[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510116571.2

[43] 公开日 2006 年 4 月 5 日

[11] 公开号 CN 1756165A

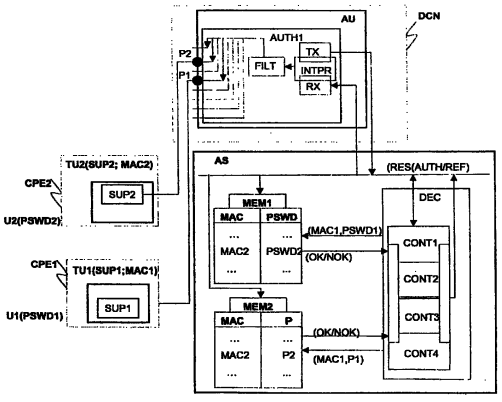
[22] 申请日 2005.9.13
[21] 申请号 200510116571.2
[30] 优先权
[32] 2004. 9.13 [33] EP [31] 04292201.3
[71] 申请人 阿尔卡特公司
地址 法国巴黎
[72] 发明人 J·E·R·德耶格
E·A·C·西克斯
M·A·T·贝克
D·帕帕季米特里乌
[74] 专利代理机构 北京市中咨律师事务所
代理人 杨晓光 李 峥
权利要求书 5 页 说明书 18 页 附图 1 页

[54] 发明名称

一种许可接入数据通信网络的方法和相关设备

[57] 摘要

公开了许可申请方接入数据通信网络的方法和相关设备。 第一申请方关联于媒体访问控制地址并且被耦合到数据通信网络的验证器的第一端口。 该方法包括：由验证器发送验证请求给与其耦合的验证服务器的步骤；和由验证服务器基于预定义的规则和条件进行验证判定的步骤；以及由验证服务器将验证答复发送给验证器的步骤，该验证答复包括验证判定的结果。 该方法还包括由验证服务器产生包括条目的第一注册存储器的步骤。 预定义的规则和条件包括在出现早先条目时控制第一注册存储器的第一控制步骤。 如果第一控制步骤是肯定的，则该方法还包括产生包括验证的结果的步骤，并且由此许可第一申请方通过验证器的第一端口接入数据通信网络。



1. 一种许可第一申请方接入数据通信网络的方法，所述第一申请方具有关联的第一媒体访问控制地址，并且被耦合到所述数据通信网络的验证器的第一端口，

所述方法包括:

由所述验证器向与其耦合的验证服务器发送验证请求的步骤；和

由所述验证服务器基于预定义的规则和条件来进行验证判定的步骤；以及

由所述验证服务器向所述验证器发送包括所述验证判定的结果的验证答复的步骤，其特征在于，所述方法还包括下面的步骤:

由所述验证服务器产生包括条目的第一注册存储器，由此，条目包括在被许可的申请方的媒体访问控制地址和所述被许可的申请方的被许可密码之间的关联，所述被许可的申请方先前接收到许可以接入所述数据通信网络;

并且其特征还在于，所述预定义的规则和条件包括第一控制步骤，该第一控制步骤在出现在先条目时控制所述第一注册存储器，该在先条目包括所述第一申请方的所述第一媒体访问控制地址和所述第一申请方的第一密码之间的第一关联；以及

由此，如果所述第一控制步骤是肯定的，则所述方法还包括:

产生结果的步骤，该结果包括针对具有所述第一密码的所述第一媒体访问控制地址的验证，并且由此许可所述第一申请方通过所述验证器的所述第一端口接入所述数据通信网络。

2. 根据权利要求 1 的许可申请方接入数据通信网络的方法，由此，如果所述第一控制步骤是否定的，则所述方法还包括:

第二控制步骤，其在出现在先条目时控制所述第一注册存储器，所述在先条目包括在所述第一申请方的所述第一媒体访问控制地址与另一个密码之间的第二关联，

由此，如果所述第二控制步骤是否定的，则所述方法还包括下面的步骤:

产生结果，该结果包括针对具有所述第一密码的所述第一媒体访问控制地

址的验证，并且由此许可所述第一申请方通过所述验证器的所述第一端口接入所述数据通信网络；并且包括下面的步骤:

利用所述第一关联将条目注册在所述第一注册存储器中，所述第一关联是在所述第一申请方的所述第一媒体访问控制地址和所述第一申请方的所述第一密码之间的关联。

3. 根据权利要求 2 的许可申请方接入数据通信网络的方法，由此，所述方法还包括:

由所述验证服务器产生包括条目的第二注册存储器，由此，条目包括在被许可的申请方的媒体访问控制地址和用于所述被许可的申请方的被验证端口之间的关联，所述被许可的申请方先前接收到许可以通过所述被验证的端口接入被允许的数据通信网络；并且

如果所述第二控制步骤是否定的，则还利用关联将条目注册在所述第二注册存储器中，所述关联是在所述第一申请方的所述第一媒体访问控制地址和所述验证器的所述第一端口之间的关联。

4. 根据权利要求 3 的许可申请方接入数据通信网络的方法，由此，如果所述第二控制步骤是肯定的，则所述方法还包括:

第三控制步骤，其在出现在先条目时控制所述第二注册存储器，所述在先条目包括在所述第一申请方的所述第一媒体访问控制地址与所述验证器的所述第一端口之间的第三关联；和

第四控制步骤，其在出现在先条目时控制所述第二注册存储器，所述在先条目包括所述第一申请方的所述第一媒体访问控制地址与所述验证器的另一个端口之间的第四关联；和

如果所述第三控制步骤是肯定的，则所述方法还包括产生结果的步骤，该结果包括针对具有所述第一密码的所述第一媒体访问控制地址的验证，并且由此许可所述第一申请方通过所述验证器的所述第一端口接入所述数据通信网络；和

如果所述第三控制步骤是否定的并且所述第四控制步骤是肯定的，则产生结果，该结果包括针对所述第一端口和所述第一媒体访问控制地址的拒绝，并且由此拒绝所述第一申请方通过所述第一端口接入所述数据通信网络。

5. 一种验证服务器，其在从所述验证器接收到验证请求时，向验证器发送包括验证判定的结果的验证答复，所述验证服务器包括:

判定装置，其用来基于预定义的规则和条件产生所述结果，所述验证请求涉及许可第一申请方接入数据通信网络的请求，所述第一申请方具有关联的第一媒体访问控制地址，并且被耦合到所述数据通信网络的所述验证器的第一端口，其特征在于，所述验证服务器还包括:

第一注册存储器，其被耦合到所述判定装置，所述第一注册存储器包括条目，由此，条目包括在被许可的申请方的媒体访问控制地址和所述被许可的申请方的密码之间的关联，所述被许可的申请方先前接收到许可以通过被验证的端口接入被允许的数据通信网络，该被许可的申请方通过所述被验证的端口而被耦合到所述验证器；其特征还在于，

所述判定装置包括第一控制装置，以在出现在先条目时执行对所述第一注册存储器的第一控制，所述在先条目包括所述第一申请方的所述第一媒体访问控制地址和所述第一申请方的第一密码之间的第一关联；并且其特征还在于，

还包括所述判定装置，从而如果所述第一控制是肯定的则产生结果，该结果包括针对所述第一端口和所述第一媒体访问控制地址的验证，由此所述第一申请方被许可通过所述验证器的所述第一端口接入所述数据通信网络。

6. 根据权利要求 5 的验证服务器，其中，所述验证服务器的所述判定装置还包括第二控制装置，从而如果所述第一控制是否定的，则在出现在先条目时执行对所述第一注册存储器的第二控制，所述在先条目包括在所述第一媒体访问控制地址与另一个密码之间的第二关联，并且

由此，如果所述第二控制是否定的，

则所述判定装置产生结果，该结果包括针对所述第一端口和所述第一媒体访问控制地址的验证，由此，所述第一申请方被许可通过所述验证器的所述第一端口接入所述数据通信网络。

7. 根据权利要求 6 的验证服务器，其中，所述验证服务器还包括:

第二注册存储器，其被耦合到所述判定装置，所述第二注册存储器包括条目，由此，条目包括在被许可的申请方的媒体访问控制地址和所述被许可的申请

方的被验证的端口之间的关联，所述被许可的申请方先前接收到许可以通过所述被验证的端口接入被允许的数据通信网络，该被许可的申请方通过所述被验证的端口而被耦合到所述验证器；并且

如果所述第二控制是否定的，则所述验证服务器还利用关联将条目注册到所述第二注册存储器中，所述关联是在所述第一申请方的所述第一媒体访问控制地址和所述第一申请方的所述第一端口之间的关联。

8. 根据权利要求 7 的验证服务器，其中，所述判定装置还包括:

第三控制装置，其用来在出现在先条目时执行对所述第二注册存储器的第三控制，所述在先条目包括在所述第一申请方的所述第一媒体访问控制地址与所述验证器的所述第一端口之间的第三关联；和

第四控制装置，其用来在出现在先条目时执行对所述第二注册存储器的第四控制，所述在先条目包括在所述第一申请方的所述第一媒体访问控制地址与所述验证器的另一个端口之间的第四关联；并且

还包括所述判定装置，从而如果所述第二控制是肯定的并且所述第三控制是肯定的，则产生结果，该结果包括针对所述第一端口和所述第一媒体访问控制地址的验证，由此，所述第一申请方被许可通过所述验证器的所述第一端口接入所述数据通信网络；以及

还包括所述判定装置，从而如果在所述第二控制是肯定的并且所述第三控制是否定的以及所述第四控制是肯定的，则产生结果，该结果包括针对所述第一端口和所述第一媒体访问控制地址的拒绝，由此，所述第一申请方被拒绝通过所述验证器的所述第一端口接入所述数据通信网络。

9. 一种验证器，其期望能使第一申请方接入数据通信网络，所述第一申请方具有关联的第一媒体访问控制地址，并且被耦合到所述数据通信网络的所述验证器的第一端口，

所述验证器因此包括:

发射机，用来发送验证请求到验证服务器，该验证服务器被耦合到所述验证器；和

接收机，用来从所述验证服务器接收验证答复，该验证答复包括基于预定

义的规则和条件的验证判定的结果，其特征在于:

所述验证器包括解释器，其用来解释如同从根据权利要求 5 的验证服务器所接收的所述验证答复，并且相应地设置所述验证器的滤波器，由此

当所述结果包括针对所述第一端口和所述第一媒体访问控制地址的验证时，由此，具有所述第一媒体访问控制地址的所述第一申请方被许可通过所述验证器的所述第一端口接入所述数据通信网络，所述滤波器仅对于所述第一媒体访问控制地址来通过所述第一端口接受所述第一申请方的业务；并且由此

当所述结果包括针对所述第一端口和所述第一媒体访问控制地址的拒绝时，由此，具有所述第一媒体访问控制地址的所述第一申请方被拒绝通过所述验证器的所述第一端口接入所述数据通信网络，所述滤波器拒绝所述第一申请方的业务。

一种许可接入数据通信网络的方法和相关设备

技术领域

本发明涉及一种许可申请方（supplicant）接入数据通信网络的方法。本发明还涉及一种实现该方法的验证服务器和验证器。已经从IEEE标准802.1X-2001获知了所述方法和设备。

背景技术

在IEEE标准802.1X-2001中，在第5页§3.1描述了申请方是位于点对点局域网网段的一端的实体，该实体由连接于该链路的另一端的验证器来验证。应当说明，该文献使用术语申请方而不是例如同级设备（peer）的设备，该同级设备被用在其它接入控制相关的规范中。

在第5页§3.1还描述了网络接入端口是到LAN（局域网）的系统连接点。它可以是物理端口，例如，连接到物理LAN网段的单个LAN媒体访问控制，或者是例如站和接入点之间的关联的逻辑端口。应当指出，术语“端口”在该文献中被用作网络接入端口的缩写。

此外，还描述了验证器是在点对点LAN网段的一端的实体，该验证器有助于验证连接到该链路另一端的实体。所述验证器负责与申请方通信，并负责将从所述申请方接收的信息提交给合适的验证服务器，以确保进行凭证（credential）检查并确定由此引起的状态。

验证服务器是向验证器提供验证服务的实体。该服务根据由申请方提供的凭证，来确定该申请方是否被授权接入由验证器提供的服务。验证服务器的功能可以通过验证器来配置，或者可以经由验证器能够接入的网络来远程接入。

这样，该方法许可申请方接入数据通信网络，由此该申请方与媒体访问控制地址相关，并且被耦合到该数据通信网络的验证器的端口，该方法包括以下步骤:

－由验证器向与其耦合的验证服务器发送验证请求的步骤；和

－由验证服务器基于预定义的规则和条件来进行验证判定的步骤；以及

－由验证服务器向验证器发送包括验证判定的结果的验证答复的步骤。

此外，在该 IEEE 标准 802.1X-2001 第 10 页，论述了验证器和验证服务器之间通信的细节是在该 IEEE 标准 802.1X-2001 的范围之外。然而，这种通信典型地能够通过在此简称为 EAP 的可扩展验证协议（Extensible Authentication Protocol）来实现，连接例如通过 EAP RADIUS 而被承载在合适的较高层协议上。因此，验证服务器可位于 LAN 的边界之外，该 LAN 支持申请方和验证器之间的“LAN 上的 EAP”即 EAPOL 申请方交换；并且验证器和验证服务器之间的通信不需要服从于相关系统的受控端口的验证状态。

这样，根据这个可能的实现，并且如 2000 年 6 月的 IETF RFC 2865 -§2Operation/Introduction 所描述的那样，如 RADIUS 服务器的验证服务器接收请求，其批准发送客户端（即验证器），并且其查找用户（即申请方）的数据库来找到其姓名与该请求匹配的用户。数据库中的用户条目包括要求列表，该要求列表必须被满足以允许用户的接入。这主要包括密码检验，但是也可以指定允许用户接入的端口的客户端。而且，在该标准的第 6 页描述了，如果所有条件都满足，则用户（即申请方）的配置值的列表被置入“接受”响应中。这些值包括服务类型和传送所期望的服务的所有必需值。这些值可以包括例如下列值: IP 地址、子网掩码、期望的压缩，以及期望的分组过滤标识符或期望的协议和主机。

由验证服务器基于预定义的规则和条件进行验证判定的步骤也在 IEEE 标准 802.1X-2001 的第 7 页被描述，即验证服务器代表验证器来执行验证功能以检查申请方的凭证，并且指示申请方是否被授权接入验证器的服务。这样，端口接入控制提供系统功能性的扩展，这提供了阻止未授权的申请方接入由该系统提供的服务的方法。例如，如果该相关系统是 MAC 网桥，则可以期望对网桥和其所连

接的 LAN 的接入上的控制，以限制对公共可接入的网桥端口的接入，或者在机构内限制部门的成员对该部门 LAN 的接入。

通过连接到系统的受控端口的申请方的系统强制验证来实现接入控制。根据验证过程的结果，系统能够确定申请方是否被授权在该受控端口上接入其服务。如果申请方没有被授权接入，则系统将受控端口状态设置为未授权。可以应用所定义的机制来允许任何系统验证连接到其受控端口之一的另一个系统。相关系统包括终端站、服务器、路由器以及 MAC 网桥。

应当注意，在 IEEE 标准 802.1X-2001 的第 21 页§8.2，描述了基于端口的接入控制的操作假定在其上进行操作的端口提供单个申请方和单个验证器之间的点对点连接。该假定允许基于每个端口来进行验证判定。此外，“连接到单个验证器的多个申请方的验证在该标准的范围之外”。然而应当说明，为了不超出本说明书和图 1，在权利要求的导言中及在说明书中所描述的验证器，是如在标准中所描述的多个验证器的综合。然而应当理解，在上述标准 802.1X-2001 中的验证判定保持基于每个端口。而且，本发明的验证器能根据在不同端口上的分配方式来被实现，这使其恢复成在申请方和验证器之间的一对一关系。

现在将通过例子来描述这种方法的突出问题，即许可例如 SUP1 的申请方接入数据通信网络。假定下面的拓扑，其中，第一用户使用具有第一申请方 SUP1 的第一客户端设备，该第一申请方 SUP1 被耦合到包括验证器 AUTH1 的接入单元的第一端口 P1；并且第二用户使用具有第二申请方 SUP2 的第二客户端设备，该第二申请方 SUP2 被耦合到该接入单元的第二端口 P2。所述许可第一申请方 SUP1 接入验证器的数据通信网络 DCN 的方法包括:

由验证器 AUTH1 向与其耦合的验证服务器 AS 发送验证请求的步骤；和

由验证服务器 AS 基于预定义的规则和条件进行验证判定的步骤；以及

由验证服务器 AS 向验证器发送包括所述验证判定的结果的验证答复的步骤。

如上所述，所述验证判定包括必须被满足以允许用户接入的要求列表。该列

表主要包括密码检验，但是也能指定用户被允许接入的端口的客户端。假定基于第一用户的密码检验，第一申请方 SUP1 被授权通过验证器的第一端口 P1 接入通信网络。

现在，许可第二申请方 SUP2 接入验证器的数据通信网络的方法包括类似的步骤。基于第二用户的密码检验，第二申请方 SUP2 被授权通过验证器的第二端口 P2 来接入通信网络。然而，当第二客户端设备使用与第二申请方 SUP2 相关联的例如 MAC2 的媒体访问控制地址时，结果还包括针对该第二申请方的验证，其例如恰好具有与媒体访问控制地址 MAC1 相同的值，该媒体访问控制地址 MAC1 由第一客户端设备来使用，即与第一申请方 SUP1 相关联。这意味着与媒体访问控制地址是否具有相同值这一事实无关，每个申请方将仅通过符合密码要求来接收其许可。这导致 MAC 地址重复并由此导致服务拒绝和/或服务降级攻击。

这种 MAC 地址重复通常通过在 MAC 数据平面或因特网协议层数据平面中的解决方案而被解决，例如接入节点本身中的 MAC 地址转换、VLAN 隔离（segregation）或 MAC 地址注册。

通过上面的方法，MAC 地址重复主要在一个接入节点中被解决而与其它接入节点无关，并且假定 MAC 地址重复是极少有的事件，这是因为用户不能获知彼此的 MAC 地址。然而，当在同一接入节点的用户和不同接入节点的用户之间允许直接对等（peer-to-peer）通信时，所述解决方案失效。当允许对等通信时，用户还将获知彼此的 MAC 地址并且因此任何用户能够窃取另一个用户的 MAC 地址。此外，这还将导致服务拒绝和/或服务降级攻击。

此外，已知的验证方法将用户凭证即其密码关联于其 DSL 线路即验证器 AUTH1 的端口，由此不允许用户的游动（nomadism）。这意味着上述第一用户将不被允许进入第二用户的住宅并利用其个人密码（第一用户的密码）来使用第二用户的第二申请方的计算机；或者这意味着上述第一用户将不被允许进入第二用户的住宅以便在那里利用其个人密码（第一用户的密码）来使用（第一用户）自己的计算机。

发明内容

本发明的目的是提供一种许可申请方接入数据通信网络的方法以及实现该方法的验证服务器和验证器，如上面已知的那样，但由此允许用户游动并且由此阻止媒体访问控制地址窃取。

根据本发明，通过所述方法、验证服务器和验证器来实现所述目的。实际上应归于该方法还包括由验证服务器产生包括条目的第一注册存储器的步骤这一事实。一个这样的条目包括在被许可的申请方的媒体访问控制地址和所述被许可的申请方的密码之间的关联，所述被许可的申请方先前接收到许可以通过验证端口来接入被允许的数据通信网络。此外，预定义的规则和条件包括第一控制步骤，该第一控制步骤在出现在先条目时通过判定装置的第一控制装置来控制第一注册存储器，所述在先条目包括第一申请方的媒体访问控制地址和该第一申请方的密码之间的第一关联。此外，如果该第一控制步骤是肯定的，则该方法还包括这样的步骤：产生结果并且由此许可第一申请方通过验证器的第一端口来接入数据通信网络，所述结果包括针对具有第一密码的第一媒体访问控制地址的验证。

事实上，由于注册存储器被建立，因此所有申请方都通过包括例如（MAC2，PSWD2）的对的条目而被注册到所述第一注册存储器中（与申请方关联的 MAC 地址；使用包括该申请方的客户端设备的用户的密码），所述所有申请方例如是 SUP2，其先前接收到验证，即对接入被允许的数据通信网络的许可。一旦验证服务器从验证器接收到对于期望接入的例如 SUP1 的特定申请方的新的验证请求，验证服务器就首先对于该特定申请方在第一注册存储器中控制关联条目的出现（特定申请方的关联的 MAC 地址；用于该申请方的用户的密码），所述关联条目即所述例如（MAC1，PSWD1）的对。当这种关联条目出现在数据库即第一注册存储器中时，第一用户使用的第一申请方被授权接入。即使当该第一用户不在其自己的位置时，只要该特定关联（MAC1，PSWD1）存在，就允许对网络的接入。

通常在验证器的验证请求中找到信息和用于申请方的密码，所述信息即特定

申请方的关联的MAC地址，所述密码即使用包括该申请方的客户端设备的用户的密码。

除了执行通常的规则和条件之外，验证服务器的所述第一控制步骤的执行，即考虑MAC地址/用户密码的关系，提供了改进的验证判定结果，即该结果现在允许用户在数据通信网络中游动。

此外，验证器包括解释器，以解释从验证服务器接收的验证答复，该验证服务器事实上考虑了所述（MAC 地址，用户密码）关联。该解释器还根据验证答复中的结果的内容来设置该验证器的滤波器。因此，当该结果包括针对媒体访问控制地址和用户密码的验证时，由此具有该媒体访问控制地址的申请方事实上被许可通过验证器的端口接入数据通信网络，所述滤波器被设置成通过该端口接受申请方的业务，但是仅对于指定的媒体访问控制地址。类似地，当所述结果包括针对具有用户密码的媒体访问控制地址的拒绝时，由此具有该媒体访问控制地址的申请方被拒绝通过验证器的端口接入数据通信网络，所述滤波器被设置成拒绝申请方的所有业务。

这意味着仅对于关联于申请方的用户密码的MAC地址，来许可该申请方通过验证器的端口接入数据通信网络，针对所述MAC地址而成功地实现所述验证过程。

因此，如果由验证服务器执行的第一控制步骤是肯定的，则根据本发明的方法包括由判定装置产生结果的步骤，所述结果包括验证，由此许可具有媒体访问控制地址和关联的用户密码的申请方通过验证器的端口接入所述数据通信网络。这意味着当在注册存储器中找到请求对（MAC 地址，密码）的第一完全匹配时，这种相同的对（MAC 地址，密码），即这种具有相同密码的相同申请方，已经先前接收到对接入通信网络的许可。所述申请方的客户端设备的用户期望再次接入所述网络。即使在不同的接入线路，准许再次接入也允许用户游动。

而且，如果第一控制步骤是否定的，则该方法还包括由第二控制装置执行的第二控制步骤，该第二控制步骤在出现在先条目时控制所述第一注册存储器，该在先条目包括申请方的媒体访问控制地址与任何其它密码之间的第二关联，即关

于与第一注册存储器的条目的半匹配的检查。事实上，即使当所述条目与另一个密码相关联时，在出现例如SUP2的申请方的MAC地址时控制所述第一注册存储器，所述另一个密码比如是这样的密码：针对该密码而为申请方请求接入。如果第二控制步骤是否定的，则该方法还包括由判定装置产生结果的步骤，所述结果包括针对具有第一密码的第一媒体访问控制地址的验证，并且由此许可第一申请方通过验证器的第一端口接入数据通信网络。而且，该方法包括这样的步骤：利用第一申请方的第一媒体访问控制地址和第一申请方的第一密码的第一关联，在第一注册存储器中注册条目。事实上，当第一媒体访问控制地址根本没有出现时，既不与第一用户密码关联也不与另一个用户密码关联，这意味着没有提供在先接入。这涉及到被允许的新的接入。因此，需要完善第一注册存储器并插入申请方的第一媒体访问控制地址和用户密码之间的新获知的关联。

应当注意，“第二关联”这一表述不意味着MAC地址应当在注册装置中针对第二时间而被找到。“第二关联”仅意为“第二种关联”，即将在第一注册存储器中查找的“第二种条目”。更准确地，关于对（MAC地址；除了针对其接收请求的密码之外的任何其它密码）的先前条目的出现由第二控制装置来控制。

此外，该方法还包括由验证服务器产生包括条目的第二注册存储器，由此条目包括在被许可的申请方的媒体访问控制地址和用于被许可的申请方的被验证端口之间的关联，该被许可的申请方先前接收到许可以通过被验证端口接入所允许的数据通信网络；并且如果第二控制步骤是否定的，则还利用第一申请方的第一媒体访问控制地址和验证器的第一端口之间的关联而在第二注册存储器中注册条目。这意味着除了具有媒体访问控制地址与密码之间的关联的条目之外，还保持具有媒体访问控制地址与验证器的端口之间的关联的条目，申请方经由该端口被耦合到验证器。

此外，如果所述第二控制步骤是肯定的，则该方法还包括：

－第三控制步骤，即在出现包括第三关联的在先条目时利用第三控制装置来控制所述第二注册存储器，所述第三关联是第一申请方的第一媒体访问控制地址与验证器的第一端口之间的关联；和

－第四控制步骤，即在出现包括第四关联的在先条目时利用第四控制装置来控制所述第二注册存储器，所述第四关联是第一申请方的第一媒体访问控制地址与验证器的另一个端口之间的关联；和

－如果所述第三控制步骤是肯定的，则该方法还包括产生结果的步骤，该结果包括针对具有第一密码的第一媒体访问控制地址的验证，并且由此许可第一申请方通过验证器的第一端口接入数据通信网络；和

－如果第三控制步骤是否定的并且第四控制步骤是肯定的，则产生结果，该结果包括针对第一端口和第一媒体访问控制地址的拒绝，并且由此拒绝第一申请方通过第一端口接入数据通信网络。

通过包括所述第三和第四控制步骤，在出现关于要求接入网络的申请方的媒体访问控制地址的条目时，还检查第二注册存储器。如果第一媒体访问控制地址与另一个密码的关联在第一注册存储器中被找到，并且该第一媒体访问控制地址也在第二注册存储器中被找到，则第二注册存储器中的关联的端口起作用。当该关联的端口实际上是第一申请方经由其请求接入的端口，即第一端口时，提供验证，这是因为这意味着用户是位于另一个住宅，利用其自己的（第一用户）密码使用该住宅的计算机，即用户游动。

最后，当第一媒体访问控制地址除了与另一个密码关联之外还在关联于另一个端口的第二注册存储器的条目中被找到时，该第一媒体访问控制地址被窃取，由此接入被拒绝，即验证服务器由此拒绝与第一媒体访问控制地址关联的第一申请方来通过验证器的被请求端口接入数据通信网络。实际上，即使在另一个端口，当所述 MAC 地址已经先前被注册到注册存储器中时允许具有特定 MAC 地址的申请方接入数据网络，将会产生 MAC 重复。关联于另一个端口的 MAC 地址的注册存储器中的条目的出现，意味着请求的申请方恰好具有与已经被注册的 MAC 地址相同的特定 MAC 地址，或者意味着恶意用户已在窃取该特定 MAC 地址并企图使用它。在这两种情况下都应避免由具有该特定 MAC 地址的申请方接入数据通信网络。这通过在判定装置的结果中包括拒绝而被实现。

应当说明，通过由判定装置产生包括验证的结果来许可接入。

应当注意，在权利要求中使用的术语“包括”不应当被解释成限于其后列出的装置。因此，“包括装置 A 和 B 的设备”这一表述的范围不应当限于仅由部件 A 和 B 组成的设备。其意味着所述设备关于本发明的相关部件是 A 和 B。

类似地，应当注意，也在权利要求中使用的术语“耦合”不应当被解释成仅限于直接连接。因此，“耦合到设备 B 的设备 A”这一表述的范围不应当限于设备 A 的输出被直接连接到设备 B 的输入的设备或系统。其意味着在 A 的输出和 B 的输入之间存在路径，该路径可能包括其它设备或装置。

附图说明

结合附图，通过参考下面对实施例的描述，本发明的上述和其它目的和特征将变得更加明显，本发明本身将被很好地理解，其中，图 1 示出了全球通信网络。

具体实施方式

将通过图 1 所示的不同块的功能描述，来解释其依照图中示出的电信环境的根据本发明的设备的工作。基于该描述，所述块的实际实现对于本领域的技术人员来说是显而易见的，并且因此将不对其作详细描述。此外，许可申请方接入数据通信网络的方法的原理工作将被更详细地描述。

参考图 1，示出了全球电信网络。

所述全球电信网络包括两个客户端设备，即第一客户端设备 CPE1 和第二客户端设备 CPE2；数据通信网络 DCN 和验证服务器 AS。

第一和第二客户端设备 CPE1 和 CPE2，每个都被耦合到数据通信网络 DCN。

验证服务器 AS 也被耦合到数据通信网络 DCN。

第二客户端设备 CPE2 包括终端单元 TU2。该终端单元 TU2 包括申请方 SUP2 并且具有媒体访问控制地址 MAC2。

另一个客户端设备 CPE1 包括终端单元 TU1。该终端单元 TU1 具有 MAC

地址 MAC1 并且包括申请方 SUP1。这样，申请方 SUP1 与 MAC1 地址关联。

假定在通常情况下，第一和第二客户端设备 CPE1 和 CPE2 分别由具有密码 PSWD1 的第一用户 U1 和具有密码 PSWD2 的第二用户 U2 使用。

数据通信网络 DCN 包括接入单元，该接入单元包括多个端口。两个端口 P1 和 P2 被明确示出。所述接入单元的这两个端口被耦合到所述客户端设备的每一个。更详细地，第一客户端设备 CPE1 通过接入单元 AU 的第一端口 P1 被耦合到数据通信网络 DCN，并且另一个客户端设备 CPE2 通过接入单元 AU 的另一个端口 P2 被耦合到数据通信网络。接入单元 AU 包括验证器 AUTH1，验证器 AUTH1 包括发射机 TX，接收机 RX 和滤波器 FILT。发射机 TX 和接收机 RX 都被耦合到验证服务器 AS。发射机 TX 和接收机 RX 也被耦合到解释器 INTPR，该解释器还被耦合到滤波器 FILT。根据该实施例，滤波器 FILT 也被耦合到接入单元 AU 的不同端口。到两个端口 P1 和 P2 的耦合在图 1 中明确示出。到其它端口的耦合仅用虚线示出。

验证服务器 AS 包括判定器 DEC，该判定器被耦合到验证服务器 AS 的输入/输出。判定器 DEC 包括第一控制器 CONT1、第二控制器 CONT2、第三控制器 CONT3 和第四控制器 CONT4。

验证服务器 AS 还包括注册存储器 MEM，该注册存储器被耦合到验证服务器 AS 的输入/输出并且被耦合到判定器 DEC。

申请方 SUP1 和 SUP2，验证器 AUTH1 和验证服务器 AS 能够互相通信以执行验证过程并且由此最后许可申请方 SUP1 或 SUP2 通过其各自的验证器的端口来接入数据通信网络。

现在将更详细地说明所述情况。

在 IEEE 标准 802.1X-2001 第 8 页说明了受控的和不受控的接入。基于端口的接入控制的操作具有这样的效果：创建两个不同的接入点（在图 1 中未示出）到验证器系统的连接点，该连接点连接到局域网 LAN。一个接入点允许下面称为 PDU 的分组数据单元在所述系统和 LAN 上的其它系统之间的不受控交换，而

与验证状态无关，即不受控的端口；另一个接入点仅在端口的当前状态是被授权的即受控端口的情况下才允许 PDU 交换。不受控的和受控的端口被认为是到 LAN 的相同连接点的一部分，例如用于与验证器 AUTH1 协作的申请方 SUP1 的端口 P1。在物理端口上接收的任何帧都可用于受控的和不受控的端口；服从于与受控端口关联的验证状态。

此外，还参见 802.1X-2001 第 8 页最后一段，可以通过能够提供到申请方系统的一对一连接的任何物理或逻辑端口，来提供到 LAN 的连接点。例如，在交换 LAN 基础设施中的单个 LAN MAC 能提供连接点。在 LAN 环境中，在单个申请方和单个验证器之间的不同关联的创建，对于运行 802.1X-2001 中描述的接入控制机制而言是必要的前提，在所述 LAN 环境中，MAC 方法允许在验证器和申请方之间的一个对多个关系的可能性，例如在共享媒体环境中。

应当指出，如上所述，每个都关联于不同申请方的不同单个验证器的功能性可以被集成到一个负责不同申请方的全局验证器中。这种具有一个被集成验证器 AUTH1 的实现对该特定实施例而言是优选的，然而，这并不限制本发明的原理观点。

现在将说明两个申请方 SUP1 和 SUP2、验证器 AUTH1 和验证服务器 AS，在接入控制机制中的不同作用。

验证器 AUTH1 出于与各个申请方交换协议信息的目的而使用不受控的端口（未示出），并且进一步负责强制分别连接到其受控端口 P1 或 P2 之一的申请方 SUP1 或 SUP2 之一的验证，并且还负责相应地控制各个受控端口的验证状态。

为了执行验证，验证器 AUTH1 利用验证服务器 AS。验证服务器 AS 可以被置于与验证器 AUTH1 相同的系统中，或者可以位于可通过基于 LAN 或其它的远程通信机制来接入的其它位置。该优选实施例描述了验证服务器 AS，其对于同一 DCN 的所有验证器是通用的。实际上，游动需求和 MAC 地址窃取是涉及到验证器所连接的整个以太网通信网络的问题，并且因此应整体上对于 DCN 来解决。这通过将用于所有验证器的同一 AS 连接到同一以太网 DCN 来实现。

申请方 SUP1 或 SUP2 负责响应于来自验证器 AUTH1 的请求而将其凭证传送到验证器 AUTH1。申请方还可以启动验证交换并且执行注销交换。

验证主要发生在系统启动时间，或者在申请方系统被连接到验证器系统的端口时。直到验证已经成功完成，所述申请方系统才具有到验证器系统的接入以执行验证交换，或接入由验证器系统提供的任何服务，该服务不服从于置于验证器的受控端口上的接入控制限制。一旦验证已经成功完成，验证器系统就允许完全接入经由验证器系统的受控端口所提供的服务。

对于该实施例，定义封装格式是优选的，该封装格式允许通过 LAN MAC 服务来直接承载验证消息。称为 LAN 上的 EAP 或 EAPOL 的这种 EAP 的被封装格式，被用于申请方 SUP1 和 SUP2 与验证器 AUTH1 之间的所有通信。验证器 AUTH1 因而执行对于向前传输到验证服务器 AS 的 EAP 协议的重新打包。对于该实施例，RADIUS 优选地用于提供通信的后一方面。但是，应当指出，这可以通过使用其它协议来实现。

此外，当验证过程开始时，可能产生下面的结果之一:

a）由于在请求和响应的先后顺序中的过度超时，因此所述验证过程终止。这造成了中断状态。

b）由于验证服务器 AS 返回“拒绝消息”给验证器 AUTH1，因此验证过程终止，所述“拒绝消息”这里称为“包括含有拒绝的结果的验证答复”。

c）由于验证服务器 AS 返回“接受消息”给验证器 AUTH1，因此验证过程终止，所述“接受消息”这里称为: “包括含有验证的结果的验证答复”。

如上所述，例如 SUP1 的申请方期望接收到许可以接入数据通信网络 DCN。该申请方还与终端单元 TU1 的 MAC1 地址关联，并且被耦合到验证器 AU 的端口 P1。用户密码 PSWD1 由第一用户 U1 来提供给第一客户端设备 CPE1 并经由申请方 SUP1 和第一端口 P1 到达验证器 AU。

为了获得所述许可，验证器 AU 的发射机 TX 发送验证请求到验证服务器 AS。验证服务器 AS 基于预定义的规则和条件来进行验证判定。在此使用验证服

务器 AS 的判定器 DEC。然后，验证服务器 AS 发送包括所述验证判定的结果的验证答复到验证器 AUTH1。

然而，为了进行对于申请方 SUP1 的验证判定，根据本发明，验证服务器 AS 还包括第一注册存储器 MEM1 和第二注册存储器 MEM2。这些注册存储器包括条目。

第一注册存储器的条目包括在例如被许可的申请方 SUP2 的 MAC2 的媒体访问控制地址与例如 PSWD2 的用户密码之间的关联，该被许可的申请方先前接收到许可以利用该用户密码 PSWD2 接入数据通信网络 DCN。

第二注册存储器的条目包括在例如被许可的申请方 SUP2 的 MAC2 的媒体访问控制地址与被验证的端口 P2 之间的关联，该端口 P2 对于被许可的申请方而被验证，该被许可的申请方已经接收到许可以通过该被验证端口 P2 接入数据通信网络 DCN。

判定器 DEC 基于预定义的规则和条件来产生验证判定的结果 RES。所述判定器 DEC 的验证判定的各个结果 RES 被包括在验证答复中，并且通过验证服务器 AS 而被发送到验证器 AUTH1。

验证器 AUTH1 的接收机 RX 从验证服务器 AS 接收所述验证答复。

验证器 AUTH1 的解释器 INTRP 解释从验证服务器 AS 接收的验证答复，根据本发明，该验证服务器实际上是激活的，以通过例如由第一控制器 CONT1 执行的所述第一控制步骤来支持其验证判定。应当说明，所述解释器是通过解码器而被实现的，该解码器对于从验证服务器 AS 接收的验证答复进行解码。

解释器 INTRP 能够以不同的方式来被实现。一个可能的方式是解释器 INTRP 根据包括在验证答复中的参考，知道其涉及哪个先前被发送的验证请求，并且由此知道其涉及哪个例如 SUP1 的申请方。解释器 INTRP 被激活，以基于该申请方 SUP1 从验证器 AUTH1 的数据库检索关联的 MAC 地址和端口，即 MAC1 和 P1。另一个可能的实现是不保持验证请求数据库并且解释器 INTRP 依赖于所述验证答复中的信息。这意味着解释器 INTRP 从验证答复检索包括在该

验证答复中的端口和 MAC 地址。

根据这些可能的实现，所述信息被转发给滤波器 FILT，该信息即相关的 MAC 地址和端口，即例子中的 MAC1 和 P1。根据包括在验证答复中的信息来设置滤波器 FILT，并且该滤波器 FILT 还相应地对端口 P1 的业务进行滤波。这意味着:

－当结果 RES（AUTH）包括对 MAC1 地址的验证时，由此具有该 MAC1 地址的申请方 SUP1 实际上被许可经由验证器 AU 的端口 P1 接入数据通信网络 DCN，滤波器 FILT 经由端口 P1 接受申请方 SUP1 的业务，但是仅对于为其给出验证的 MAC1 地址；并且

－当结果 RES（REF）包括对 MAC1 地址的拒绝时，由此具有该 MAC1 地址的申请方 SUP1 被拒绝经由验证器 AU 的端口 P1 接入数据通信网络 DCN，滤波器 FILT 拒绝具有 MAC1 地址的申请方 SUP1 的业务。

应当指出，滤波器 FILT 可以通过用于验证器 AUTH1 的每个端口的一个滤波器块而被实现，或者可以作为一个控制验证器 AUTH1 的不同端口上的业务的集中式功能块而被实现。

判定器 DEC 基于预定义的规则和条件来产生验证判定的结果 RES。

这些预定义的规则和条件包括四个控制步骤，分别由第一控制器 CONT1、第二控制器 CONT2、第三控制器 CONT3 和第四控制器 CONT4 来执行。

根据本发明，判定器 DEC 的第一控制器 CONT1 执行第一控制步骤，即在出现在先条目时控制第一注册存储器 MEM1，所述在先条目包括申请方 SUP1 的第一媒体访问控制地址 MAC1 与该申请方的用户密码 PSWD1 之间的第一关联。

例如所述媒体访问控制地址和密码的信息在验证请求中被找到，并且由判定器 DEC 从该验证请求中提取。第一控制器 CONT1 使用该信息作为第一注册存储器 MEM1 的输入。第一注册存储器 MEM1 作为输入（MAC1，PSWD1）接收。

第一注册存储器MEM1利用OK消息来或NOK消息对所述输入作出反应，该OK消息意味着对条目（pair-entry）（MAC1，PSWD1）在第一注册存储器MEM1中被找到，该NOK消息意味着所述对条目（MAC1，PSWD1）没有在该第一注册存储器MEM1中被找到。这种OK消息或NOK消息由判定器DEC来考虑以产生结果RES，将在后面的段落中说明该结果。

在下面的段落中将进一步说明第一控制步骤并且介绍第二控制步骤。

如果第一控制步骤是肯定的，则这意味着条目（MAC1，PSWD1）在第一注册存储器MEM1（图1中未示出）中被找到，判定器DEC产生包括针对端口P1和MAC1地址的验证的结果RES（AUTH），由此具有MAC1地址且具有密码PSWD1的申请方SUP1被许可经由验证器AU的端口P1来接入数据通信网络DCN。由于各个关联出现在第一注册存储器MEM1中，因此不需要产生其它条目。

需要说明的是，肯定的验证结果与申请方所耦合的端口无关。这意味着具有其终端单元TU1的用户也可以被耦合到验证器AUTH1的另一个端口，即出现在另一住宅（图1中未示出）。因此以安全的方式实现了用户游动。

如果第一控制是否定的，则这意味着条目（MAC1，PSWD1）没有在第一注册存储器MEM1（图1中未示出）中被找到，判定器DEC包括第二控制器CONT2，以在出现在先条目时执行对于第一注册存储器MEM的第二控制，所述在先条目包括在申请方SUP1的MAC地址MAC1与另一个密码之间的第二关联，即对（MAC1；除了验证请求中的密码之外的任何其它密码）。

如果第二控制是否定的，则判定器DEC产生包括针对端口P1和MAC1地址的验证的结果RES（AUTH），由此具有MAC1地址且具有密码PSWD1的申请方SUP1被许可经由验证器AU的端口P1来接入数据通信网络DCN。这还意味着媒体访问控制地址MAC1根本没有第一注册存储器MEM1中被找到，由此假设申请方SUP1是第一次请求接入。由于各个关联（MAC1；PSWD1）没有出现在第一注册存储器MEM1中，因此需要产生该关联的条目。

应当指出，第二控制器CONT2可以通过如第一控制器CONT1的另一个功能块而被实现。然而，应当说明，两个控制器都可以通过同一个功能块而被实现。根据这样的实现，由所述全局控制器所使用的参数是以不同的方式而被定义的，其取决于必须被执行的不同的控制步骤，即第一控制步骤，其具有例如（MAC1; PSWD1）作为输入，或第二控制步骤，其具有例如（MAC1; 除 PSWD1 之外的任何其它密码）作为输入。

此外，应当说明，两个控制步骤还可以通过执行一个全局控制步骤而被实现，该全局控制步骤提供更详细的反馈而不是OK消息或Not OK消息，所述反馈例如是（MAC1 OK; PSWD1 NOK），其意味着MAC1在与另一个端口相关的第一注册存储器 MEM1 中被找到。然而，不同实现方式的详细描述超出了本发明的目的。

如果第一控制是否定的并且第二控制是否定的，则验证服务器AS在第一注册存储器MEM1中插入新的条目，该条目包括申请方SUP1的MAC1地址和验证器的密码PSWD1。此外，判定器DEC产生包括针对端口 P1 和媒体访问控制地址MAC1的验证的结果RES（AUTH），由此具有MAC1地址的申请方SUP1被许可经由验证器AU的端口 P1 来接入数据通信网络DCN。

如果第一控制是否定的并且第二控制是否定的，则还利用关联注册在第二注册存储器 MEM2 中，所述关联是在第一申请方 SUP1 的第一媒体访问控制地址MAC1与验证器（AUTH）的第一端口 P1 之间的关联。应当说明，在极为特别的情况下，这样的条目（MAC1; P1）可能在第二注册存储器 MEM2 中已经存在。在提供验证之前此处应当进行关于MAC窃取的进一步检验。

如果第二控制步骤是肯定的，即在具有另一个密码的 MACI 的第一注册存储器MEM1中的实际条目，则下面的控制步骤被用于本发明的方法:

－出现在先条目时利用第三控制器 CONT3 来执行第二注册存储器 MEM2 的第三控制步骤，所述在先条目包括第一申请方SUP1的第一媒体访问控制地址MAC1与验证器的第一端口 P1 之间的第三关联; 并且

－出现在先条目时利用第四控制器 CONT4 执行控制第二注册存储器 MEM2 的第四控制步骤，所述在先条目包括第一申请方 SUP1 的第一媒体访问控制地址 MAC1 与所述验证器的另一个端口之间的第四关联。

如果第三控制步骤是肯定的，则该方法还包括产生结果的步骤，该结果包括针对具有第一密码 PSWD1 的第一媒体访问控制地址 MAC1 的验证，并且由此许可第一申请方 SUP1 通过验证器 AU 的第一端口 P1 接入数据通信网络 DCN。这意味着虽然没有关联（MAC1; PSWD1）被获知，但实际获知的关联（MAC1; 另一个 PSWD）指示了可能存在（MAC1; P1）。当该第三关联实际上在第二注册存储器 MEM2 中也被获知时，这说明具有 PSWD1 的用户 U1 位于另一个住宅，使用该另一住宅的计算机（具有含 MAC1 地址的 SUP1 的 CPE1－图 1 中未示出），并且该计算机被耦合到验证器 AUTH1 的端口 P1。由此允许了根据一种安全方式的用户游动的第二种方式。

如果第三控制步骤是否定的并且第四控制步骤是肯定的，则该方法还包括产生结果的步骤，该结果包括针对第一端口 P1 和第一媒体访问控制地址 MAC1 的拒绝，并且由此拒绝第一申请方 SUP1 通过第一端口 P1 接入数据通信网络 DCN。实际上，在第二注册存储器 MEM2 中，当不知道第一关联（MAC1; PSWD1）但知道第二关联（MAC1; 另一个 PSWD）时；并且当不知道第三关联（MAC1; P1）但知道第四关联（MAC1; 另一个 P）时，意味着 PSWD1 的用户正窃取 MAC1 地址。

这意味着通过考虑在所述过程的这个阶段的预定义的规则和条件、在判定器 DEC 的验证判定期间对于对（MAC，端口）关系（pair-relation）的可能的早期许可，并且通过仅针对为其提供验证的 MAC 地址 MAC1 来相应地设置用于请求的申请方 SUP1 的验证器 AUTH1 的端口 P1，即如果产生验证结果则允许业务，避免了针对重复的 MAC 地址的接入许可并且预先发现恶意的用户。

因此提供了一种方法，由此首先允许用户游动，并且其次阻止媒体访问控制地址的窃取。

最后应当指出，上面就功能块描述了本发明的实施例。根据上面给出的这些

块的功能描述，如何利用公知的电子元件来制造这些块的实施例，对于设计电子设备领域的技术人员而言是显而易见的。因此没有给出所述功能块的内容的详细结构。

虽然上面已经结合指定装置描述了本发明的原理，但是应当清楚地理解，该描述仅作为例子而不限制如所附的权利要求所定义的本发明的范围。

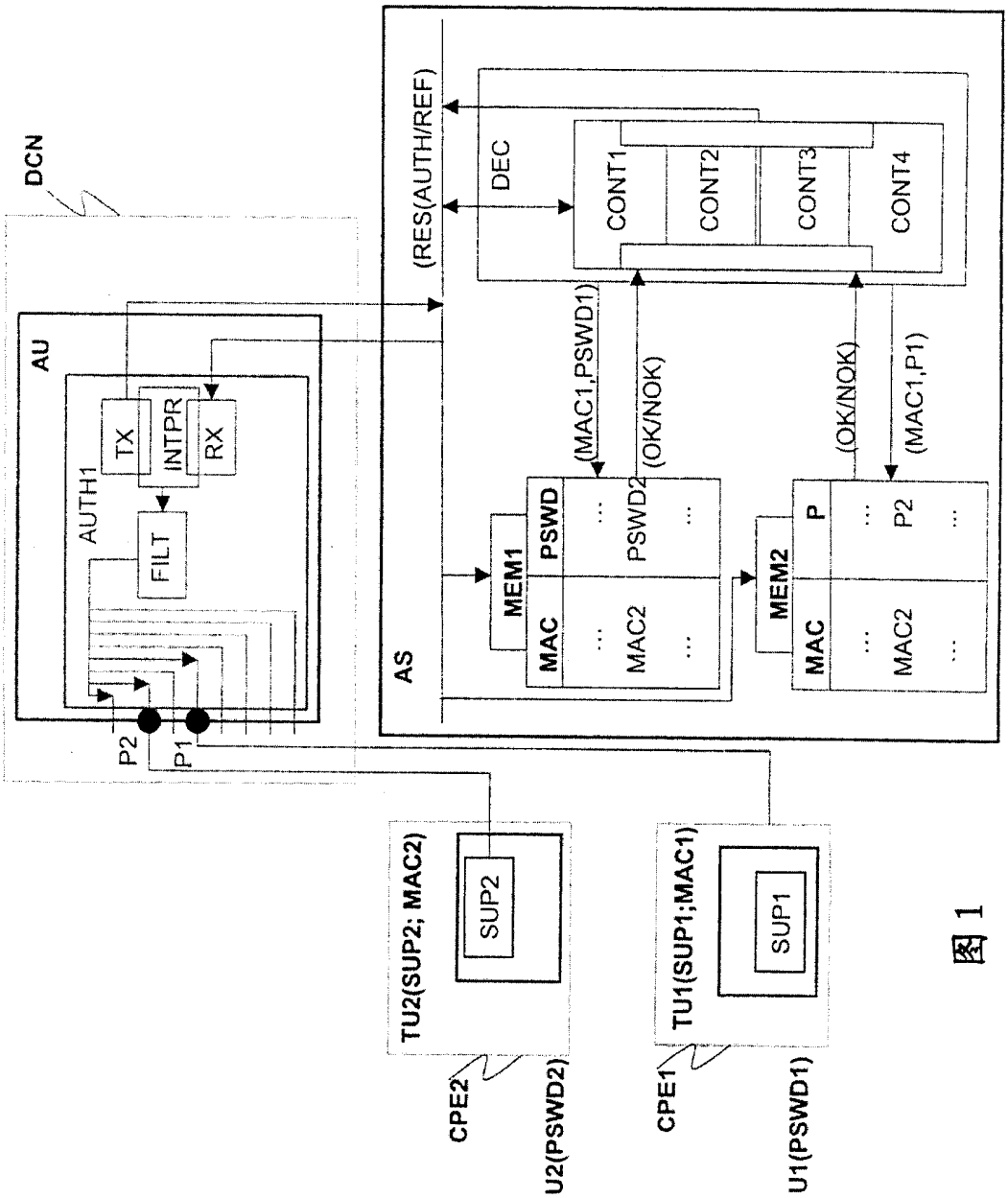

DCN
AU
AUTH1
TX
INTPR
RX
FILT
P2
P1
AS
(RES(AUTH/REF)
DEC
CONT1
CONT2
CONT3
CONT4
(MAC1,PSWD1)
(OK/NOK)
(OK/NOK)
(MAC1,P1)
MEM1
PSWD
MAC
PSWD2
MAC2
MEM2
P
P2
TU2(SUP2; MAC2)
SUP2
TU1(SUP1;MAC1)
SUP1
CPE2
U2(PSWD2)
CPE1
U1(PSWD1)

图 1