[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 200410088262.4

[43] 公开日 2005 年 4 月 27 日

[11] 公开号 CN 1610297A

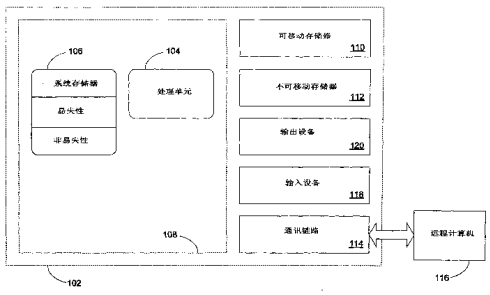
[22] 申请日 2004.10.18
[21] 申请号 200410088262.4
[30] 优先权
[32] 2003.10.17 [33] US [31] 10/688,656
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 S·O·林德塞 T·摩尔
V·巴努 W·V·巴克利 Y·姚
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 李家麟

权利要求书 8 页 说明书 17 页 附图 11 页

[54] 发明名称 网络指纹

[57] 摘要

用于计算机化系统的指纹组件发出对计算机网络的网络识别符(NID)。对关于当前计算机网络的每个发出的网络识别符确定身份置信度。计算机网络属性能包括被动网络属性和主动网络属性。检索对主动网络属性的值包括产生网络通信量。结果，被动网络属生能在主动网络属性之前对网络指纹组件可用。学习的身份置信度修改符能应用到无关于主动网络属性确定的身份置信度，以便立即得到更精确的身份置信度。通过将对无关于主动网络属性确定的特定的计算机网络的身份置信度与对主动网络属性一旦变得可用时确定的计算机网络的身份置信度相比较，获得更好的学习的身份置信度修改符，并随后调节学习的身份置信度修改符，使任何差别最小。



ISSN1008-4274

1、具有用于完成一个方法的计算机可执行指令的计算机可读介质，所述方法包括：

建立到至少一个计算机网络的至少一个连结；

对所述至少一个计算机网络的至少一个计算机网络发出一个发出的网络识别符；和

对关于至少一个当前的计算机网络的每个发出的网络识别符确定身份置信度。

2、如权利要求 1 的计算机可读介质，其特征在于所述方法还包括，用一应答响应对所述至少一个当前计算机网络的身份的请求，所述请求包括：

至少一个发出的网络识别符；和

对所述应答中的每个发出的网络识别符，对相对于所述至少一个当前计算机网络确定的所述发出的网络识别符的身份置信度。

3、如权利要求 2 的计算机可读介质，其特征在于：

每个身份置信度具有值，所述值的范围是从最小身份置信度值的最大身份置信度值；和

当所述应答中的每个身份置信度的值是所述最大身份置信度值。

4、如权利要求 2 的计算机可读介质，其特征在于：

每个身份置信度具有值；和

在所述应答中的每个身份置信度的值高于最小身份置信度响应阈值。

5、如权利要求 1 的计算机可读介质，其特征在于每个发出的网络识别符包括全球统一的识别符（GUID）。

6、如权利要求 1 的计算机可读介质，其特征在于：

每个计算机网络具有至少一个网络属性；

每个网络属性与至少一个身份置信度修改符相关联；

每个网络属性具有值；和

对关于所述至少一个当前计算机网络的每个发出的网络识别符确定所述身份置信度包括，若由发出的网络识别符识别的计算机网络的网络属性的值匹配所述当前计算机网络的网络属性的值，对每个当前的计算机网络和每个网络属性将与所述网络属性相关联的所述至少一个身份置信度修改符的至少

一个应用到每个发出的网络识别符的身份置信度。

7、如权利要求 **6** 的计算机可读介质，其特征在于：

每个身份置信度修改符规定身份置信度转换；和

将所述身份置信度修改符应用到所述身份置信度包括，按照由所述身份置信度修改符规定的所述身份置信度转换，转换所述身份置信度。

8、如权利要求 **7** 的计算机可读介质，其特征在于每个身份置信度修改符规定线性身份置信度转换。

9、如权利要求 **1** 的计算机可读介质，其特征在于，

每个计算机网络具有多个网络属性，所述多个网络属性包括：

至少一个被动的网络属性；和

至少一个主动的网络属性；

每个被动的网络属性与至少一个被动的网络属性身份置信度修改符关联；

每个主动的网络属性与至少一个主动的网络属性身份置信度修改符关联；

每个网络属性具有值；

检索每个主动网络属性的所述值包括在具有主动网络属性的计算机网络上生成网络通信量；和

对每个关于所述至少一个当前计算机网络的发出的网络识别符确定身份置信度包括：

若由所述发出的网络识别符识别的计算机网络的被动网络属性的值匹配所述当前计算机网络的被动网络属性的值，则对每个当前计算机网络和每个被动网络属性，将与所述被动网络属性关联的所述至少一个被动网络属性身份置信度修改符的至少一个应用到每个发出的网络识别符的所述身份置信度；和

若由所述发出的网络识别符识别的计算机网络的主动网络属性的值匹配所述当前计算机网络的主动网络属性的值，则对每个当前计算机网络和每个主动网络属性，将与所述主动网络属性关联的所述至少一个主动网络属性身份置信度修改符的至少一个应用到每个发出的网络识别符的所述身份置信度。

10、如权利要求 **1** 的计算机可读介质，其特征在于：

每个计算机网络具有至少一个被动网络属性；

每个被动网络属性与至少一个被动网络属性身份置信度修改符关联；

每个发出的网络识别符与学习的身份置信度修改度关联；

每个网络属性具有值；

检索每个被动网络属性的值与在具有所述被动网络属性的计算机网络上产生网络通信量无关；和

对每个关于所述至少一个当前计算机网络的发出的网络识别符确定身份置信度包括：

若由所述发出的网络识别符识别的计算机网络的被动网络属性的值匹配所述当前计算机网络的被动网络属性的值，则对每个当前计算机网和每个被动网络属性，将与所述被动网络属性关联的所述至少一个被动属性身份置信度修改符的至少一个应用到每个发出的网络识别符的所述身份置信度；和

若所述发出的网络识别符的身份置信度高于最小学习的修改身份置信度阈值，则对每个当前计算机网络将与所述发出的网络识别符关联的学习的身份置信度修改符应用到每个发出的网络识别符的所述身份置信度。

11、如权利要求 **10** 的计算机可读介质，其特征在于：

第一组身份置信度包括对关于所述至少一个当前计算机网络的每个发出的网络识别符确定的身份置信度；

每个计算机网络具有多个网络属性，所述多个网络属性包括：

至少一个被动的网络属性；和

至少一个主动的网络属性；

每个主动网络属性与至少一个主动网络属性身份置信度修改符关联；

检索每个主动网络属性的值包括在具有所述主动网络属性的计算机网络上产生网络通信量；和

所述方法还包括：

作为至少一个主动网络属性成为可用的结果，确定第二组身份置信度，使得确定第二组身份置信度包括：

应用至少一个主动网络属性身份置信度修改符到第二组身份置信度；和

调节与每个发出的网络识别符关联的学习的身份置信度修改符，使得若第一组身份置信度被重新确定，则在重新确定的第一组身份置信度和所述第二组身份置信度之间的差应是最小化。

12、具有用于完成一个方法的计算机可执行指令的计算机可读介质，所述方法包括：

确定第一组身份置信度，使得确定所述第一组身份置信度包括将一组学习的身份置信度修改符的至少一个应用到所述第一组身份置信度的至少一个；

确定第二组身份置信度，使得确定所述第二组身份置信度包括将一组主动网络属性身份置信度修改符的至少一个应用到所述第二组身份置信度的至少一个；和

调节所述的学习的身份置信度修改符的组，使得若所述第一组身份置信度拟被重新确定，则在重新确定的第一组身份置信度和所述第二组身份置信度之间的差最小化。

13、如权利要求 12 的计算机可读介质，其特征在于：

在学习的身份置信度修改组中的每个学习的身份置信度修改符与发出的网络识别符的组中的一个关联；

在所述第一组身份置信度中每个身份置信度与发出的网络识别符的组中的一个关联；和

将学习的身份置信度修改符的组的至少一个应用到所述第一组身份置信度包括，对发出的网络识别符的组中每个发出的网络识别符，若与所述发出的网络识别符关联的所述身份置信度高于最小学习的修改身份置信度阈值，则将与所述发出的网络识别符关联的所述学习的身份置信度修改符应用到与所述发出的网络识别符关联的所述身份置信度。

14、如权利要求 12 的计算机可读介质，其特征在于：

在所述第二组身份置信度中的每个身份置信度与发出的网络识别符的一组中的一个关联；

在发出的网络识别符的组中的每个发出的网络识别符与发出的主动网络属性的至少一个关联；

与主动网络属性身份置信度修改符的组中每个主动网络属性身份置信度修改符与当前主动网络属性的一组中至少一个关联；

每个主动网络属性具有值；和

将主动网络属性身份置信度修改符的组的至少一个应用到所述第二组身份置信度包括，对发出的网络识别符的组中的每个发出的网络识别符以及当

前主动网络属性的组中的每个主动网络属性，若在当前主动网络属性的组中的主动网络属性的值匹配在与所述发出的网络识别符关联的发出的主动网络属性的组中的主动网络属性的值，则将与所述主动网络属性关联的所述主动网属性身份置信度修改符应用与所述发出的网络识别符关联的身份置信度。

15、如权利要求 12 的计算机可读介质，其特征在于：

每个身份置信度修改符规定身份置信度转换，和

将所述身份置信度修改符应用到所述身份置信度包括按由所述身份置信度修改符规定的身份置信度转换，转换所述身份置信度。

16、如权利要求 15 的计算机可读介质，其特征在于每个身份置信度修改符规定线性身份置信度转换。

17、如权利要求 12 的计算机可读介质，其特征在于：

每个身份置信度与一组发出的网络识别符的一个关联；

每个学习的身份置信度与发出的网络识别符的所述组的一个关联；

每个身份置信度具有值；且

调节学习的身份置信度修改符的所述组包括，对在发出的网络识别符的所述组中每个发出的网络识别符，若与在第一组身份置信度中的所述发出的网络该识别符关联的身份置信度的值大于匹配容量，而容量小于与所述第二组身份置信度中的所述发出的网络识别符关联的所述身份置信度的值，由增大与所述发出的网络识别符关联的所述学习的身份置信度修改符。

18、如权利要求 17 的计算机可读介质，其特征在于调节学习的身份置信度修改符的所述组还包括，对在发出的网络识别符的所述组中每个发出的网络识别符，若与在第一组身份信度的中的所述发出的网络识别符关联的身份置信度的值大匹配容差，而该容差大于所述第二组身份置信度中的所述发出的网络识别符关联的所述身份置信度的值，则减少与所述发出的网络识别符关联的所述学习的身份置信度修改值。

19、如权利要求 17 的计算机可读介质，其特征在于增大所述学习的身份置信度修改符包括转换所述学习的身份置信度修改符，使得应用所述经转换的学习的身份置信度修改符到一身份置信度导致比将未转换的所述学习的身份置信度修改符应用到所述身份置信度具有更高的身份置信度值。

20、如权利要求 17 的计算机可读介质，其特征在于：

每个学习的身份置信度修改符通过将学习的变量添加到侯选的身份置信

度的值来修改侯选的身份置信度；和

增大所述学习的身份置信度修改符包括将增大常数加到所述学习的变量。

21、一个计算机化的系统，其特征在于，包括一网络指纹组件，它配置成至少包括：

对至少一个计算机网络发出至少一个网络识别符；

保持一组发出的网络识别符；和

保持一组当前的身份置信度，所述当前的身份置信度组包括对于关系到至少一个当前的计算机网络的每个发出的网络识别符的身份置信度。

22、如权利要求 **21** 的计算机化系统，其特征在于所述网络指纹组件还配置成至少：

保持一组发出的网络属性，所述发出的网络属性的组对所述发出的网络识别符的组中的每个发出的网络识别符包括至少一个由所述发出的网络识别符的计算机网络的网络属性；和

保持一组当前的网络属性，所述的当前网络属性的组至少包括每个当前计算机网络的一个网络属性。

23、如权利要求 **22** 的计算机化系统，其特征在于所述网络指纹组件还配置成至少：

保持一组身份置信度修改符，所述的身份置信度修改符组，对在所述的当前网络属性的组内的每个网络属性包括至少一个身份置信度修改符；和

应用至少一个身份置信度修改符到至少一个身份置信度。

24、如权利要求 **21** 的计算机化系统，其特征在于：

每个计算机网络具有多个网络属性，所述多个网络属性包括：

至少一个被动网络属性；和

至少一个主动网络属性；

每个网络属性具有值；

检索每个主动网络属性的值包括在具有所述主动网络属性的计算机网络生成网络通信量；和

所述网络指纹组件还配置成至少：

保持一组发出的被动网络属性，所述发出的被动网络属性的组对在发出的网络识别符的组中的每个发出的网络识别符包括由发出的网络识别符识别

的计算机网络的至少一个被动网络属性；

保持一组发出的主动网络属性，所述发出的主动网络属性的组对在发出的被动网络属性的组对在发出的网络识别符的组中的每个发出的网络识别符包括由发出的网络识别符识别的计算机网络的至少一个被动网络属性；

保持一组发出的主动网络属性，所述发出的主动网络属性的组对在发出的网络识别符的组中的每个发出的网络识别符包括由发出的网络识别符的计算机网络的至少一个主动网络属性；

保持一组当前被动网络属性，所述当前被动网络属性的组饭知每个当前计算机网络的至少一个被动网络属性；和

保持一组当前主动网络属性，所述当前主动网络属性的组包括每个当前计算机网络的至少一个主动网络属性。

25、如权利要求 **24** 的计算机化系统，其特征在于所述网络指纹组件还配置成至少：

保持一组被动网络属性身份置信度修改符，所述被动网络属性身份置信度修改符组对在当前被动网络属性组的每个被动网络属性包括至少一个被动网络属性身份置信度修改符；

保持一组主动网络属性身份置信度修改符，所述主动网络属性身份置信度修改符组对在当前主动网络属性组的每个主动网络属性包括至少一个主动网络属性身份置信度修改符；

应用至少一个被动网络属性身份置信度修改符到至少一个身份置信度；和

应用至少一个主动网络属性身份置信度修改符所述的至少一个身份置信度。

26、如权利要求 **25** 的计算机化系统，其特征在于所述网络指纹组件还配置成至少：

保持一组学习的身份置信度修改符，所述学习的身份置主度修改符的组对每个在发出的网络识别符的所述组中的每个发出的网络识别符包括至少一个学习的身份置信度修改符；和

应用至少一个学习的身份置信度修改符到至少一个身份置信度。

27、如权利要求 **26** 的计算机化系统，其特征在于所述网络指纹组件还配置成：至少调节学习的身份置信度修改符的所述组，使得在第一组当前身

份置信度和第二组当前身份置信度之间的差最小，所述第一组当前身份置信度在对所述至少一个当前计算机网络检索主动网络属性之前确定，而所述第二组当前身份置信度在对所述至少一个当前计算机网检索主动网络属性之后确定。

28、如权利要求 **25** 的计算机化系统，其特征在于所述网络指纹组件还配成至少：

对在发出的网络识别符的所述组中每个发出的网络识别符以及对在当前的被动网络属性的所述组的每个被动网络属性，若在当前被动网络属性的所述组中所述被动网络属性的值匹配对在发出的主动网络属性的所述组中的所述发出的主动网络属性的值，则将对所述主动网络属性的所述至少一个主动网络属性身份置信度修改符的至少一个，应用到对所述发出的网络识别符的所述身份置信度；及

对在发出的网络识别符的所述组中每个发出的网络识别符以及对在当前的主动网络属性的所述组的每个主动网络属性，若在当前主动网络属性的所述组中所述主动网络属性的值匹配对在发出的主动网络属性的所述组中的所述发出的主动网络属性的值，则将对所述主动网络属性的所述至少一个主动网络属性身份置信度修改符的至少一个，应用到对所述发出的网络识别符的所述身份置信度。

29、如权利要求 **25** 的计算机化系统，其特征在于：

每个身份置信度修改符规定身份置信度的一个转换；和

将所述身份置信度修改符应用到所述身份置信度包括按照由身份置信度修改符规定的转换来转换所述身份置信度。

30、如权利要求 **29** 的计算机化系统，其特征在于每个身份置信度修改符规定所述身份置信度的一个线性转换。

31、如权利要求 **21** 的计算机化系统，其特征在于每个网络识别符是全球统一识别符（**GUID**）。

网络指纹

技术领域

本发明一般涉及计算机网络，具体涉及计算机网络的身份。

背景技术

现代计算机经过各种计算机网络互相通讯。移动计算机一天内可使用若干计算机网络。甚至固定位置的计算机可访问多个计算机网络，例如为了通过冗余达到更高的可靠性，得益于计算机网络之间的花费差别，或为了改变通讯安全性要求。

计算机，计算机操作系统，和/或通讯应用程序能根据它连接的一个或多个网各需要改变其配置。区分计算机网络的某些传统方法是特定的，或限于特定的网络类型。在现代异种网络环境中，这能导致配置的不一致性，并最终导致计算机系统用户的混淆及失败。

某些传统的区分计算机网络的方法提供不明确的结果，没有提供有关不明确的级别的信息。那样的方法尤其对安全性关切的应用是不合适的。此外，例如为了安全的原因，对网络服务的访问可以被拒绝，直到不明确的级别足够低。结果，希望网络的去除不明确性是快速有效的。

发明内容

这部分进行本发明某些实施例的简要概述。此概述不是本发明广泛的综述。不试图确定本发明的关键/重要元素，或勾划出本发明的范围。其唯一目的是以简化方式给出本发明的某些实施例，作为后面给出的更详细描述的序言。

在本发明的一个实施例中，建立到一个或多个计算机网络的一个或多个连接。对每个计算机网络能产生一网络识别符。对关于一个或多个当前计算网络的每个发出的网络识别符能确定一身份置信度。

在本发明的一个实施例中，确定第一组和第二组身份置信度。确定第一组身份置信度包括将一组学习的身份置信度修改符的一个或多个应用到第一

组的身份置信度的一个或多个。确定第二组身份置信度包括将一组活动的网络属性身份置信度的一个或多个。该组学习的身份置信度修改符可以被调节，使得若第一组身份置信度被重新确定，使得在重新确定的第一组身份置信度和第二组身份置信度之间的差将为最小。

在本发明的一个实施例中，计算机化的系统包括网络指纹组件。该网络指纹组件能配置成对一个或多个计算机网络发出一个或多个网络识别符。网络指纹组件能配置成保持一组发出的网络识别符。该网络指纹组件还能配置成保持一组当前的身份置信度。该组当前的身份置信度可包括对关于一个或多个当前的计算机网络的每个发出的网络识别符的身份置信度。

附图说明

虽然附后的权利要求详细列出本发明的特征，本发明及其优点从结合附图的后面详述中得到最好的理解附图是：

图 1 是示出可用来实现本发明的实施例的示例计算机系统的示意图；

图 2 是示出由计算机网络以各种方式连结的计算机的示意图；

图 3 是示出按本发明的实施例的示例意层系统架构的示意图；

图 4 是示出按本发明的实施例的示例网络指纹组件结构的示意图；

图 5 是示出按本发明的实施例响应对网络识别符的请求的的示例步骤的流程图；

图 6 是示出按本发明的实施例用于确定对一计算机网络的当前身份置信度的示例步骤的流程图；

图 7 是示出按本发明的实施例用于将被动的网络属性身份置信度修改符应用到当前的身份置信度的示例步骤的流程图；

图 8 是示出按本发明的实施例用于学习的身份置信度修改符应用到当前的身份置信度的示例步骤的流程图；

图 9 是示出按本发明的实施例用于将有效的网络属性身份置信度修改符应用到当前的身份置信度的示例步骤的流程图；

图 10 是示出按本发明的实施例用于将学习的身份置信度修饰词更新成新的可用的有效的网络属性的结果的示例步骤的流程图；和

图 11 是更详细地示出图 10 的诸方面的流程图。

具体实施方式

在进行本发明的各个实施例的描述之前，提供可以实现本发明的各实施例的计算机的描述。虽然不是必须，本发明将在诸如由计算机执行的程序模块那样的计算机可执行指令的一般情况中描述。通常，程序包括例行程序，对象，组件，数据结构等，它们完成特定任务或实行特定的抽象数据类型。这里用的术语“程序”可以不是单个程序模块或协同工作的多个程序模块。这里使用的术语“计算机”或“计算设备”包括用电子方法执行一个或多个程序的任何设备，如个人计算机（PC），手持设备，多处理器系统，基于微处理器的可编程消费者电子设备，网络 PC，小型机、输入板 PC、膝上计算机，具有微处理器或微控制器的消费者电器设备，路由器，网关，集线器等。本发明也能在分布式计算环境中使用，在那里任务由通过通讯网络连接的远程处理设备执行。在分布式计算环境中，程序可位于本地或远程的存储器存储设备中。

参考图 1，示出其中可实施这里描述的本发明的诸方面的计算机 102 的基本配置的例。在此最基本的配置中，计算机 102 通常至少包括一个处理单元 104 和存储器 106。处理单元 104 按本发明的各实施例执行指令来执行任务。在执行那样任务中，处理单元 104 能发送电子信号到计算机 102 的其他部分和计算机 102 之外的设备来引起某个结果。根据计算机 102 的精确配置及类型，存储器能量易失性（如 RAM），非易失性（如 ROM 或闪存）或两者的某种组合。此最基本的配置在图 2 中用虚线 108 示出。

计算机 102 也能具有另外的特征/功能。例如，计算机 102 也能包括另外的存储器（可移除的和/或不可移除的），包括，但不限于，磁盘或光盘，或磁带。计算机存储介质包括以任何方法或技术实现的易失的和非易失的，可移除的和不可移除的介质，用于存储包括计算机可执行指令，数据结构，程序模块，或其他数据那样的信息。计算机存储介质包括，但不限于，RAM，ROM，E EPROM，闪存，CD-ROM，数字多功能盘（DVD）或其他光存储器，盒式磁带，磁带，磁盘存储器或其他磁存储设备，或任何能用于存储所希望的信息并能由计算机 102 访问其他介质。任何那样的计算机存储介质能是计算机 102 的一部分。

计算机 102 最好还包含通讯连结 114，它允许该设备与诸如远程计算机 116 那样的其他设备通讯。通讯连接是通讯媒体的例子。通讯媒体通常体现在以

诸如载波或其他传输机制那样的调制数据信号中的计算机可读指令，数据结构，程序模块和其他程序数据中，并包括任何信息提交媒体。作为例子但不作限止，术语“通讯媒体”包括诸如声音，RF，红外和其他无线媒体的无线媒体这里使用的术语“计算机可读介质”包括计算机存储介质和通讯媒体。

计算机 102 也能具有诸如键盘/键板，鼠标，笔，声音输入设备，接触输入设备等那样的输入设备 118。也能包括诸如显示器，扬声器，打印机等的输出设备 120。所有这些设备在本专业内是熟知的，不必在此阐述。

除非另外说明，在下面描述中，本发明将参照由一个或多个计算设备完成的动作或操作的符号表示来描述。因此可以理解，有时称为计算机可执行的那些动作和操作包括由计算机的处理单元对以结构形表示数据的电信号的处理。此处理转换了数据，或将其保持在计算机存储系统的位置中，此数据以本专业熟知的方式重新配置或更换计算机的操作。保持数据的数据结构是存储器的物理位置，它具有由数据的格式定义的特定属性。然而，虽然本发明以上述情况描述，这不意味着加以限止，如本专业人士理解，后面描述的各种动作和操作也能在硬件中实现。

参考图 2 描述适合于加入本发明的诸方面的计算机网络环境的例子。示例计算机网络环境 200 包括通过每个以云表示的若干计算机网络 220，222，224，226，228 互相通讯的若干计算机 202，204，206，208，210，212，214，216，218（例如每个能是上面参考图 1 描述的计算机 102）。每个计算机网络 220，222，224，226，228 能包括众知的组件，如路由器，网关，集线器等，并能允许计算机 202，204，206，208，210，212，214，216，218 通过有线和/或无线媒体通讯。当通过计算机网络 220，222，224，226，228 互相交互时，一个或多个计算机 202，204，206，208，210，212，214，216，218 相对于另外的计算机 202，204，206，208，210，212，214，216，218 能扮演客户机，服务器或对等设备的角色。因而，本发明的各实施例能在客户机，服务器，对等设备或其组合上实现，即使这里包含的具体例子不专指所有这些类型的计算机。

计算机 202 连结到计算机网络 220。认证（Auth）服务器 204 也连结到计算机网络 220，认证服务器在本专业是众知的，所以这里只强调它们的某些特征。认证服务器 24 是一类计算机（通常具有在该计算机上执行的认证服务应用程序或操作系统组件），它提供认证服务，如向成功地认证或本地保持来

源可靠的认证状态的计算机发出认证权标。例如安全策略那样的计算机网络策略可要求，计算机在被授予对诸如文件，数据库，目录，打印机等的网络服务和资源的进一步访问之前应成功地认证。配置成域控制器的微软的 Windows®XP 服务器是认证服务器之一例。

计算机网络 220 通过防火墙 206 连接到网络 222。防火墙是本专业众知的，所以这里只强调它们的某些特征。防火墙 206 是一类计算机（通常具有在计算机上执行的防火墙应用程序或操作系统组件），它对于到达该防火墙的计算机网络通信量强制实行计算机网络通信量策略，如安全策略。例如，防火墙 260 能允许某些类型的计算机网络通讯量从计算机网络 222 通过到计算机网络 220，但阻断其他类型的通讯量。

计算机 208 连结到计算机网络 224。认证服务器 210 也连结到计算机网络 224。计算机网络 224 连结到计算机网络 222。计算机 212 连结到计算机网络 226。计算机网络 226 连结到计算机网络 222。表示计算机网络 222 的云比表示计算机网络 220，224，226，228 的云大，表明计算机网络 222 是其他计算机网络经过它通讯的计算机网络（即中间网），例如，计算机网络 224 和计算机网络 226 通过计算机网络 222 通讯。计算机 214 连接到计算机网络 222。计算机 216 和计算机 218 连接到计算机网络 228。计算机网络 228 不连接到图 2 的其他计算机网络 220，222，224，226。

图 3 示出适合于加入本发明的诸方面的示例高层系统结构。应用程序 302 得益于通过网络应用程序编程界面（API）306 的网络服务 304。网络 API306 包括一网络位置认知（network location awareness-NLA）组件 308。NLA 组件 308 包括一网络指纹组件 310。

网络服务 304 包括诸如建立和维持通讯连接 114（图 1）的基本计算机网络服务。网络服务 304 包括由低层通讯设备和协议提供的服务，例如按电气电子工程师协会（IEEE）802.1x 系列通讯标准，因特网协议（IP），传输控制协议（ICP）的设备和协议。网络服务 304 还能包括计算机网络底层结构服务，例如由动态主机配置协议（DHCP），因特网域名系统（DNS）等提供的服务。网络服务 304 也能包括较高层通讯服务，如由分布式组件对象模型（DCOM）等提供的那些。这些网络服务例子的每一个在本专业中是众知的，不需在此详述。对于示例的分布式组件对象模型的细节见微软的 Developer Network (MSDN®)库的 DCOM 段。

网络应用程序编程界面在本专业是众知的。Windows Socket2（Winsock）是合适的网络 API306 的例子，其细节在 MSDN 库中 2003 年 2 月的微软的 Windows® Platform Software Devolopment Kit (SDK)文档的 Windows Sovkets 2 段中。网络 API306 的网络位置认知组件 308 检索并监控计算机网络的属性。应用程序 302 能通过网络 API306 和带有网络位置认知组件 308 的寄存器访问计算机网络的属性，以便通知对计算机网络属性的改变。网络位置认知是本专业熟知的，所以这里只强调其某些特征。对于示例的网络位置认知组件的细节，见 MSDN 库中 2003 年 2 月的微软的 Windows®Platform SDK 文档的 Network Location Awareness Service Provider 段。

能由 NLA 组件 308 检索及监控的计算机网络属性的例子包括低层通讯设备操作参数，如按无线通讯标准的 IEEE802.11 序列的无线接入点的媒体访问控制（MAC）地址。如 IP 地址和 IP 子网规格那样的通讯协议操作参数也能由 NLA 组件 308 检索和监控。另外以计算机网络属性能包括底层结构服务配置和操作参数，操作参数如默认网关、DHCP 服务器、认证服务器、DNS 和其他名字服务器的网络地址；以及认证域名；服务器名；如全球统一识别符（GUID）那样的唯一的服务器识别符；和如由全球定位系统确定的服务器和/或网络单元的物理位置。NLA 组件 308 能检索和监控任何合适的网络服务配置或操作参数。

NLA 组件 308 能直接从网络服务 304 检索参数，或通过网络 API306 检索参数。如网络服务 304 配置和操作参数等计算机网络属性可分类为被动（Passive）和主动（active）的。在本发明的一实施例中，当检索主动的网络属性（ANA）时，由 NLA 组件 308 产生如一对请求和响应消息的计算机网络通信量，但在检索被动网络属性（PNA）时不产生计算机网络通信量。连结状态，IP 地址，IP 子网和默认的网关网络地址的通信媒体每个均是被动网络属性之例。在本发明的一实施例中，被动网络属性是在建立主动通讯连结之前存在的计算机网络属性。主动网络属性的例子包括认证状态（如来自可靠来源的远程认证服务器）和在存在远程网络服务时由远程网络服务提供者保持的其他网络服务属性。检索和/或检测主动网络属性改变比被动网络属性占用更多 NLA 组件时间。

不同的计算机网络能具有某些相同的计算机网络属性。例如图 2 的计算机网络 220 和计算机网络 228 能使用相同的专用 IP 子网（如 192、168、1、0/24）。

特定计算机网络的计算机网络属性能随时间改变。例如，在计算机网络 226 中的无线接入点的数目（图 2）能随时间改变。计算机网络的这些特征是为什么对明确地确定特定计算机网络的身份是一个挑战的部分理由。

网络指纹组件 310 确定对被网络位置认知组件 308 认知的每个计算机网络的计算机网络识别符（NID），如 GUID。在本发明的一实施例中，网络指纹组件 310 还相对于各种计算机网络确定对每个网络识别符的置信度级（“身份置信度”）。特定网络识别符的身份置信度能是正确识别被网络位置认知组件 308 认知的一个计算机网络的概率。例如，身份置信度能具有最小身份置信度值（如 0%）和最大身份置信度值（如 100%）之间的值。身份置信度能具有数量化标度上的值，如标度 0（无置信度）到 5（最高置信度）。

特定网络识别符的身份置信度能根据当前的和以前的网络属性组的比较。网络指纹组件 310 能具有对由网络位置认知组件 308 检索的每个网络属性的访问。网络指纹组件 310 可预订对由网络位置认知组件 308 监控的网络属性的改变。某些计算机网络可能不拥有可作为确定身份置信度的部分使用的特定的计算机网络属性，例如，某些计算机网络可以不包括认证服务器。对那些计算机网络可能不可用一个或多个最高级的身份置信度。

响应对被网络位置认知组件 308 认知的一个计算机网络的身份的请求，例如由一个应用程序 302 产生的请求，网络指纹组件 310 可以用网络识别符和每个网络识别符的身份置信度的响应组作为回答。例如，网络识别符的响应组按网络识别符的身份置信度的降序分类。在本发明的一实施例中，加入网络指纹组件 310 的计算机能交换关于被识别的网络（如网络识别符）与它们的邻网的信息，使能作共享的网络映射。

图 4 示出按本发明的一实施例的示例网络指纹组件 310 的结构。由网络指纹组件 310 保持的数据结构包括一组发出的网络识别符 402，一组发出的被动网络属性 404，和一组发出的主动网络属性 406。每个发出的网络识别符能与一组被动网络属性关联，关还能与一组主动网络属性关联。发出的被动网络属性组 404 能包含与发出的网络识别符 402 关联的被动网络属性组。发出的主动网络属性组 406 能包含与发出的网络识别符 402 关联的主动网络属性组。

由网络指纹组件 310 保持的数据结构还包括一组当前的被动网络属性（PNA）408 和一组当前的主动网络属性（ANA）410。在特例中，与加入网

络指纹组件 310 的计算机连接的每个计算机网络具有被动网络属性的特别组和主动网络属性的特别组。在该特例中，对网络指纹组件 310 可用的那些被动网络属性（即在此例中从图 3 的网络位置认知组件 308 可用）可由当前的被动网络属性的组 408 所包含。在该特例中对网络指纹组件 310 可用的主动网络属性可由主动网络属性的组 410 所包含。

由网络指纹组件 310 保持的数据结构还包括一组当前的身份置信度（CIC）412，一组被动的网络属性（PNA）身份置信度修改符（ICM）414，一组主动的网络属性（ANA）身份置信度修改符（ICM）416，和一组学习的身份置信度修改符（LICM）418。在本发明的一实施例中，通过应用身份置信度修改符到基本置信度（如 0%）对每个发出的网络识别符确定当前的身份置信度。在当前的被动的网络属性 408 匹配对应的发出的被动网络属性 404 时，能将被动的网络属性身份置信度修改符 414 应用到当前的身份置信度 412。在当前的主动的网络属性 410 匹配对应的发出的主动网络属性 406 时，能将主动的网络属性身份置信度修改符 416 应用到当前的身份置信度 412。学习的身份置信度修改符 418 能应用到当前的身份置信度 412，来修改不依赖于当前主动的网络属性 410 确定的当前的身份置信度 412。除非在下面另外表明或明显与上下文矛盾，若属性值之间的差在匹配容差由，计算机网络和其他属性可以匹配。

由网络指纹组件 310 保持的数据结构还包括一组被动网络属性（PNA）已改变的指示符 420，和一组主动网络属性（ANA）已改变的指示符 422。被动网络属性已改变的指示符 420 能包括表示当前的被动网络属性 408 何时最后一次更新的一个或多个时间标记；表示对应的当前被动网络属性 408 自从当前身份置信度 412 被最后一次确定后已经改变的一个或多个布乐值；或帮助重复确定身份置信度的任何合适的属性改变指示符。主动的网络属性已改变的指示符 422 组能包括类似的改变指示符。

在被动的网络属性列中示出被动的网络属性身份置信度修改符 414，当前从动网络属性 408，被动网络属性已改变的指示符 420，和发出的被动网络属性 404 数据结构。在被动网络属性列中的每个数据结构能具有对每个被动网络属性的对应条目。在主动网络属性列中示出主动网络属性身份置信度修改符 416，当前主动网络属性 410，主动网络属性已改变的指示符 422，和发出的主动网络属性 406 数据结构。主动网络属性列中的每个数据结构对每个主

动网络属性能具有对应的条目。在发出的网络识别符行中示出发出的网络识别符 402，当前身份置信度 412，发出的被动网络属性 404，学习的身份置信度修改符 418 和发出的主动网络属性 406。在发出的网络识别符行中对每个发出的网络识别符能具有对应的条目。本专业人士明白，图 4 中示出的数据结构能保持在如关系数据库的一个或多个表中。

在本发明的一实施例中，对网络识别符的关键使用是作为对网络有关的配置和/或策略，如安全策略的索引。那样的配置和策略能早期在加入网络指纹组件的计算机初始化时，如在任何网络接口硬件和/或通讯连结 114（图 1）使能前被参照。网络指纹组件 310 作为初始化的一部分能频繁地接收对网络识别符的请求，如 2 分钟内 100 次请求。此计算机初始化过程对网络指纹组件 310 不必须是最重要的操作过程，但它确实帮助提供了关于将网络识别符与计算机网络相关联的方法的下面讨论的环境。

图 5 示出按本发明的实施例响应对网络识别符的请求能执行的示例步骤。图 5 中示出的步骤能对网络位置认知组件 308 当前认知的每个计算机网络（每个“当前计算机网络”）执行。一个或多个网络识别符能被添加到对带有由网络位置认知组件 308 认知的至少一个网络属性的每个计算机网络的响应组（返回的）。

网络指纹组件 310 通常不能预订被网络位置认知组件 308 认知的每一个网络属性。例如，网络指纹组件 310 能预订三个被动的网络属性，如网络接口硬件 MAC 地址，IP 子网和认证域名，以及两个主动网络属性，如远程认证服务器的存在和远程认证服务器的认证状态。当网络位置认知组件 310 开始变得认知或检索到网络指纹组件 310 感兴趣的网络属性时，该网络位置认知组件 308 能将新的或更新的传送到网络指纹组件 310。

网络指纹组件 310 能添加新的或经更新的被动网络属性到当前的被动网络属性 408（图 4），并更新对应的被动网络属性已改变的指示符 420。网络指纹组件 310 能添加新的或经更新的主动网络属性到当前的主动网络属性 410，并更新对应的主动网络属性已改变的指示符 422。在当前的主动网络属性 410 成为可用之前，当前的被动网络属性 408 能成为可用。结果在步骤 502，网络指纹组件 310 判断，对该计算机网络当前主动网络属性 410 是否变得可用，或是否它们当未确定（即，空）。若对该计算机网络的当前主动网络属性 410 已成为可用（即它们非空），则过程进到步骤 504。否则过程进到步骤

506。

在步骤504，例如通过检验主动网络属性已改变的指示符422判断，自从当前身份置信度412被最近一次计算以来当前主动网络属性410（图4）是否已改变。若当前主动网络属性410已改变，则过程进到步骤508，在那里确定当前的身份置信度412。否则跳过步骤508，过程进到步骤510。

在步骤506，例如通过检验被动网络属性已改变的指示符420判断，自从当前身份置信度412被最近一次计算以来，当前被动网络属性408（图4）是否已改变。若当前被动网络属性408已改变，则过程进到步骤508。否则跳过步骤508，过程进到步骤510。

在步骤508，确定对计算机网络的当前身份置信度412（图4）。确定当前身份置信度412的示例步骤在下面参考图6作更详细的描述。在步骤510判定，是否对该计算机网络的任何当前身份置信度412具有最大的身份置信度值（如100%）。若对该计算机网络的一个或多个当前身份置信度412具有最大值，则过程进到步骤512。否则过程进到步骤514。在步骤512，那些带有最大值的当前身份置信度412的发出的网络识别符402被添加到响应组（被返回给请求者）。

在步骤514判定，是否对该计算机网络的任何当前身份置信度412（图4）具有高于最小身份置信度响应阈值（如50%）。若对该计算机网络的一个或多个当前身份置信度412确定具有高于最小身份置信度响应阈值的值；则过程进到步骤516。否则过程进到步骤518。在步骤516，那些带着高于最小身份置信度响应阈值的发出的网络识别符402被添加到响应组（返回给请求者）。

在步骤518，发出新的网络识别符。例如，网络指纹组件能产生新的网络识别符，并将新的网络识别符添加到发出的网识别符402（图4）。与新的网络识别符关联的发出的被动网络属性404和发出的主动网络属性406可以是在确定对该计算机网络的当前身份置信度412中使用的当前被动的网络属性408和当前主动的网络属性410的值。与该新的网络识别符关联的当前身份置信度和学习的身份置信度修改符的值可以是它们对应的默认值。在步骤520，新的网络识别符被添加到响应组（即被返回给请求者）。对新的网络识别符返回的身份置信度能是非正常返回的特殊值，如0%，表明它是新的网络识别符（即以前未知的计算机网络），且不是以前发出的网络识别符的那一个（即以前识别的计算机网络之一）。

图 6 示出按本发明的一实施例确定对特定计算机网络的当前身份置信度值的示例步骤。在步骤 602，与发出的网络识别符 402（图 4）关联的每个当前身份置信度被复位到初始身份置信度值，如 0%。在步骤 604，将被动的网络属性身份置信度修改符 414 被应用到与匹配当前的被动网络属性 408 的发出的被动网络属性 404 相关联的每个当前身份置信度上。按本发明的一实施例，应用被动的网络属性身份置信度修改符的示例过程在下面参考图 7 予以描述。

应用了被动的网络属性身份置信度修改符 414（图 4）之后，过程进到步骤 606。在步骤 606 判断，对该计算机网络的当前主动网络属性 410 是否已变成可用，或它们仍然未确定（即空）。若当前主动的网络属性 410 尚未变得可用，过程进到步骤 608。否则过程进到步骤 610。

在步骤 608，学习的身份置信度修改符 418（图 4）被应用到带有高于最小学习的修改身份置信度阈值（如 20%）的值的对应的当前身份置信度 412。按本发明的一实施例应用学习的身份置信度修改符的示例过程在下面参考图 8 描述。在步骤 608 之后，如上参考图 5 所述，可利用当前的身份置信度 412。

在步骤 610，主动的网络属性身份置信度修改符 416 被应用到与匹配当前主动的网络属性 410 的发出的主动的网络属性 406 相关联的每个当前的身份置信度。按本发明的一实施例应用主动的网络属性身份置信度修改符的示例过程在下面参考图 9 描述。步骤 610 之后，如上面参考图 5 所述，可以使用当前的身份置信度 412。

图 7 示出按本发明的一实施例，将被动的网络属性身份置信度修改符应用到当前的身份置信度的示例步骤。在步骤 702，从发出的网络识别符组 402（图 4）选择下一个发出的网络识别符（NID）作为候的网络识别符。每个发出的网络识别符能与一个或多个被动的网络属性如 PNA_1、PNA_2 和 PNA_3 关联。在步骤 704，选择下一个被动的网络识别符（PNA）作为候选的被动网络属性。候选的被动网络属性在当前被动网络属性 408（当前值）的组及与候选的网络识别符（发出的值）相关联的发出的被动网络属性 404 的子集中均有条目。例如，PNA_1 具有在当前被动网络属性 408 中的当前值，和在发出的被动网络属性 404 中与候选的网络识别符相关联的发出值。

在步骤 706，在当前被动网络属性 408（图 4）中的候选的被动网络属性条目与在发出的被动网络属性 404 中与候选的网络识别符关联的候选的被动

网络属性条目相比较。若在当前被动网络属性值与发出的被动网络属性值之间存在匹配，则过程进到步骤 708。否则过程进到步骤 710。

每个被动网络属性能与一个或多个被动的网络属性身份置信度修改符 414（图 4）关联，例如，被动网络属性 PNA_1、PNA_2 和 PNA_3 能关系到被动网络属性身份置信度修改符 $PNA\ ICM_1$、$PNA\ ICM_2$，和 $PNA\ ICM_3$。在当前与发出的网络属性之间的匹配能增加在特定计算机网络识别中的置信度。某些身份置信度修改符，即正的（+ve）身份置信度修改符打算作为当前和发出的网络属性之间匹配的结果被应用。在当前和发出的网络属性之间的不匹配能减少在特定计算机网络识别中的置信度。某些身份置信度修改符，即负的（-ve）身份置信度识别符打算作为当前和发出的网络属性之间的不匹配的结果被应用。每个被动网络属性能与正的和负的被动网络属性身份置信度修改符相关联。

在步骤 708，与候选的被动网络属性相关的正的被动网络属性身份置信度修改符（+ve PNA ICM）被应用到与候选的网络识别符相关的当前身份置信度。在步骤 710，与候选的被动网络属性相关的负的被动网络属性身份置信度修改符（-ve PVA ICM）被应用到与候选的网络识别符相关的当前身份置信度。

在本发明的一实施例中，身份置信度修改符 414、416 和 418（图 4）能将当前身份置信度设置成特定值，或当前身份置信度的函数的结果，如设置成当前的身份置信度的线性变换的结果。例如，对 IP 子网的被动网络属性的身份置信度修改符能被“设置当前身份置信度到 50%。对认证域名被动网络属性的正的身份置信度修改符可以被“增加 20%到当前身份置信度”。对认证域名被动网络属性的负的身份置信度修改符可以被“从当前身份置信度减去 20%。对 IP 子网规格被动网络属性的负的身份置信度修改符能被“设置当前的身份置信度为 0%”。身份置信度修改符 414，416 和 418 也能是空修改符，即在应用到当前身份置信度时不起作用。

在步骤 712 判断，对该候选网络识别符是否还有更多被动网络属性的候选。若还有被动网络属性候选，则过程返回到步骤 704。否则过程进到步骤 714。在步骤 714 判断，是否还有更多发出的网络识别符候选。若对该计算机网络还有更多发出的网络识别符候选，则过程返回到步骤 702。否则，被动的网络属性身份置信度修改符 414（图 4）已被应用到当前的身份置信度 412。本专业人士明白，等价的过程是可能的，例如步骤 704 可以被理解成穿越身份置

信度估值树的决策操作。

图 8 示出按本发明的一实施例将学习的身份置信度修改符应用到当前的身份置度的示例步骤。在步骤 802，从发出的网络识别符 402（图 4）的组选择下一个发出的网络识别符（NID）作为候选的网络识别符。在步骤 804 判断，该候选的网络识别符的当前身份置信度是否高于最小学习的修改身份置信度阈值。若候选的网络识别符的当前身份置信度高于最小学习的修改阈值，则过程进到步骤 806。否则过程进到步骤 808。

每个发出的网络识别符能具有相关的学习的身份置信度修改符以及当前的身份置信度。在步骤 806，与候选的网络识别符关联的学习的身份置信度修改符（LICM）被应用到候选的网络识别符的当前身份置信度。在本发明的一实施例中，存在当前身份置信度的封顶值，如 80%，当前的身份置信度不能通过学习的身份置信度修改符提升到超过它。按本发明的一实施例，确定学习的身份置信度修改符的示例过程在下面参考图 10 予以描述。

在步骤 808 判断，是否还有更多的发出的网络识别符候选者。若存在更多的发出的网络识别符候选者，则过程返回到步骤 802。否则，学习的身份置信度修改符 418（图 4）被应用到当前的身份置信度 412。

图 9 示出按本发明的一实施例，将主动的网络属性身份置信度修改符应用到当前的身份置信度的示例步骤，此示例过程与参考图 7 的示例过程具有相似性。结果，参考图 7 描述的各方面能应用于此例，反之亦然。

在步骤 902，选择下一个发出的网络识别符 401（图 4）作为侯选的网络识别符。每个发出的网络识别符能与一个或多个主动的网络属性，如 ANA，和 ANA2，相关联。在步骤 904，选择下一个那样的主动的网络属性作为侯选的主动的网络属性。该侯选的主动网络属性具有在当前的主动网络属性 410 中的当前值，和在发出的主动网络属性 406 中与侯选的网络识别符相关的发出值。

在步骤 906 中，候选的网络属性的当前值和与侯选的网络识别符相关的发出值比较。若在当前的主动网络属性和发出的主动网络属性之间存在匹配，则过程进到步骤 908。否则过程进到 910。

如被动的网络属性的情况，每个主动的网络属性能与一个或多个主动的网络属性身份置信度修改符 416（图 4）相关。某些主动的网络属性身份置信度修改符能是正的主动的网络属性身份置信度修改符(+ve NAN ICM)，作为在

当前及发出的主动网络属性之间匹配的结果被应用。某些主动的网络属性身份置信度修改符能是负的主动网络属性身份置信度修改符(-ve ANA ICM)，作为在当前及发出的主动网络属性之间不匹配的结果被应用。例如，主动的网络属性 ANA1 能与主动的网络属性身份置信度识别符+ve ANA ICM1 相关，而主动网络属性 ANA2 能与主动网络属性身份置信度修改符+ve ANA ICM2 和-ve ANA ICM2 相关联。

在步骤 908，与侯选的主动网络属性相关的正的主动网络属性身份置信度修改符被应用到与侯选的网络识别符相关的当前身份置信度。在步骤 910，与侯选的主动网络属性相关的负的主动网络属性身份置信度修改符被应用到与侯选的网络识别符相关的当前身份置信度。对认证状态（带特定远程认证服务器），主动网络属性的示例正的主动网络属性身份置信度修改符是“设置当前身份置信度到 100%”。对认证状态，主动网络属性的示例负的主动网络属性身份置信度修改符是“设置当前身份置信度到 0%”。

在步骤 912 判断对该侯选的网络识别符是否还存在更多的主动网络属性侯选者。若存在更多的主动网络属性侯选者，则过程返回到 904。否则过程进到步骤 914。在步骤 914 判断，是否存在认为是对该计算机网络的更多的发出的网络识别符侯选者。若还存在更多的发出的网络识别符，则过程进到步骤 902。否则该主动网络属性身份置信度修改符 416（图 4）已被应用到当前的身份置信度 412。本专业人士明白，等价于所描述的例子的过程是可能的，例如，步骤 906 能理解成穿过身份置信度估值树的分支决策。

对特定的计算机网络的被动网络属性在主动网络属性之前变成可用。可能没有主动网络属性就不能达到高的网络身份置信度，如 100%，例如被动网络属性可能是不安全的，或可能就是那种策略，即高的置信度网络识别包括由主动网络属性的确认。为了提供与主动网络属性无关的精确的网络身份置信度，可将学习的身份置信度修改符 418（图 4）应用到当前身份置信度 412。

学习的身份置信度修改符 418 能开始作为默认的身份置信度修改符，例如作为空修改符。若主动网络属性在一旦变成可用时确认无关于主动网络属性作出的特定身份置信度测定，则相关的学习的身份置信度修改符将被增加，即如此转换，使得在应用时，学习的身份置信度修改符将导致更高的身份置信度值。若主动的网络属性与无关于主动网络属性作出的特定身份置信度测定矛盾，则有关的学习的身份置信度修改符能被减少，即如此转换，使得在

应用时，学习的身份置信度修改符将导致更低的身份置信度值。例如，学习的身份置信度修改符能通过将学习的变量值加到身份置信度值修改身份置信度修改身份置信度。为增加此学习的身份置信度修改符，可将增加常数加到学习的身份置信度修改符，可将增加常数加到学习的变量上。为减少此学习的身份置信度，从学习的变量中减去该增加常数。在本发明的一实施例中，学习的身份置信度修改符 418 如此调节，使得对特定的计算机网络在主动网络变得可用之前和之后的当前身份置信度 412 之间的差最小。

图 10 和 11 示出按本发明的一实施例将学习的身份置信度修改符更新成为新可用的主动网络属性的结果的示例步骤。在图 10 的步骤 1002，一个或多个主动网络属性已成为最新可用的。例如，网络位置认知组件 308 能通知网络指纹组件 310（图 3），该网络指纹组件 310 预订的主动网络属性的新的可用性。在更新当前的主动网络属性 410（图 4）之前判断，自从当前身份置信度 412 最近一次无关于主动网络属性地计算以来，该主动网络属性是否第一次变成新的可用的。

例如，网络指纹组件 310 可以将主动网络属性已改变的指示符 422 与被动网络属性已改变的指示符 420 作比较。若每个主动网络属性已改变的指示符小于（如具有较早的时间标记）最早的被动网络属性已改变的指示符，则可以确定，这是自从当前身份置信度 412 最近一次无关主动网络属性被计算以来主动网络属性第一次变成最新可用。若确实如此，则过程进到步骤 1004。否则，过程进到步骤 1006。

在步骤 1004，无关于主动网络属性（pre-ANA CIC）计算的当前身份置信度 412（图 4）的拷贝被记录，如记录在临时存储器中。在步骤 1006，用新可用的主动网络属性更新一个或多个当前主动网络属性 410。在步骤 1008，更新对应的主动网络属性已改变的指示符 422。在本发明的一实施例中，步骤 1006 和 1008 作为基本更新操作出现。

在步骤 1010，如上面参考图 5 描述地计算当前的身份置信度 412（图 4）。得到的当前身份置信度 412（新 CIC）被更新，以反映由新可用的主动网络属性提供的信息。在步骤 1012，通过将记录的身份置信度（老的 pre-ANA CIC）与新计算的当前身份置信度（新 CIC）比较，调节学习的身份置信度修改符 418。若特定的老的和新的身份置信度对比较结果较差（如具有大的差别），则可以调节对应的学习的身份置信度修改符，使得在未来计算中减少该差。

与特定的老的和新的身份置信度对相关的学习的身份置信度修改符若比较良好（如具有低的差），则可以保持不调整。

图 11 示出按本发明的一实施例更新学习的身份置信度修改符的示例步骤。例如，图 11 中示出的步骤可用来执行图 10 的步骤 1012。在步骤 1102，选择下一个发出的网络识别符作为侯选的网络识别符。在步骤 1104，候选的网络识别符的当前身份置信度（新 CIC 的一个）与最小学习的身份置信度阈值比较。若侯选的网络识别符的当前身份置信度高于最小学习的身份置信度阈值，如 0%，则过程进行步骤 1106。否则，过程进到步骤 1108。

在步骤 1106，侯选的网络识别符的新计算的（即上面参考图 10 描述的）当前身份置信度与该侯选的网络识别符的记录的身份置信度(即老的，pre-ANA CIC）比较。若当前（新）身份置信度与记录的（老的）身份置信度比较结果很好（如匹配），则不希望调节到学习的身份置信度修改符，且过程进到步骤 1108。若记录的身份置信度小于当前的身份置信度，则希望增加学习的身份置信度修改符，且过程进到步骤 1110。若记录的身份置信度大于当前的身份置信度，则希望减少学习的身份置信度修改符，且过程进到步骤 1112。

在步骤 1110，侯选的网络识别符的学习的身份置信度修改符能（如线性地）增加，使得下次应用较高的当前身份置信度结果。例如，若在步骤 1110 之间学习的身份置信度修改符能是“增加 20%到当前的身份置信度”，则在步骤 1110 之后，学习的身份置信度修改符能是“增加 40%到当前的身份置信度。”在步骤 1112，侯选的网络识别符的学习的身份置信度修改符可以（如线性地）减少，使得下次应用较低的当前身份置信度结果。例如，若在步骤 1112 之前学习的身份置信度修改符被“从当前身份置信度减少 20%”，则在步骤 1112 之后，学习的身份置信度修改符被“从当前身份置信度减少 40%。”

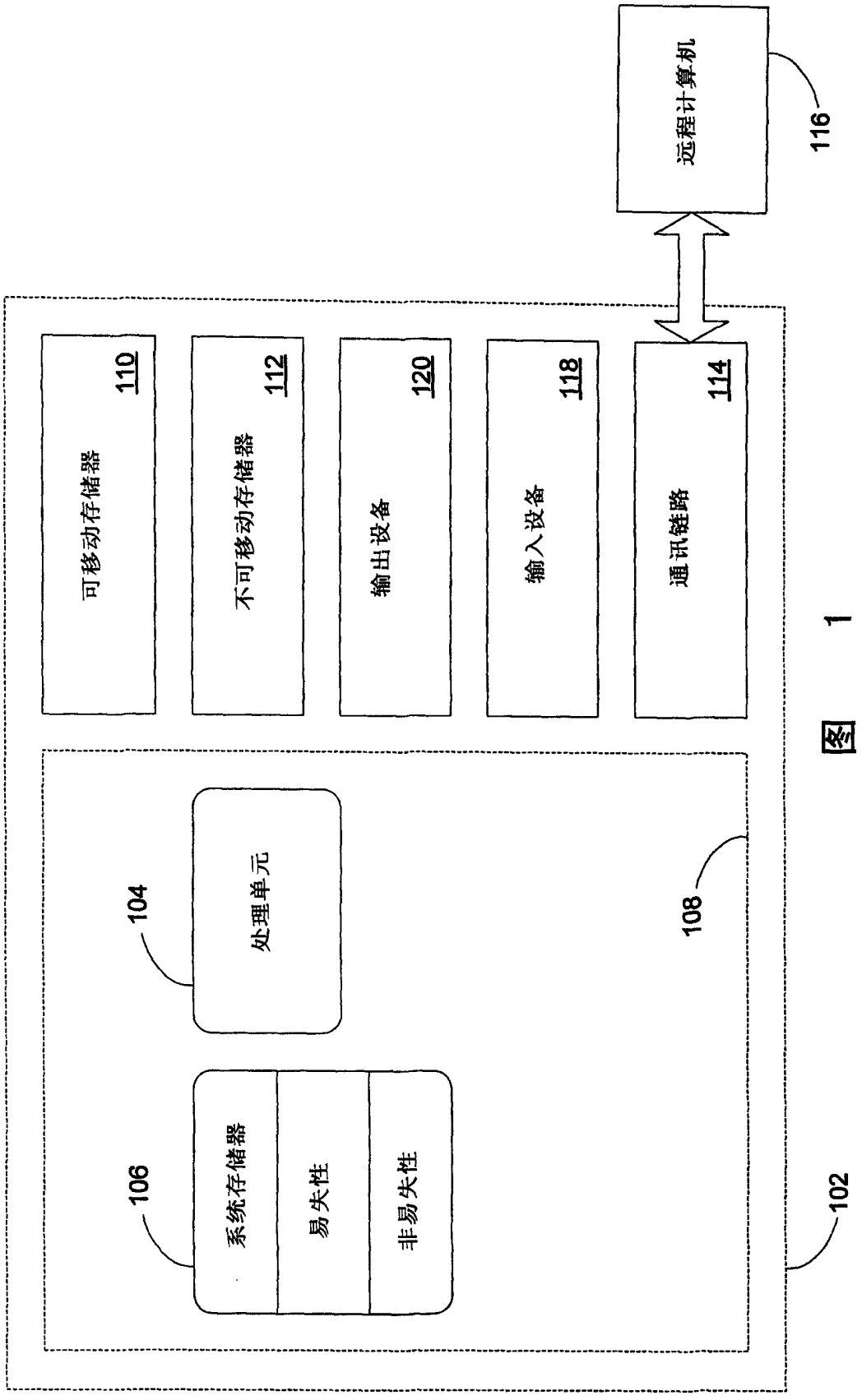
在步骤 1108，判断，是否存在更多的发出的网络识别符侯选者。若还有更多的侯选的网络识别符，则过程返回步骤 1102。否则按本发明的一实施例，学习的身份置信度修改符 418（图 4）已被调整。

包括出版的资料，专利申请及专利的所有这里引用的参考资料加入这里作为同样范围内容的参考，好象每个参考资料单独和特别地表明加入这里作为参考，并以其整体列举在这里。

在描述本发明的上下文中术语“a”和“an”和“the”及相关事物的使用（尤其在下面权利要求中）被解释为包括单数与复数，除非特地指出或明显

与上下文矛盾。术语“**comprising-**由...组成”，“**having-**具有”，“**including-**包括”，“**containing-**包含”被解释为无终止的术语（即，意味着“包括但不限于”），除非另作说明。这里对值的范围的列举仅试图用作参照落入该范围的每个各别的值的简化方法，除非这里另作说明，且每个单独的值被加入到说明中，好象它在这里单独地被列举。这里描述的所有方法能以任何合适的次序执行，除非这里另外指出或明显与上下文矛盾。任何和所有例子或这里提供的示例语言（如“诸如”）的使用只试图更好地解释本发明，而不对本发明的范围提出限止，除非另加声明。在专利说明中没有语言被解释为将任何非权利要求的元素解释为对实施本发明是重要的。

这里描述了本发明的较佳实施例，包括发明者所知的完成本发明的最好方式。在阅读前面描述后，这里较佳实施例的变种对本专业人士是明白的。本发明期待专业人士合适的采用那些变动，且本发明者希望本发明在不同于这里说明性描述的情况实践。因此，本发明包括在附后的权利要求引用的被专利应用的法律允许的主题的所有修改及等价物。此外，在所有可能变种中上述元素的所有组合被本发明所包含，除非这里另外指出或明显与上下文矛盾。


远程计算机
116
可移动存储器
110
不可移动存储器
112
输出设备
120
输入设备
118
通讯链路
114
处理单元
104
系统存储器
易失性
非易失性
106
108
102
1

图

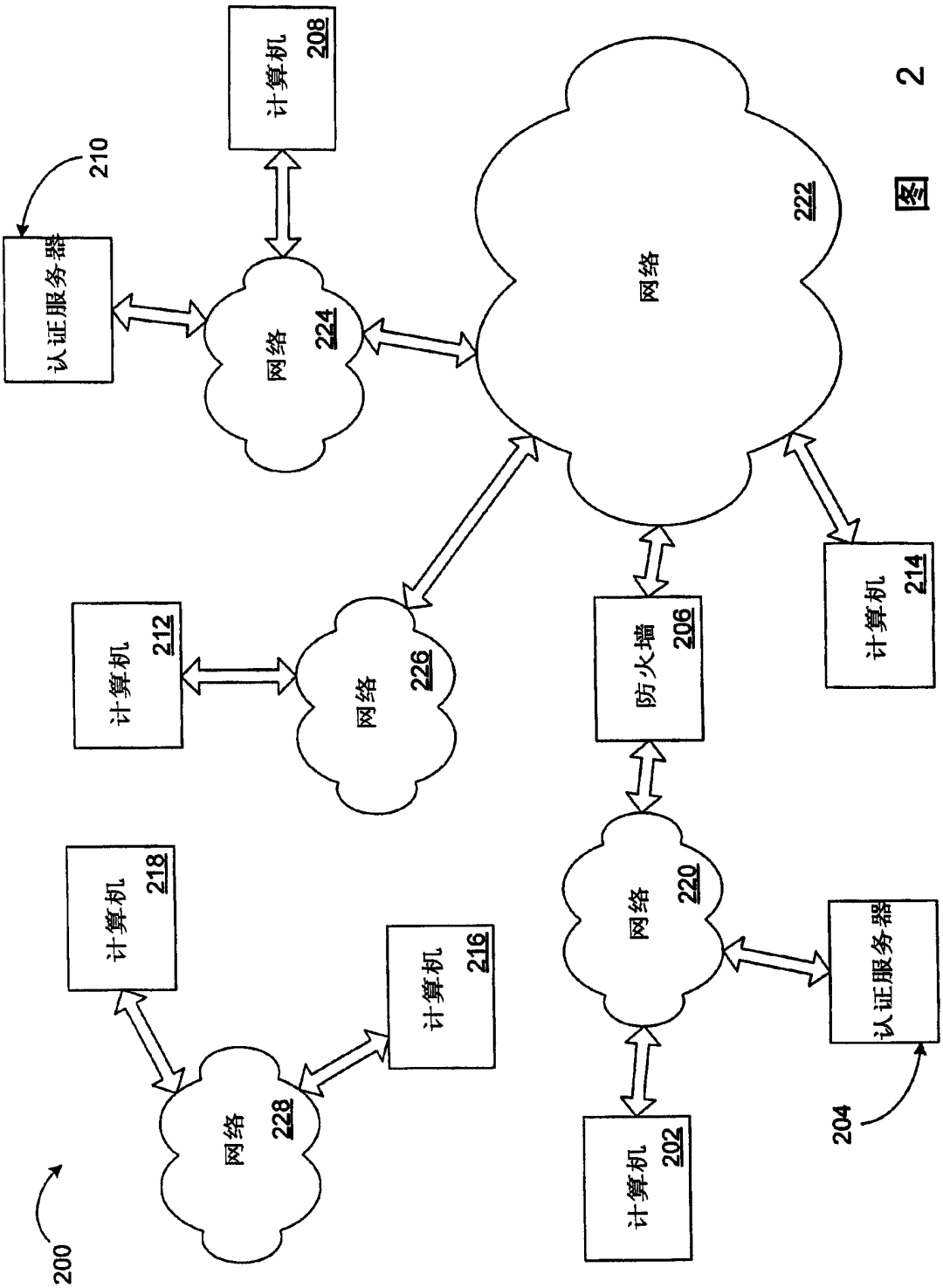

200
计算机 202
计算机 208
210
认证服务器
网络 224
网络 222
网络 226
计算机 212
网络 228
计算机 218
计算机 216
网络 220
防火墙 206
计算机 214
204
认证服务器

图 2

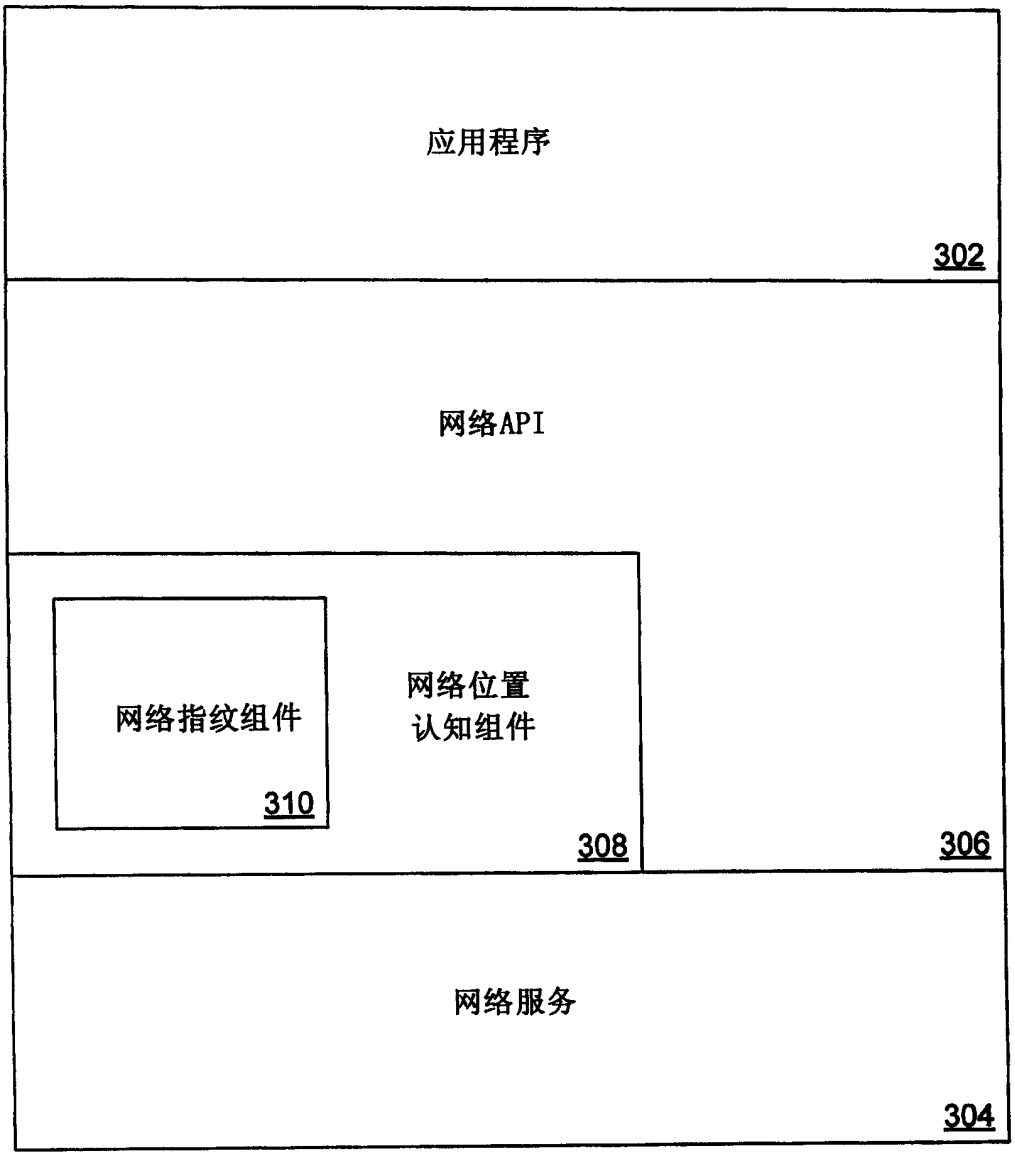


图 3

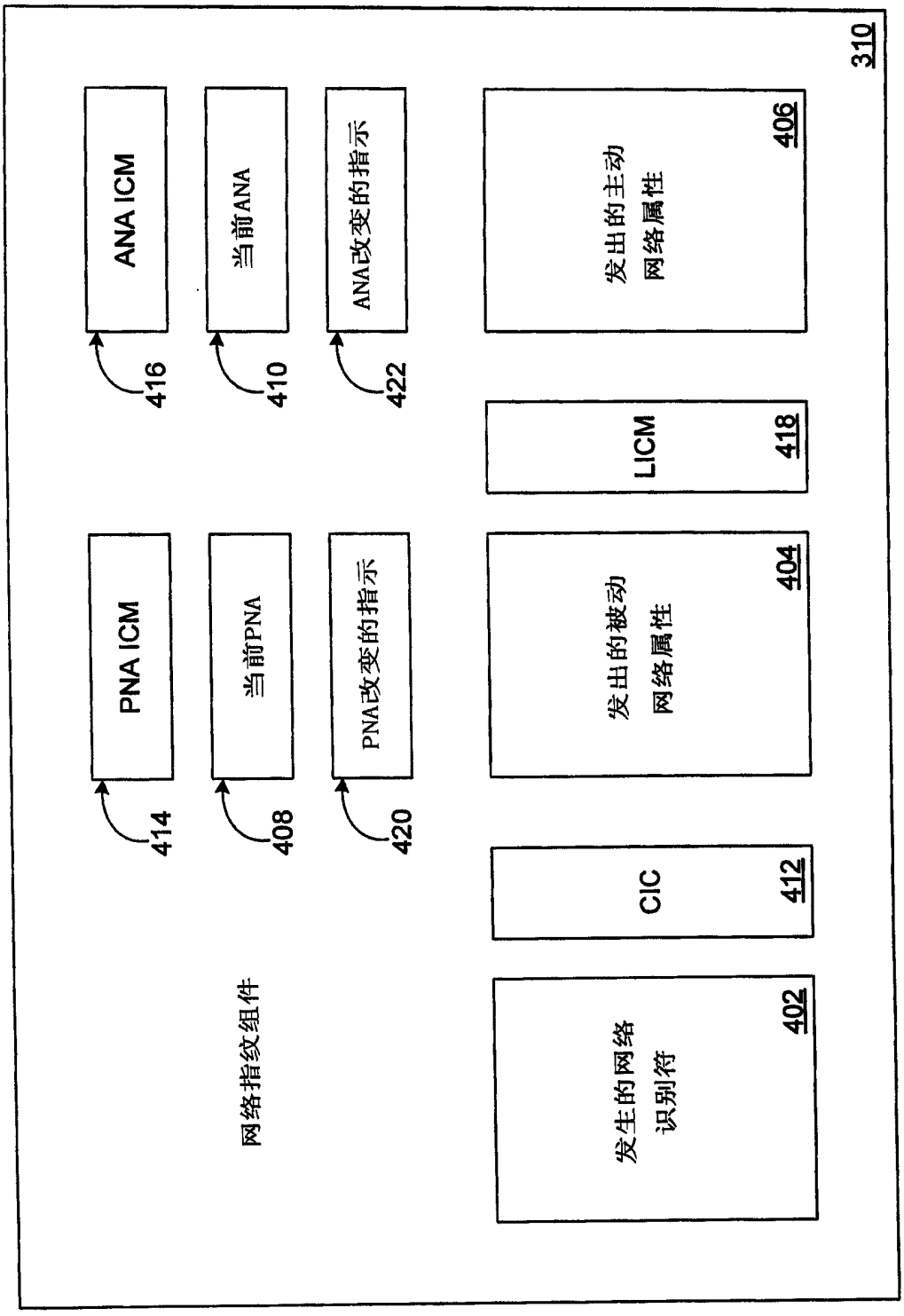

310
网络指纹组件
发生的网络识别符
402
CIC
412
发出的被动网络属性
404
LICM
418
发出的主动网络属性
406
PNA ICM
414
当前PNA
408
PNA改变的指示
420
ANA ICM
416
当前ANA
410
ANA改变的指示
422

图 4

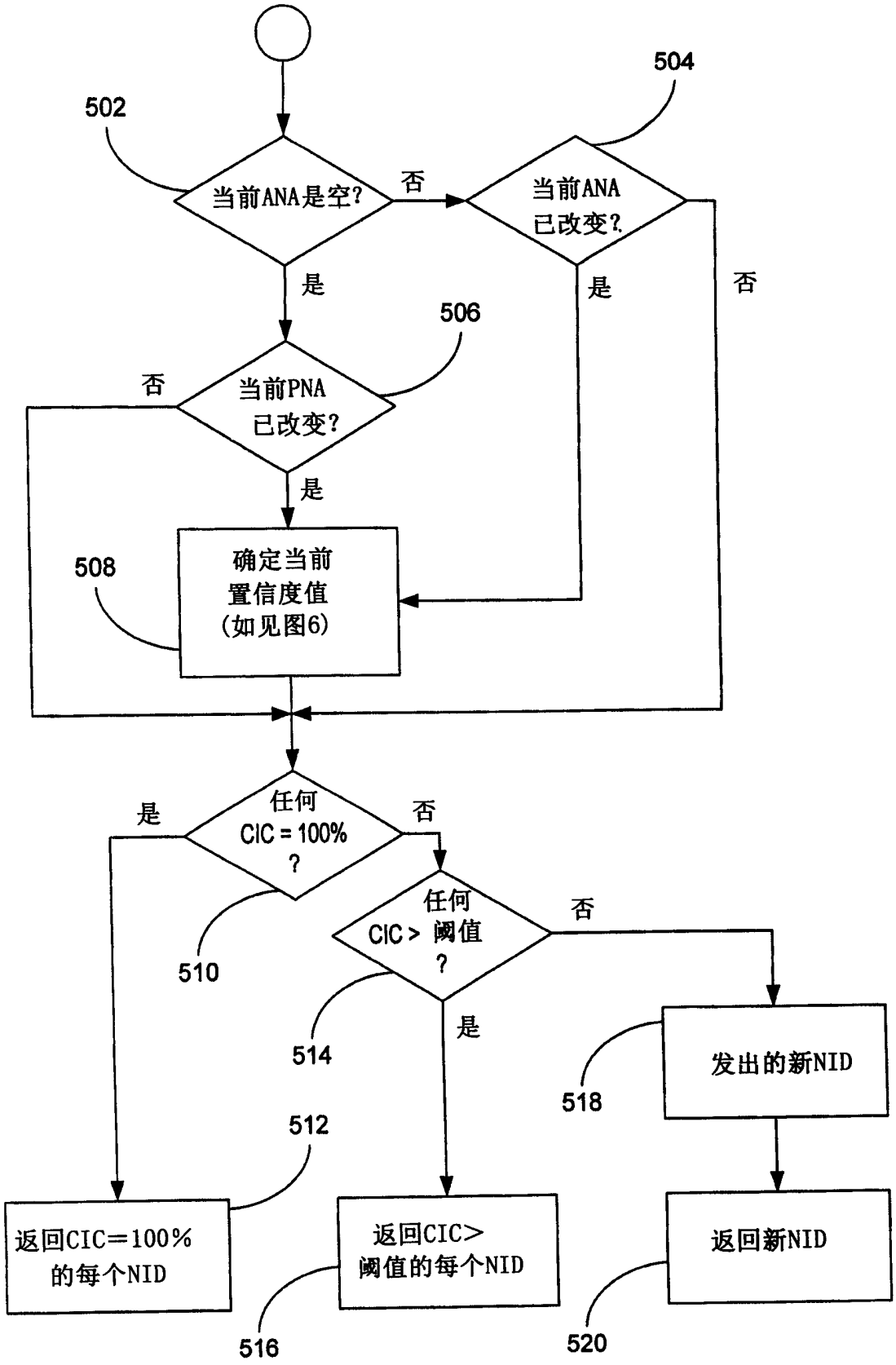

502
当前ANA是空?
否
504
当前ANA
已改变?
是
否
是
506
当前PNA
已改变?
否
是
508
确定当前
置信度值
(如见图6)
任何
CIC = 100%
?
是
否
510
任何
CIC > 阈值
?
否
514
是
发出的新NID
518
512
返回CIC=100%
的每个NID
返回CIC>
阈值的每个NID
516
返回新NID
520

图 5

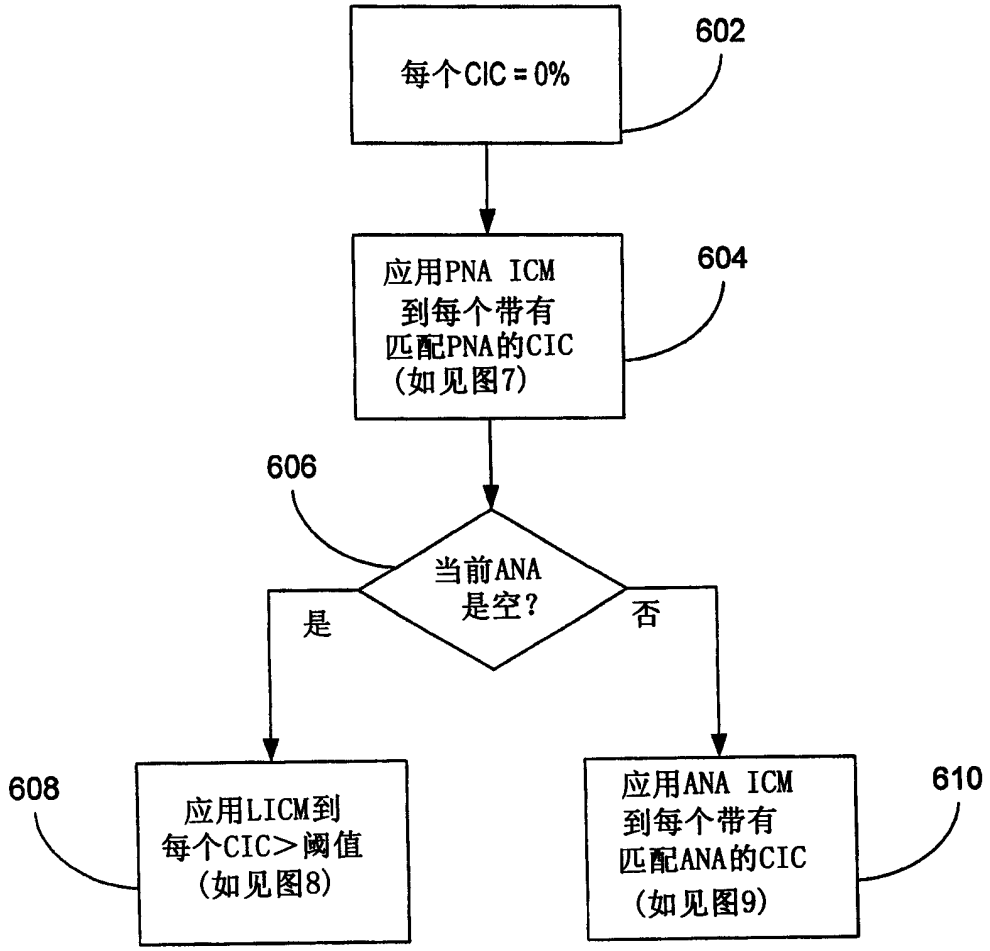

每个CIC = 0%
602
应用PNA ICM
到每个带有
匹配PNA的CIC
(如见图7)
604
606
当前ANA
是空?
是
否
608
应用LICM到
每个CIC>阈值
(如见图8)
应用ANA ICM
到每个带有
匹配ANA的CIC
(如见图9)
610

图 6

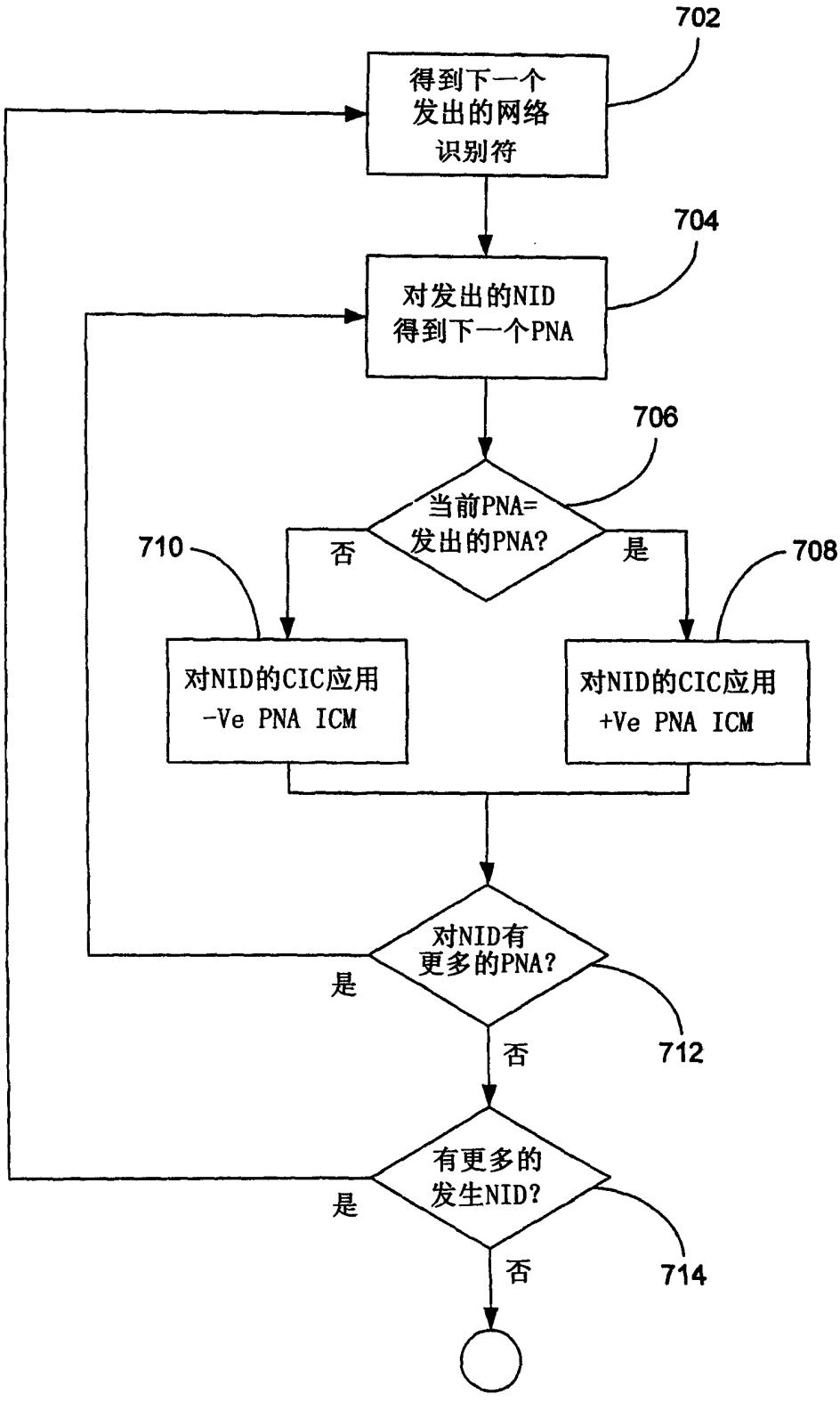

702
得到下一个
发出的网络
识别符
704
对发出的NID
得到下一个PNA
706
当前PNA=
发出的PNA?
否
是
710
708
对NID的CIC应用
-Ve PNA ICM
对NID的CIC应用
+Ve PNA ICM
对NID有
更多的PNA?
是
否
712
有更多的
发生NID?
是
否
714

图 7

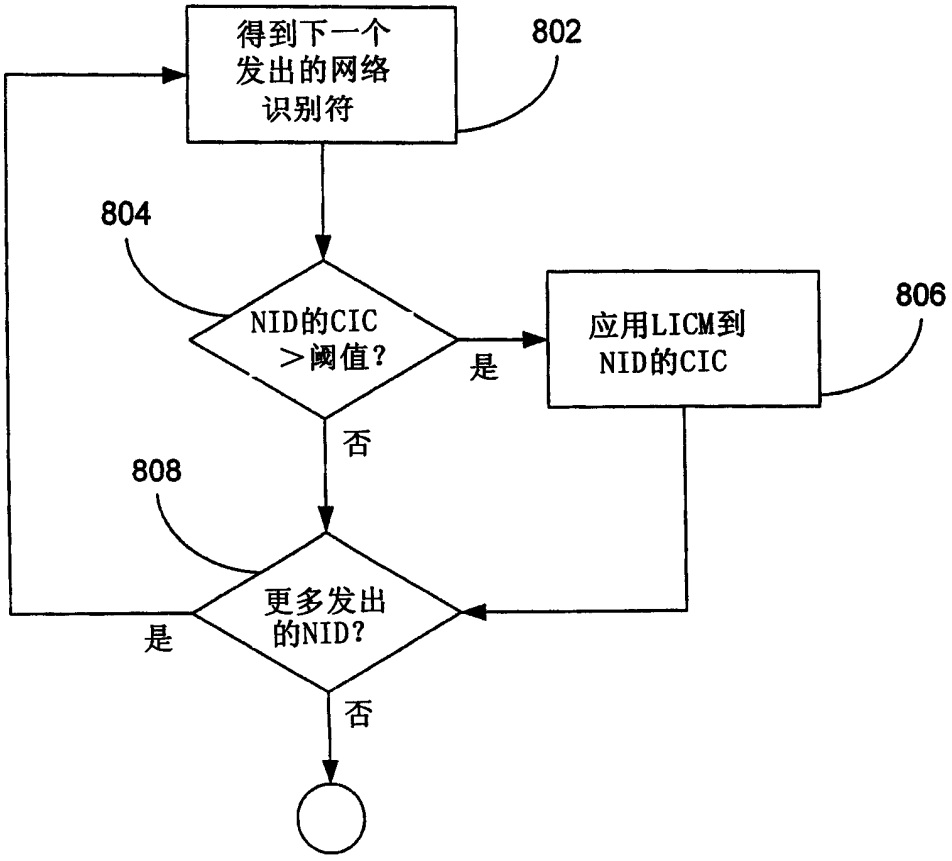

得到下一个
发出的网络
识别符
802
804
NID的CIC
＞阈值?
是
应用LICM到
NID的CIC
806
否
808
更多发出
的NID?
是
否

图 8

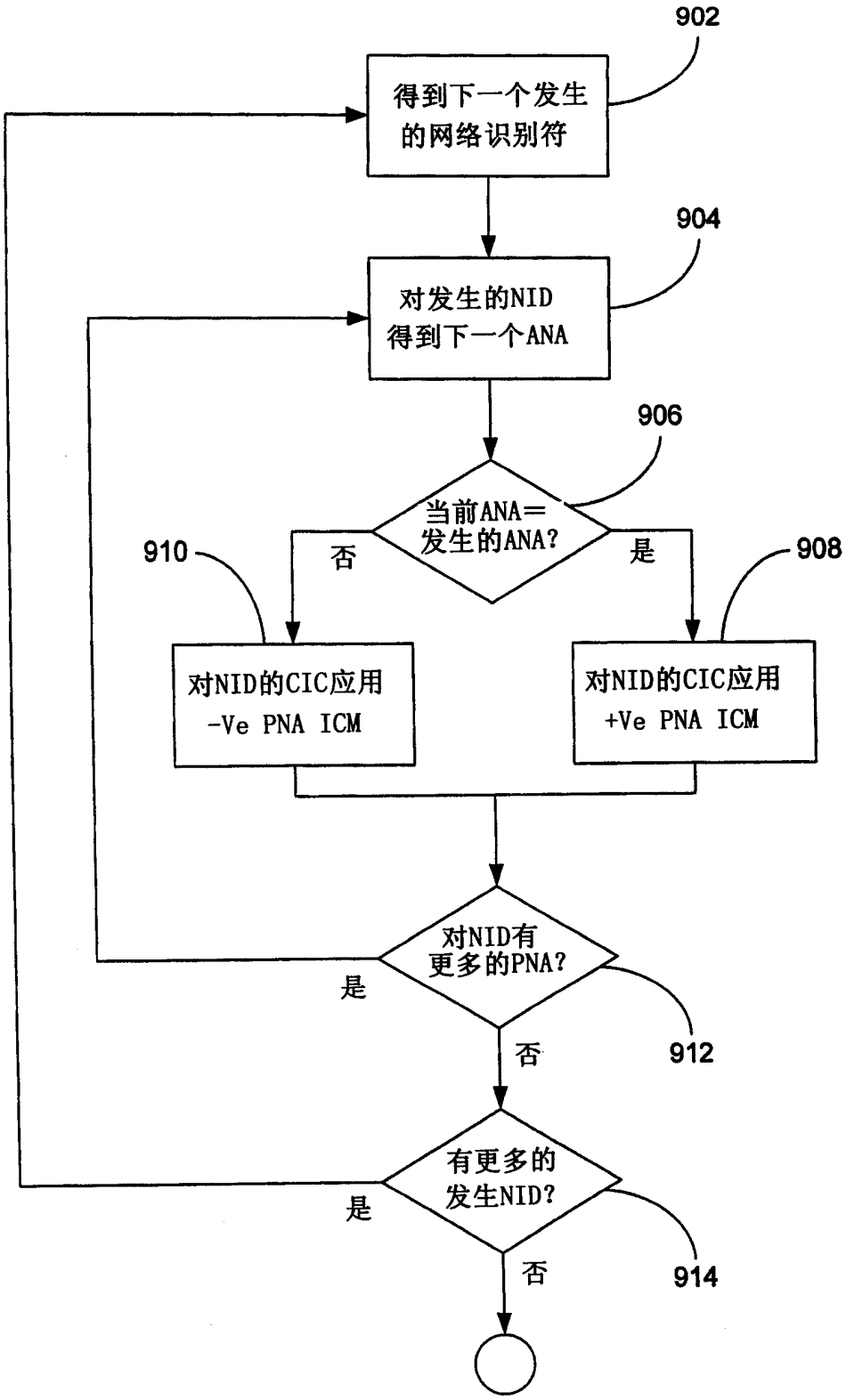

902
得到下一个发生的网络识别符
904
对发生的NID得到下一个ANA
906
当前ANA=发生的ANA?
否
是
910
908
对NID的CIC应用-Ve PNA ICM
对NID的CIC应用+Ve PNA ICM
对NID有更多的PNA?
是
否
912
有更多的发生NID?
是
否
914

图 9

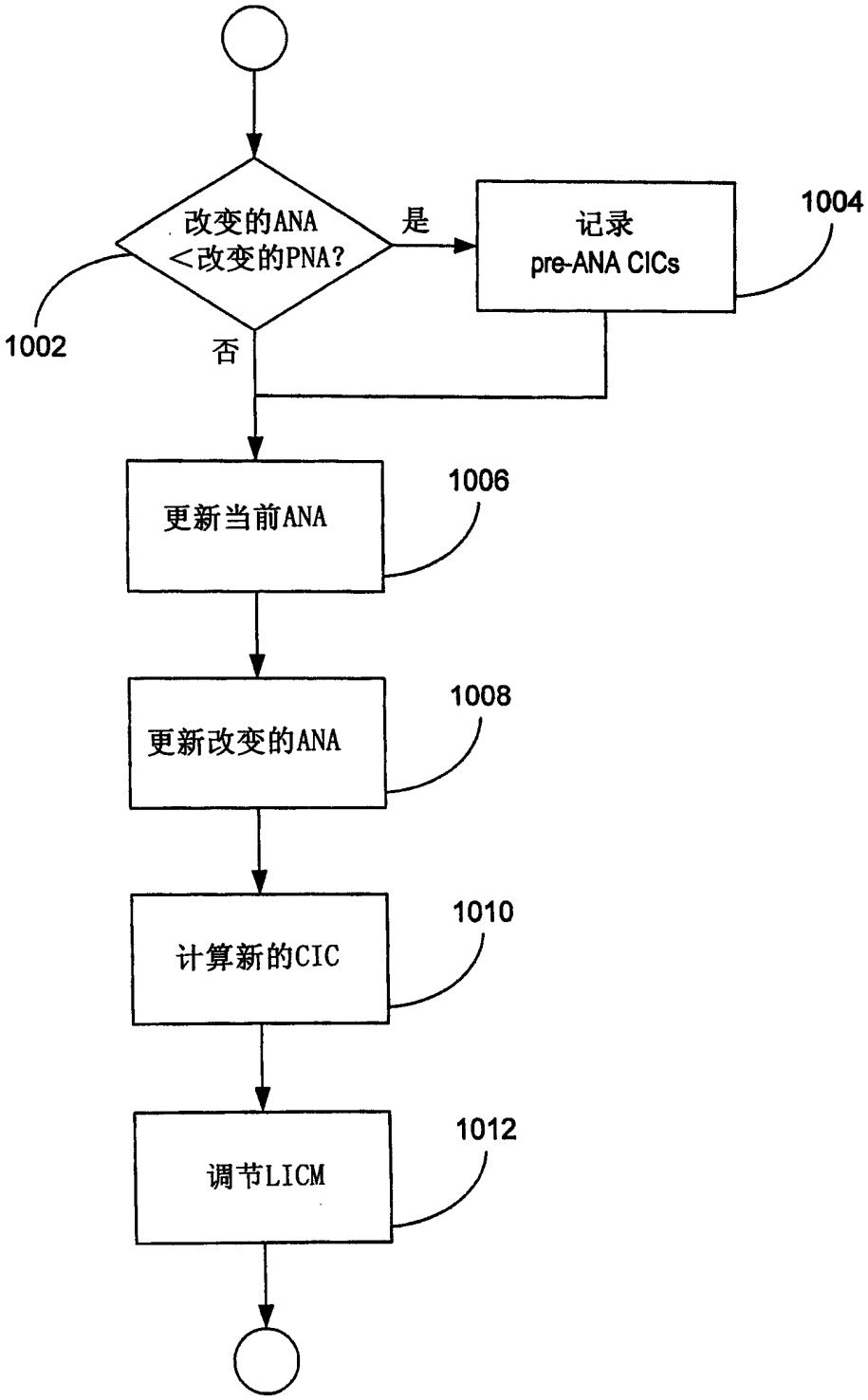

改变的ANA
<改变的PNA?
是
记录
pre-ANA CICs
1004
1002
否
更新当前ANA
1006
更新改变的ANA
1008
计算新的CIC
1010
调节LICM
1012

图 10

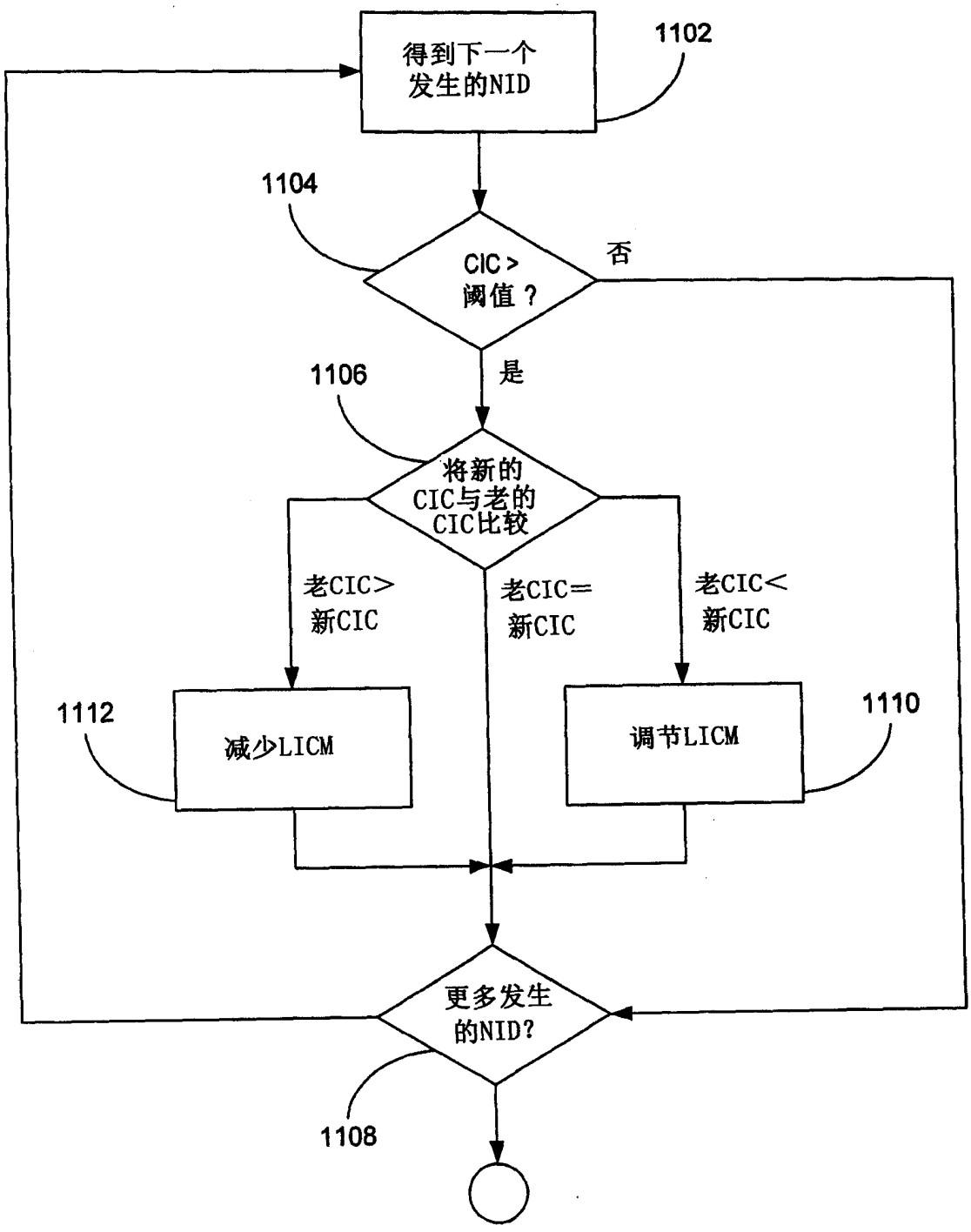

得到下一个
发生的NID
1102
1104
CIC>
阈值？
否
是
1106
将新的
CIC与老的
CIC比较
老CIC>
新CIC
老CIC=
新CIC
老CIC<
新CIC
1112
减少LICM
调节LICM
1110
更多发生
的NID?
1108

图 11