器的计算机鼠标或者跟踪球，如公众所知道的，这些部件也可以结合各种实施例来使用。

[0097] 处理器501、601可以是能通过软件指令(应用)进行配置，以执行多种功能(其包括下面所描述的各种实施例的功能)的任何可编程的微处理器、微计算机或多个处理器芯片或芯片集。在一些移动设备中，可以提供多个处理器，例如，一个处理器专用于无线通信功能，一个处理器专用于运行其它应用。通常，在访问软件应用并将它们装载到处理器501和601之前，可以将这些软件应用存储在内部存储器504、506、602中。处理器501和601可以包括足够用于存储这些应用软件指令和其它信息的内部存储器。

[0098] 本领域普通技术人员应当理解的是，信息和信号可以使用多种不同的技术和方法中的任意一种来表示。例如，在贯穿上面的描述中提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或粒子、光场或粒子或者其任意组合来表示。

[0099] 此外，本领域普通技术人员应当理解的是，前述的方法描述和过程流程图仅仅是提供用作为说明性例子，而不是旨在要求或者隐含着必须以所给出的顺序来执行各个实施例的步骤。如本领域普通技术人员所应当理解的，可以以任何顺序来执行上述的实施例中的步骤顺序。此外，诸如“其后”、“之后”、“接着”等等之类的词语并不旨在限制这些步骤的顺序；这些词语仅仅只是用于引导读者遍历该方法的描述。此外，任何对权利要求元素的单数引用(例如，使用冠词“一个(a)”、“某个(an)”或者“该(the)”)，不应被解释为将该元素限制为单数形式。

[0100] 结合本文所公开的实施例描述的各种示例性的逻辑框、模块、电路和算法步骤均可以实现成电子硬件、计算机软件或二者的组合。为了清楚地表示硬件和软件之间的这种可交换性，上面对各种示例性的部件、框、模块、电路和步骤均围绕其功能进行了总体描述。至于这种功能是实现成硬件还是实现成软件，取决于特定的应用和对整个系统所施加的设计约束条件。熟练的技术人员可以针对每个特定应用，以变通的方式实现所描述的功能，但是，这种实现决策不应解释为背离本发明的保护范围。

[0101] 用于执行本文所述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件部件或者其任意组合，可以用来实现或执行结合本文所公开的实施例描述的用于实现各种示例性的逻辑、逻辑框、模块和电路的硬件。通用处理器可以是微处理器，或者，该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可以实现为计算设备的组合，例如，DSP和微处理器的组合、若干微处理器、一个或多个微处理器与DSP内核的结合，或者任何其它此种结构。替代地，一些步骤或方法可以由特定于给定的功能的电路来执行。

[0102] 各个实施例中的功能可以用硬件、软件、固件或它们任意组合的方式来实现。当在软件中实现时，可以将这些功能存储成非临时性计算机可读介质或者非临时性处理器可读介质上的一个或多个处理器可执行指令或代码。本文所公开的方法或算法的步骤可以体现在处理器可执行软件模块中，其可以位于非临时性计算机可读或者处理器可读存储介质上。非临时性计算机可读或者处理器可读存储介质可以是计算机或处理器能够存取的任何存储介质。举例而言，但非做出限制，这种非临时性计算机可读或处理器可读介质可以包括RAM、ROM、EEPROM、闪存、CD-ROM或其它光盘存储器、磁盘存储器或其它磁存储设备、或者能够用于存储具有指令或数据结构形式的期望的程序代码并能够由计算机进行存取的任何其它介质。如本文所使用的，磁盘(disk)和光盘(disc)包括压缩光盘(CD)、激光光盘、光盘、数字多用途光盘(DVD)、软盘和蓝光光盘，其中磁盘通常磁性地复制数据，而光盘则用激光来光学地复制数据。上述的组合也应当包括在非临时性计算机可读介质和处理器可读介质的保护范围之内。另外，一种方法或算法的操作可以作为一个代码和/或指令集或者其任意组合，位于非临时性处理器可读介质和/或计算机可读介质上，其中该非临时性处理器可读介质和/或计算机可读介质可以并入到计算机程序产品中。

[0103] 为使本领域任何普通技术人员能够实现或者使用本发明，上面围绕所公开的实施例进行了描述。对于本领域普通技术人员来说，对这些实施例的各种修改是显而易见的，并且，本文定义的总体原理也可以在不脱离本发明的保护范围的基础上应用于其它实施例。因此，本发明并不限于本文所示出的实施例，而是要被给予与所附权利要求书和本文公开的原理和新颖性特征相一致的最广范围。

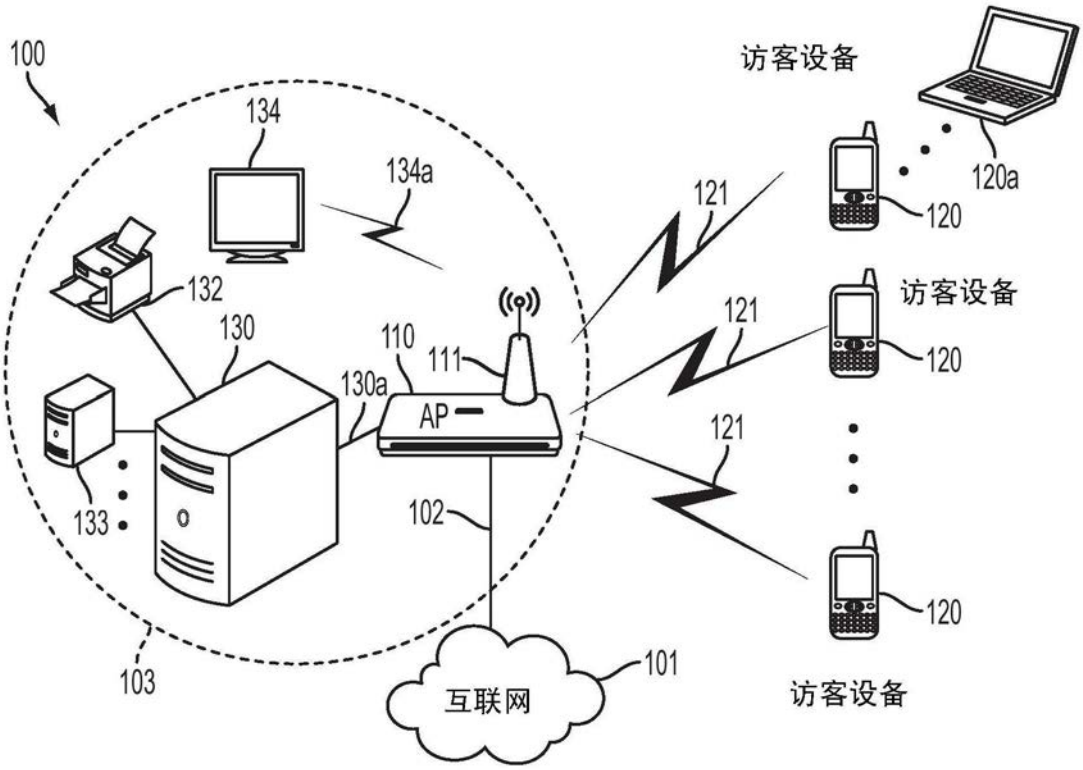


图1A现有技术

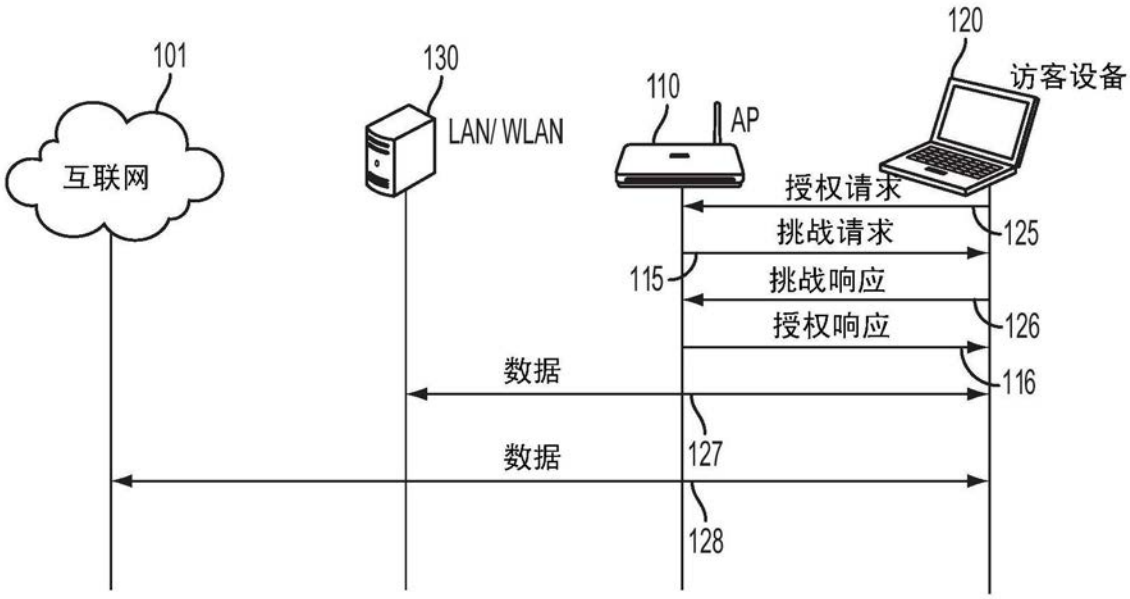


图1B现有技术

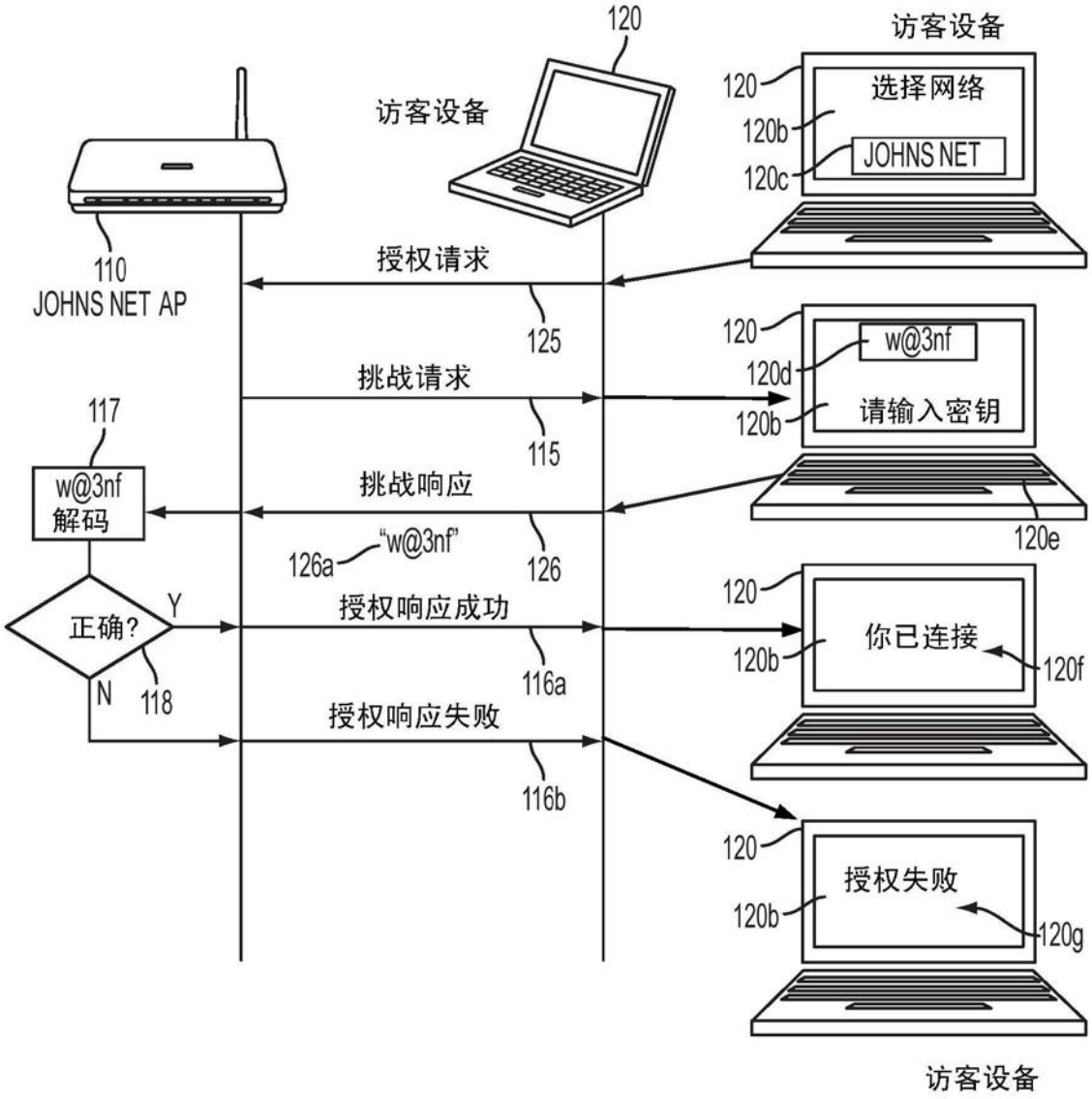

120
访客设备
访客设备
120
选择网络
120b
JOHNS NET
120c
110
JOHNS NET AP
授权请求
125
120
w@3nf
120d
120b
请输入密钥
挑战请求
115
117
w@3nf
解码
挑战响应
126a
"w@3nf"
126
120e
正确?
Y
授权响应成功
120
你已连接
120b
120f
116a
N
118
授权响应失败
116b
120
授权失败
120b
120g
访客设备

图1C现有技术

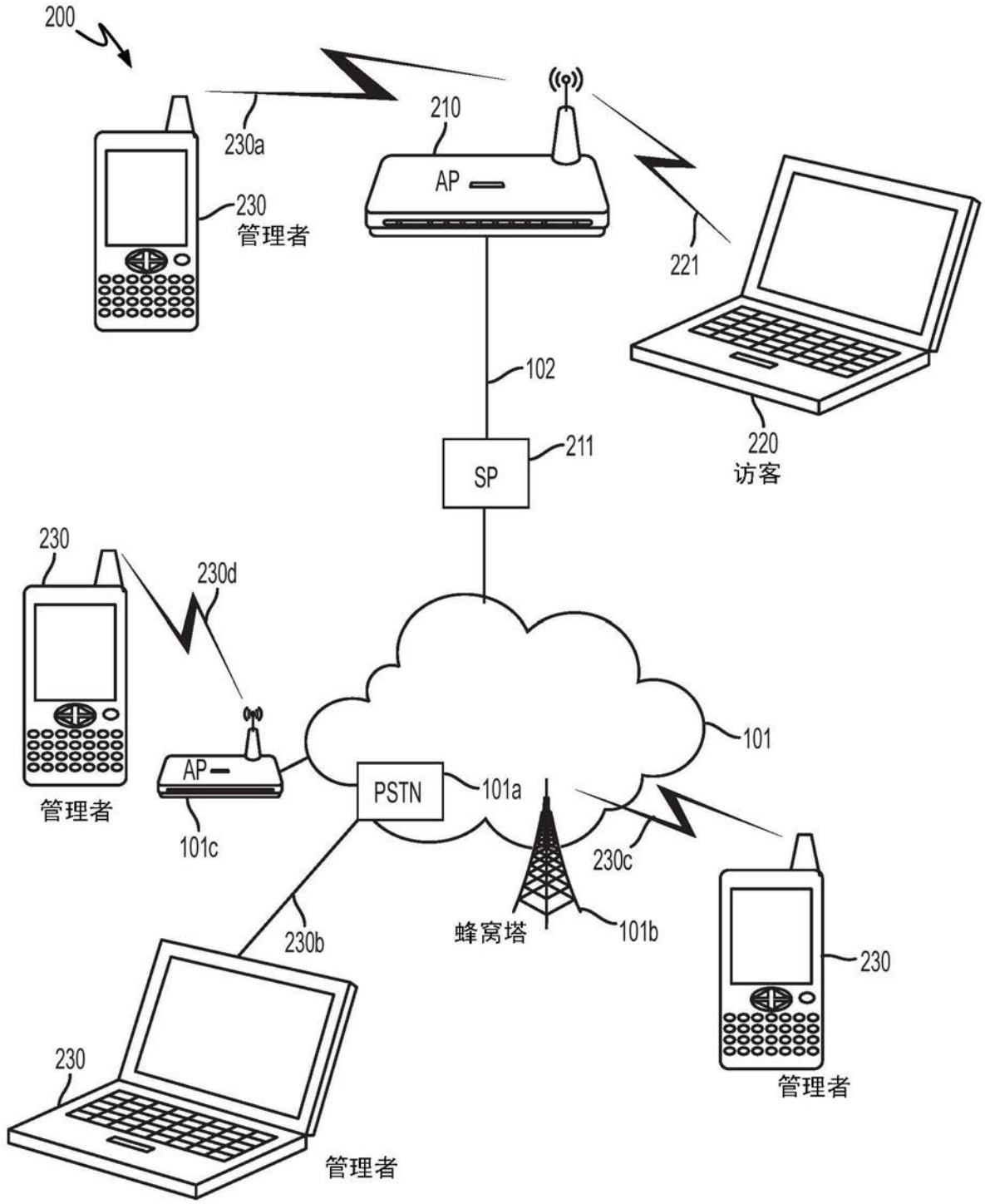

200
230a
210
AP
230
管理者
221
102
SP
211
220
访客
230
230d
AP
管理者
101c
PSTN
101a
101
230c
蜂窝塔
101b
230
230b
230
管理者

图2A

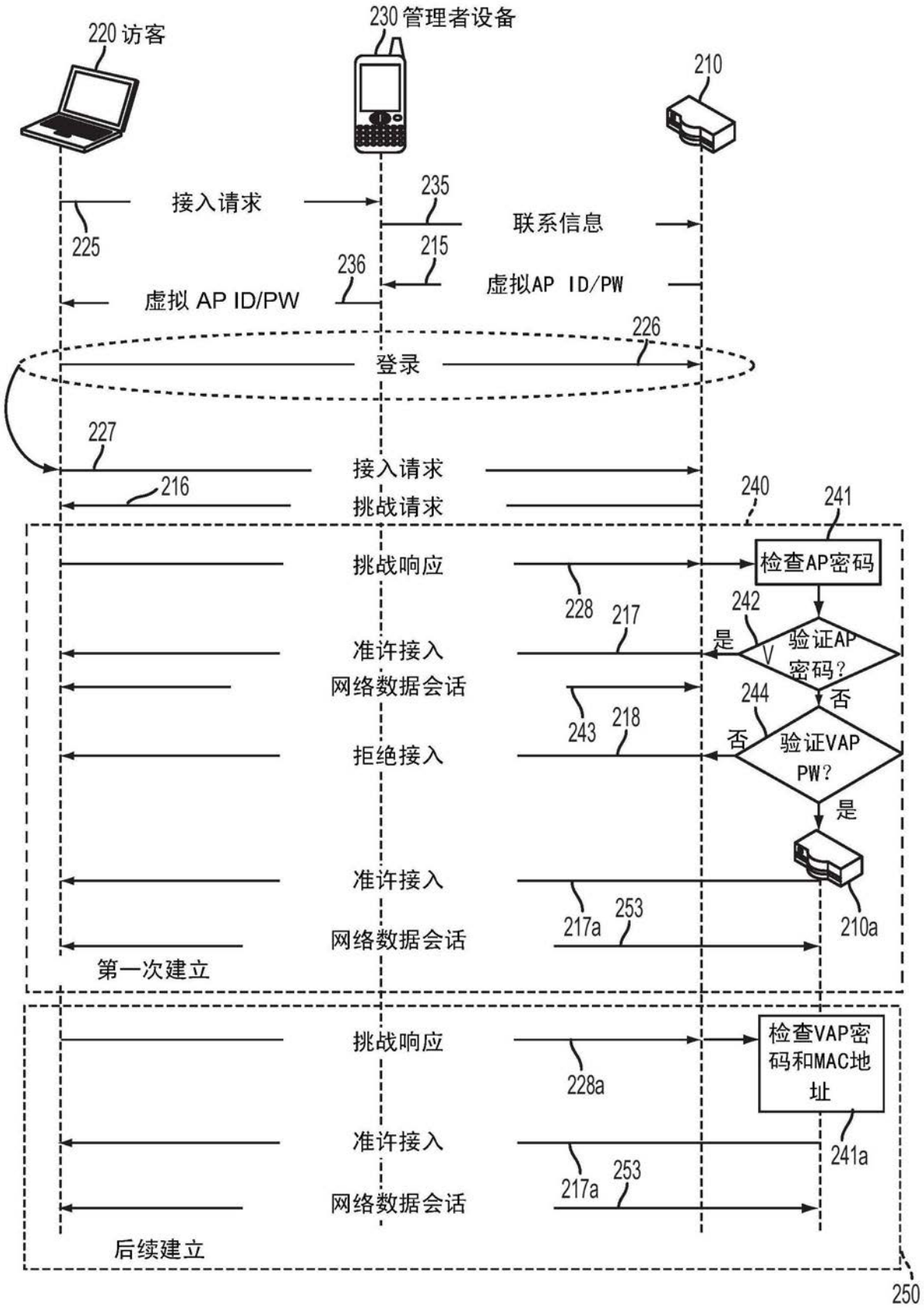

220 访客
230 管理者设备
210
接入请求
225
235
联系信息
215
236
虚拟AP ID/PW
虚拟 AP ID/PW
226
登录
227
接入请求
216
挑战请求
240
241
挑战响应
检查AP密码
228
217
242
是
验证AP密码?
准许接入
网络数据会话
否
244
243
218
否
拒绝接入
验证VAP PW?
是
准许接入
217a
253
210a
网络数据会话
第一次建立
挑战响应
检查VAP密码和MAC地址
228a
准许接入
241a
217a
253
网络数据会话
后续建立
250

图2B

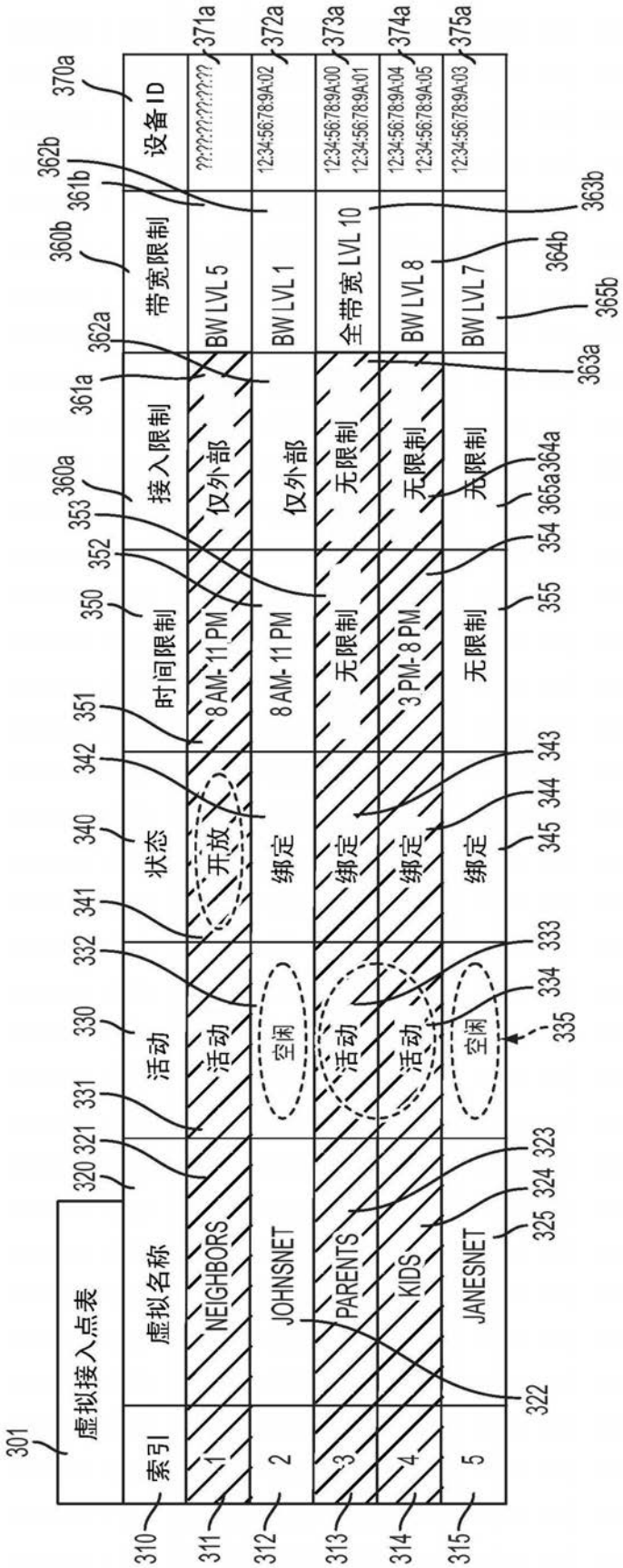

虚拟接入点表
索引
虚拟名称
状态
活动
时间限制
接入限制
带宽限制
设备ID
NEIGHBORS
JOHNSNET
PARENTS
KIDS
JANESNET
开放
绑定
空闲
活动
8 AM- 11 PM
3 PM- 8 PM
无限制
仅外部
BW LVL 5
BW LVL 1
全带宽 LVL 10
BW LVL 8
BW LVL 7
??:??:??:??:??:??
12:34:56:78:9A:02
12:34:56:78:9A:00
12:34:56:78:9A:01
12:34:56:78:9A:04
12:34:56:78:9A:05
12:34:56:78:9A:03

图3A

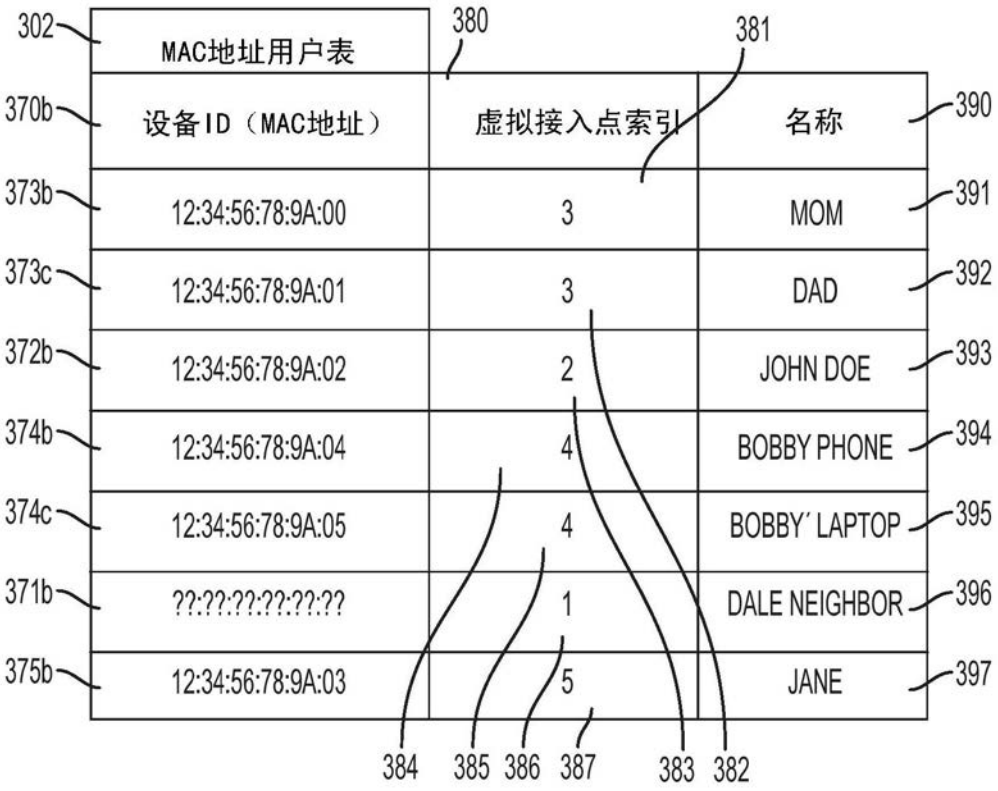

302
MAC地址用户表
380
381
370b
设备ID（MAC地址）
虚拟接入点索引
名称
390
373b
12:34:56:78:9A:00
3
MOM
391
373c
12:34:56:78:9A:01
3
DAD
392
372b
12:34:56:78:9A:02
2
JOHN DOE
393
374b
12:34:56:78:9A:04
4
BOBBY PHONE
394
374c
12:34:56:78:9A:05
4
BOBBY' LAPTOP
395
371b
??:??:??:??:??:??
1
DALE NEIGHBOR
396
375b
12:34:56:78:9A:03
5
JANE
397
384
385
386
387
383
382

图3B

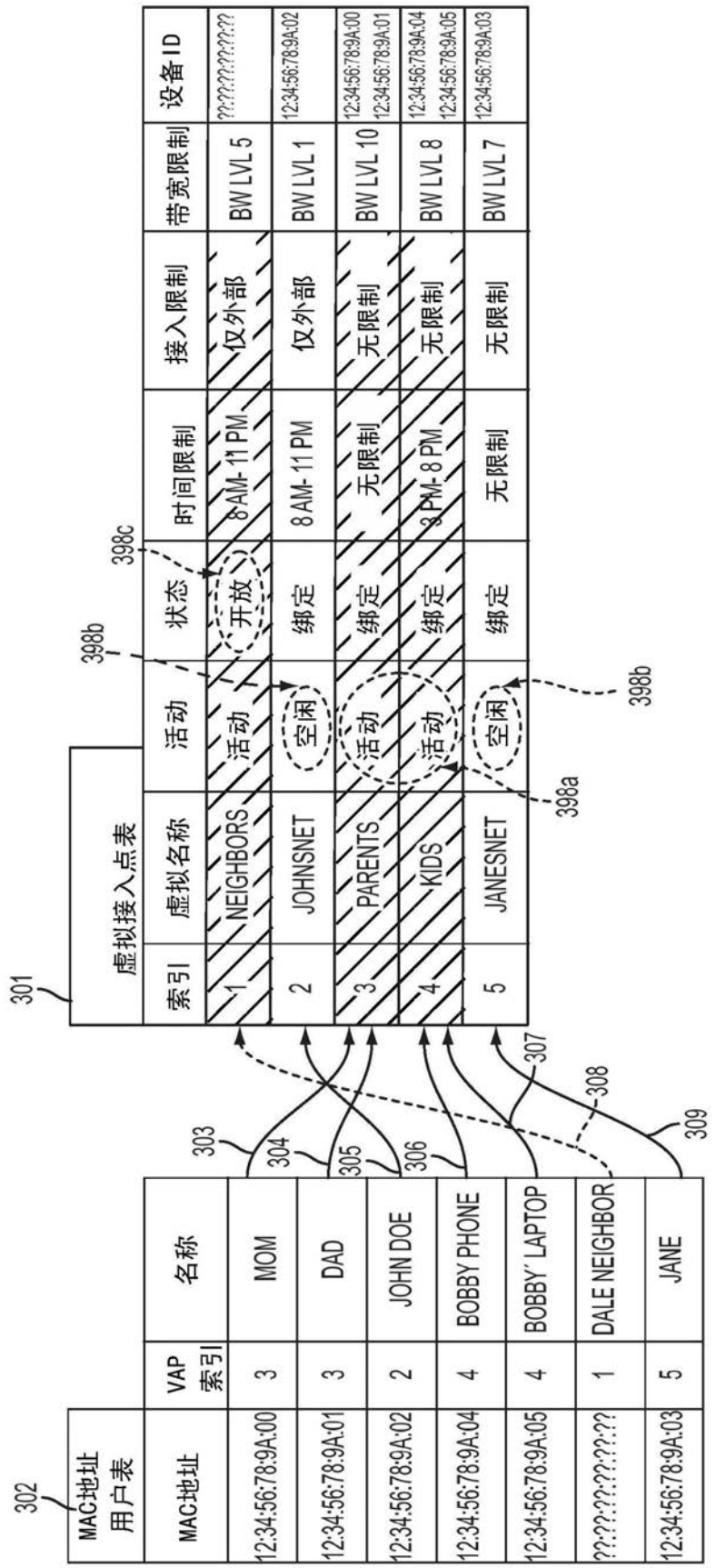

301
虚拟接入点表
索引
虚拟名称
活动
状态
时间限制
接入限制
带宽限制
设备ID
1
NEIGHBORS
活动
开放
8 AM- 11 PM
仅外部
BW LVL 5
??:??:??:??:??:??
2
JOHNSNET
空闲
绑定
8 AM- 11 PM
仅外部
BW LVL 1
12:34:56:78:9A:02
3
PARENTS
活动
绑定
无限制
无限制
BW LVL 10
12:34:56:78:9A:00
12:34:56:78:9A:01
4
KIDS
活动
绑定
3 PM- 8 PM
无限制
BW LVL 8
12:34:56:78:9A:04
12:34:56:78:9A:05
5
JANESNET
空闲
绑定
无限制
无限制
BW LVL 7
12:34:56:78:9A:03
398b
398c
398a
302
MAC地址
用户表
MAC地址
VAP
索引
名称
12:34:56:78:9A:00
3
MOM
12:34:56:78:9A:01
3
DAD
12:34:56:78:9A:02
2
JOHN DOE
12:34:56:78:9A:04
4
BOBBY PHONE
12:34:56:78:9A:05
4
BOBBY' LAPTOP
??:??:??:??:??:??
1
DALE NEIGHBOR
12:34:56:78:9A:03
5
JANE
303
304
305
306
307
308
309

图3C

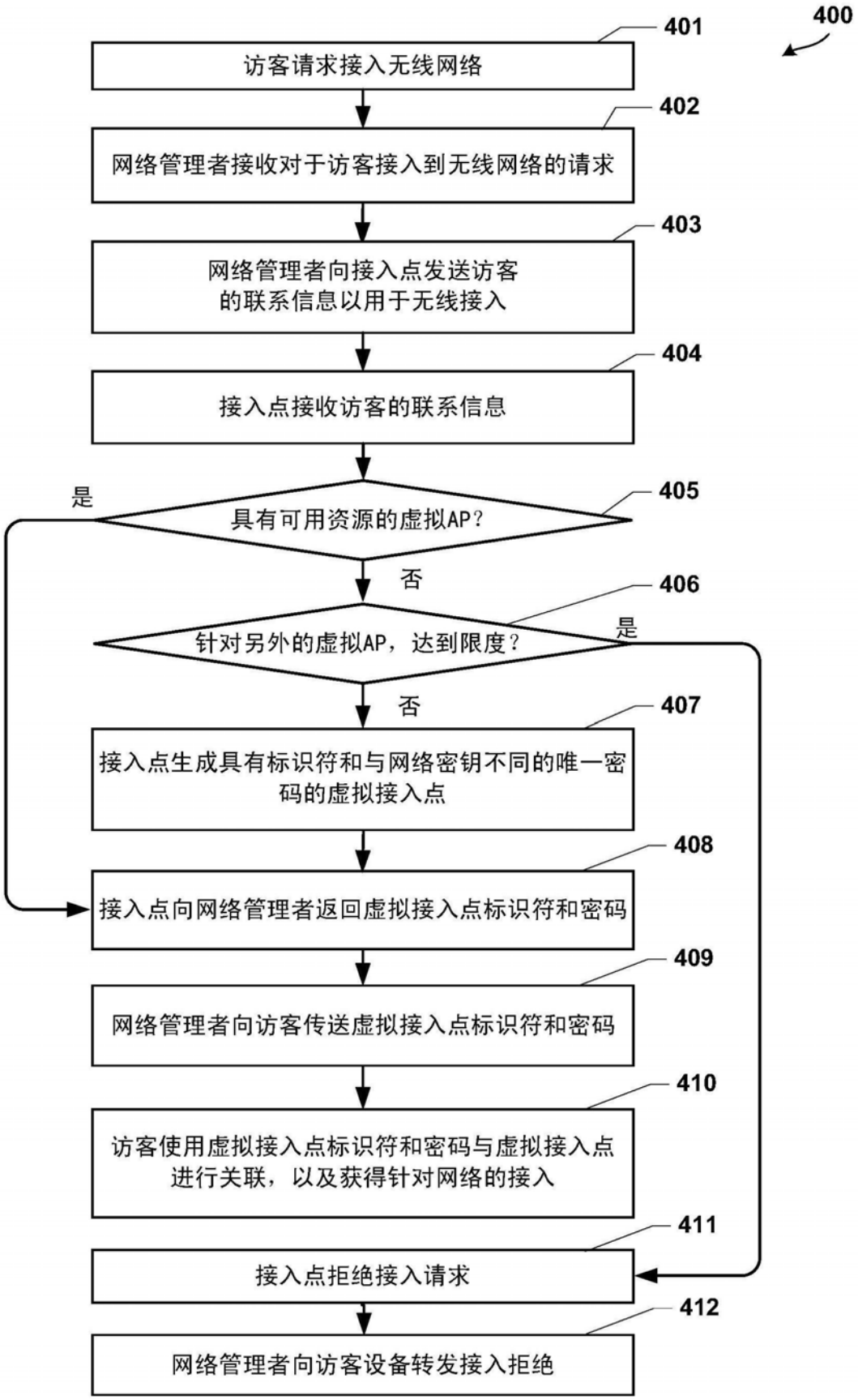

400
401
访客请求接入无线网络
402
网络管理者接收对于访客接入到无线网络的请求
403
网络管理者向接入点发送访客的联系信息以用于无线接入
404
接入点接收访客的联系信息
405
具有可用资源的虚拟AP？
是
否
406
针对另外的虚拟AP，达到限度？
是
否
407
接入点生成具有标识符和与网络密钥不同的唯一密码的虚拟接入点
408
接入点向网络管理者返回虚拟接入点标识符和密码
409
网络管理者向访客传送虚拟接入点标识符和密码
410
访客使用虚拟接入点标识符和密码与虚拟接入点进行关联，以及获得针对网络的接入
411
接入点拒绝接入请求
412
网络管理者向访客设备转发接入拒绝

图4A

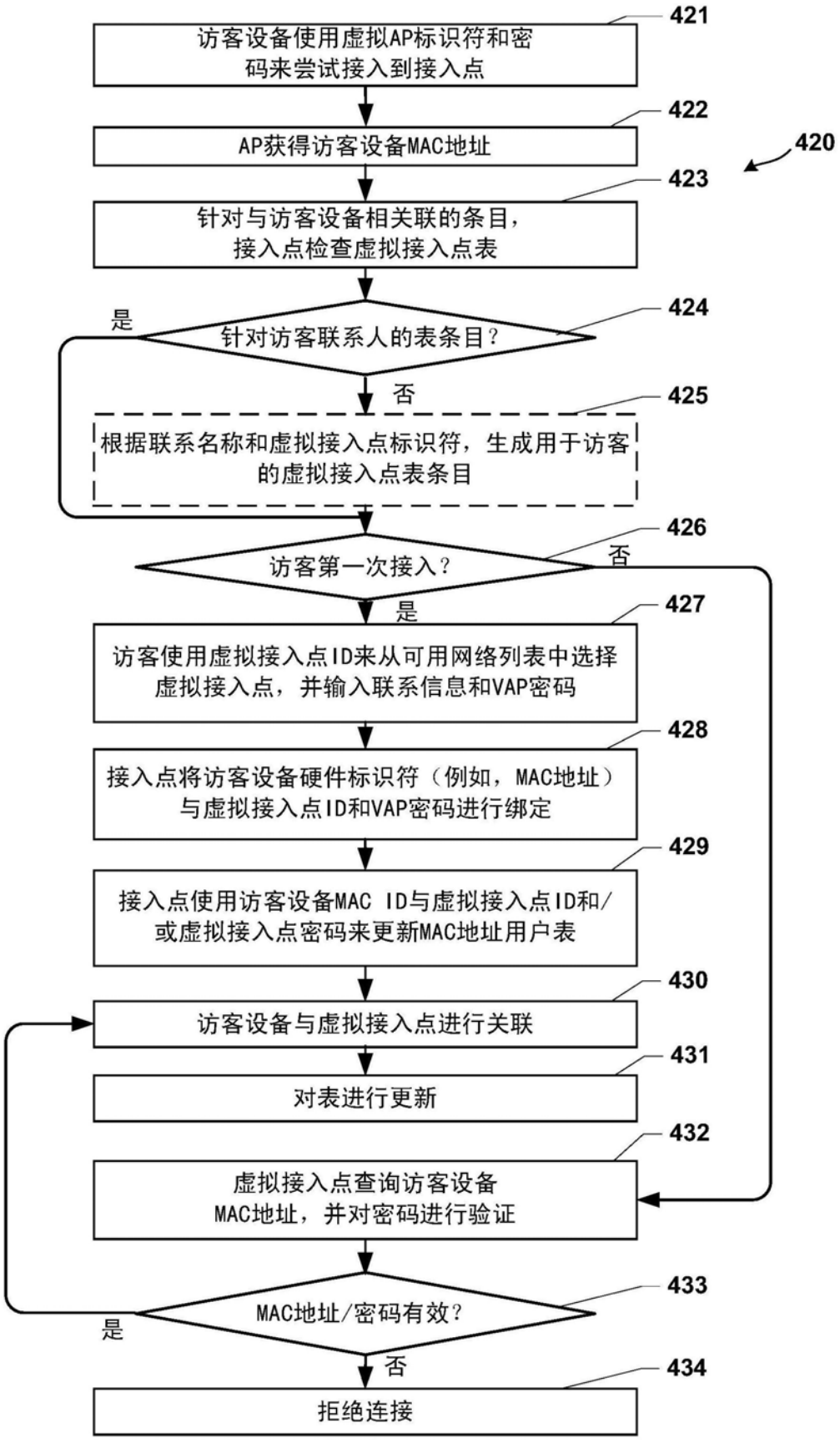

421
访客设备使用虚拟AP标识符和密码来尝试接入到接入点
422
AP获得访客设备MAC地址
420
423
针对与访客设备相关联的条目，接入点检查虚拟接入点表
424
是
针对访客联系人的表条目？
否
425
根据联系名称和虚拟接入点标识符，生成用于访客的虚拟接入点表条目
426
否
访客第一次接入？
是
427
访客使用虚拟接入点ID来从可用网络列表中选择虚拟接入点，并输入联系信息和VAP密码
428
接入点将访客设备硬件标识符（例如，MAC地址）与虚拟接入点ID和VAP密码进行绑定
429
接入点使用访客设备MAC ID与虚拟接入点ID和/或虚拟接入点密码来更新MAC地址用户表
430
访客设备与虚拟接入点进行关联
431
对表进行更新
432
虚拟接入点查询访客设备MAC地址，并对密码进行验证
433
是
MAC地址/密码有效？
否
434
拒绝连接

图4B

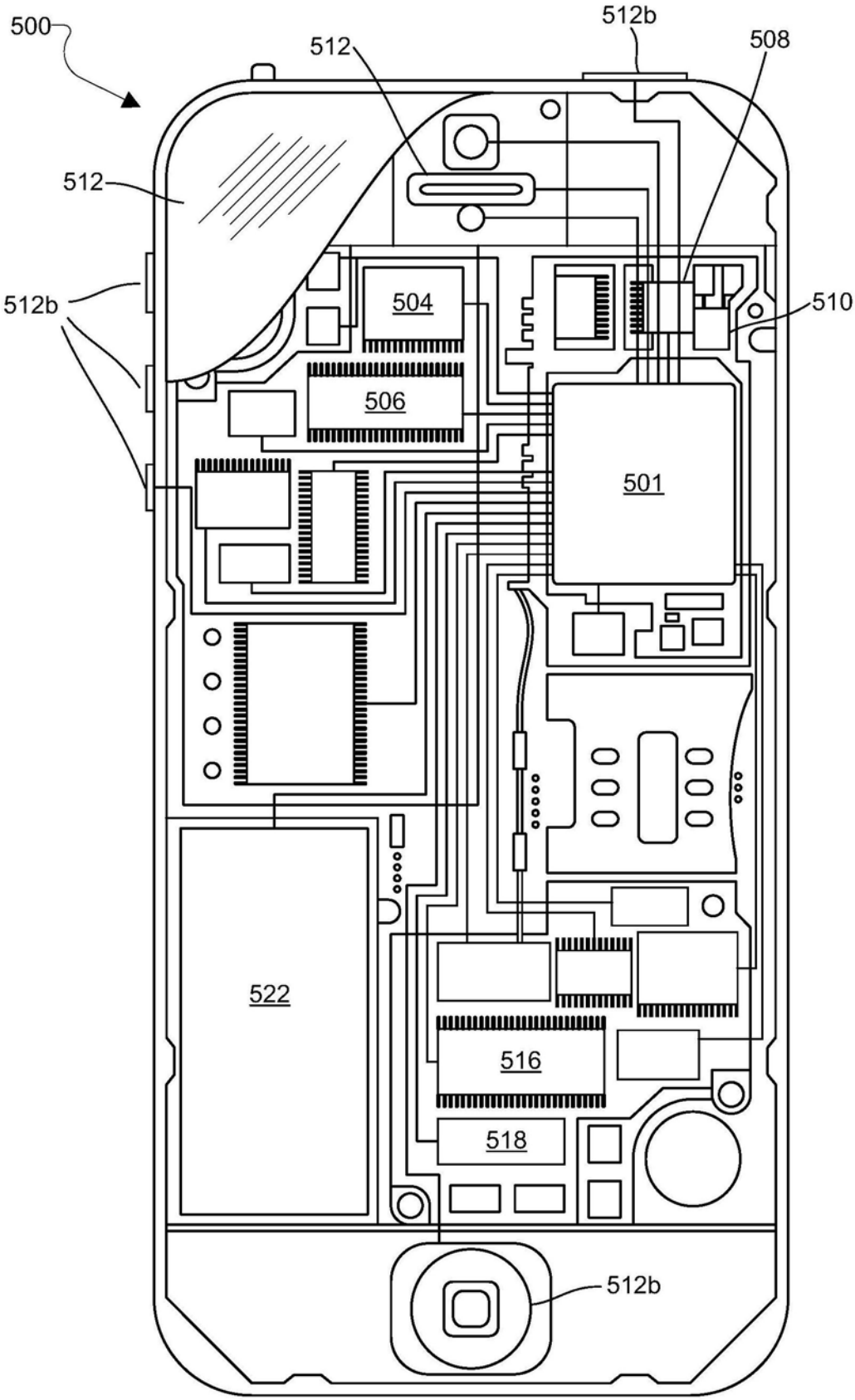


图5

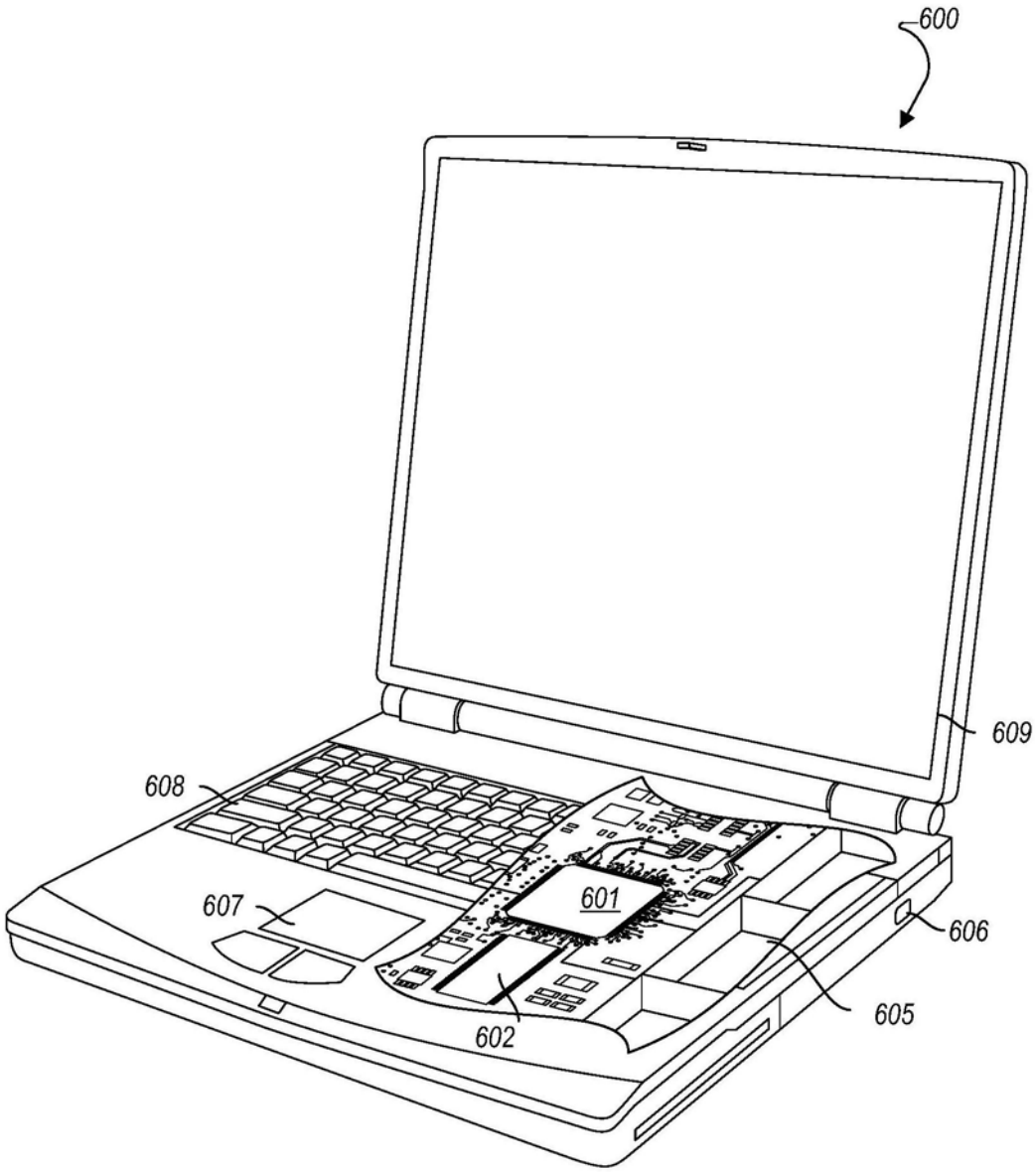


图6