



(12) 发明专利申请



(10) 申请公布号 CN 116457754 A

(43) 申请公布日 2023. 07. 18

(21) 申请号 202180077033.4

(22) 申请日 2021.11.24

(30) 优先权数据

17/122,363 2020.12.15 US

(85) PCT国际申请进入国家阶段日

2023.05.16

(86) PCT国际申请的申请数据

PCT/CN2021/132683 2021.11.24

(87) PCT国际申请的公布数据

W02022/127538 EN 2022.06.23

(71) 申请人 国际商业机器公司

地址 美国纽约

(72) 发明人 L·P·戈麦斯

(74) 专利代理机构 北京市中咨律师事务所

11247

专利代理师 于静 刘薇

(51) Int.Cl.

G06F 9/30 (2006.01)

权利要求书3页 说明书23页 附图15页

(54) 发明名称

辅助处理器命令类型过滤

(57) 摘要

辅助处理器命令类型过滤包括确定目标辅助处理器是否被配置为支持选定命令类型过滤模式,以及另一辅助处理器是否被配置为支持选定命令类型过滤模式。基于确定目标辅助处理器未被配置为支持选定命令类型过滤模式并且基于另一辅助处理器被配置为支持选定命令类型过滤模式,将命令转发到另一辅助处理器以供处理以确定命令对于选定命令类型过滤模式是否有效。基于在另一辅助处理器处的处理,获得关于命令对于选定命令类型过滤模式是否有效的指示。基于获得命令对于选定命令类型过滤模式有效的指示,将命令发送到目标辅助处理器以供执行。



1. 一种用于促进计算环境内的处理的计算机程序产品,所述计算机程序产品包括:
一个或多个计算机可读存储介质以及共同存储在所述一个或多个计算机可读存储介质上的程序指令,以执行一种方法,所述方法包括:

确定所述计算环境的多个辅助处理器中的目标辅助处理器是否被配置为支持选定命令类型过滤模式;

检查所述多个辅助处理器中的另一辅助处理器是否被配置为支持所述选定命令类型过滤模式;

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式,向所述另一辅助处理器转发命令以供处理,以确定所述命令对于所述选定命令类型过滤模式是否有效;

基于在所述另一辅助处理器处的处理,获得关于所述命令对于所述选定命令类型过滤模式是否有效的指示;以及

基于获得所述命令对于所述选定命令类型过滤模式有效的指示,将所述命令发送到所述目标辅助处理器以供执行。

2. 根据权利要求1所述的计算机程序产品,其中所述方法进一步包括,基于获得所述命令对于所述选定命令类型过滤模式无效的指示,将所述命令由于对于所述选定命令类型过滤模式无效而拒绝,并且制止在所述目标辅助处理器上执行所述命令。

3. 根据权利要求2所述的计算机程序产品,其中,所述拒绝进一步包括将错误代码放置在中央位置以促进访问所述错误代码。

4. 根据权利要求1所述的计算机程序产品,其中,所述方法进一步包括:

基于获得所述命令对于所述选定命令类型过滤模式有效的指示,将所述命令作为选定命令类型过滤模式命令添加到命令列表,所述命令列表用于确定哪些命令对于在所述目标辅助处理器上的执行是有效的;以及

基于获得所述命令对于所述选定命令类型过滤模式无效的指示,将所述命令作为有效的辅助处理器命令添加到所述命令列表。

5. 根据权利要求1所述的计算机程序产品,其中,所述方法进一步包括,基于确定所述多个辅助处理器未被配置为支持所述选定命令类型过滤模式,拒绝所述命令。

6. 根据权利要求1所述的计算机程序产品,其中,所述方法进一步包括:

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式,确定所述命令是否在命令列表上,所述命令列表用于确定所述命令是否将在所述目标辅助处理器上执行;以及

基于确定所述命令不在所述命令列表上,将所述命令转发到所述另一辅助处理器以供处理。

7. 根据权利要求6所述的计算机程序产品,其中,所述方法进一步包括,基于所述命令在所述另一辅助处理器上成功执行,将所述命令作为有效的选定命令类型过滤模式命令添加到所述命令列表。

8. 根据权利要求6所述的计算机程序产品,其中,所述方法进一步包括,基于所述命令在所述另一辅助处理器上未成功执行,将所述命令作为有效的辅助处理器命令添加到所述命令列表。

9. 根据权利要求1所述的计算机程序产品,其中,所述选定命令类型过滤模式是无状态命令过滤模式。

10. 根据权利要求1所述的计算机程序产品,其中,所述多个辅助处理器包括多个密码卡。

11. 一种用于促进计算环境内的处理的计算机系统,所述计算机系统包括:

存储器;以及

至少一个处理器,与所述存储器通信,其中,所述计算机系统被配置为执行一种方法,所述方法包括:

确定所述计算环境的多个辅助处理器中的目标辅助处理器是否被配置为支持选定命令类型过滤模式;

检查所述多个辅助处理器中的另一辅助处理器是否被配置为支持所述选定命令类型过滤模式;

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式,向所述另一辅助处理器转发命令以供处理,以确定所述命令对于所述选定命令类型过滤模式是否有效;

基于在所述另一辅助处理器处的处理,获得关于所述命令对于所述选定命令类型过滤模式是否有效的指示;以及

基于获得所述命令对于所述选定命令类型过滤模式有效的指示,将所述命令发送到所述目标辅助处理器以供执行。

12. 根据权利要求11所述的计算机系统,其中所述方法进一步包括,基于获得所述命令对于所述选定命令类型过滤模式无效的指示,将所述命令由于对于所述选定命令类型过滤模式无效而拒绝,并且制止在所述目标辅助处理器上执行所述命令。

13. 根据权利要求11所述的计算机系统,其中,所述方法进一步包括:

基于获得所述命令对于所述选定命令类型过滤模式有效的指示,将所述命令作为选定命令类型过滤模式命令添加到命令列表,所述命令列表用于确定哪些命令对于在所述目标辅助处理器上的执行是有效的;以及

基于获得所述命令对于所述选定命令类型过滤模式无效的指示,将所述命令作为有效的辅助处理器命令添加到所述命令列表。

14. 根据权利要求11所述的计算机系统,其中,所述方法进一步包括,基于确定所述多个辅助处理器未被配置为支持所述选定命令类型过滤模式,拒绝所述命令。

15. 根据权利要求11所述的计算机系统,其中,所述方法进一步包括:

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式,确定所述命令是否在命令列表上,所述命令列表用于确定所述命令是否将在所述目标辅助处理器上执行;以及

基于确定所述命令不在所述命令列表上,将所述命令转发到所述另一辅助处理器以供处理。

16. 一种促进计算环境内的处理的计算机实施的方法,所述计算机实施的方法包括:

确定所述计算环境的多个辅助处理器中的目标辅助处理器是否被配置为支持选定命令类型过滤模式;

检查所述多个辅助处理器中的另一辅助处理器是否被配置为支持所述选定命令类型过滤模式；

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式，向所述另一辅助处理器转发命令以供处理，以确定所述命令对于所述选定命令类型过滤模式是否有效；

基于在所述另一辅助处理器处的处理，获得关于所述命令对于所述选定命令类型过滤模式是否有效的指示；以及

基于获得所述命令对于所述选定命令类型过滤模式有效的指示，将所述命令发送到所述目标辅助处理器以供执行。

17. 根据权利要求16所述的计算机实施的方法，进一步包括，基于获得所述命令对所述选定命令类型过滤模式无效的指示，将所述命令由于对于所述选定命令类型过滤模式无效而拒绝，并且制止在所述目标辅助处理器上执行所述命令。

18. 根据权利要求16所述的计算机实施的方法，进一步包括：

基于获得所述命令对所述选定命令类型过滤模式有效的指示，将所述命令作为选定命令类型过滤模式命令添加到命令列表，所述命令列表用于确定哪些命令对于在所述目标辅助处理器上的执行是有效的；以及

基于获得所述命令对于所述选定命令类型过滤模式无效的指示，将所述命令作为有效的辅助处理器命令添加到所述命令列表。

19. 根据权利要求16所述的计算机实施的方法，进一步包括，基于确定所述多个辅助处理器未被配置为支持所述选定命令类型过滤模式，拒绝所述命令。

20. 根据权利要求16所述的计算机实施的方法，进一步包括：

基于确定所述目标辅助处理器未被配置为支持所述选定命令类型过滤模式并基于所述另一辅助处理器被配置为支持所述选定命令类型过滤模式，确定所述命令是否在命令列表上，所述命令列表用于确定所述命令是否将在所述目标辅助处理器上执行；以及

基于确定所述命令不在所述命令列表上，将所述命令转发到所述另一辅助处理器以供处理。

辅助处理器命令类型过滤

背景技术

[0001] 一或多个方面总体上涉及促进计算环境内的处理,且明确地说,涉及促进与计算环境内的命令处理相关联的处理。

[0002] 计算环境常常包括不同类型的处理器以增强处理。作为示例,计算环境可以包括被认为是主处理器的一个或多个中央处理单元,以及被认为是从属于中央处理单元的一个或多个辅助处理器(adjunct processor)。辅助处理器通常执行特定类型的任务。例如,辅助处理器的特定示例是用于执行密码操作的密码(加密)卡。

[0003] 由纽约州阿蒙克的国际商业机器公司提供的密码卡的示例是信道附接Crypto Express卡。Crypto Express卡被定义为支持多种类型的命令,诸如使用加密密钥的命令(称为安全密钥命令)、使用清除密钥的命令(称为清除密钥命令)、散列命令、查询命令、随机数生成器命令等。进一步地,Crypto Express卡被设计成支持多种模式,包括例如:公共加密架构(CCA)模式、加速器模式、以及企业公钥加密标准(PKCS)模式(又名XCP/EP11-企业PKSC#11模式)。每个模式被配置为处理特定类型的命令。

[0004] Crypto Express卡可被配置为在激活的机器配置的持续时间内以不同的多个模式之一操作。因此,如果客户希望使用不同模式,那么计算环境将至少包括用于不同的多个模式的数量的卡,每个卡配置在不同模式中并且能够处理如对该模式定义的特定类型的命令。

发明内容

[0005] 通过提供一种用于促进计算环境内的处理的计算机程序产品来克服现有技术的缺点,并且提供附加的优点。计算机程序产品包括一个或多个计算机可读存储介质和共同存储在一个或多个计算机可读存储介质上以执行方法的程序指令。所述方法包括:确定计算环境的多个辅助处理器中的目标辅助处理器是否被配置为支持选定命令类型过滤模式;以及检查多个辅助处理器中的另一辅助处理器是否被配置为支持选定命令类型过滤模式。基于确定目标辅助处理器未被配置为支持选定命令类型过滤模式并且基于另一辅助处理器被配置为支持选定命令类型过滤模式,命令被转发到另一辅助处理器以供处理以确定命令对于选定命令类型过滤模式是否有效。基于在另一辅助处理器处的处理,获得命令对于选定命令类型过滤模式是否有效的指示。基于获得命令对选定命令类型过滤模式有效的指示,将命令发送到目标辅助处理器以供执行。

[0006] 通过由另一辅助处理器处理命令,模拟命令的执行,使得知道命令对于在目标辅助处理器上的执行是否有效。模拟消除了对于为所支持的每个辅助处理器类型保持每个命令类型过滤模式的辅助处理器命令的静态列表的需要。由此,处理变得容易,性能提高。

[0007] 在一个实施例中,基于获得命令对于选定命令类型过滤模式无效的指示,命令由于对于选定命令类型过滤模式无效被拒绝,并且制止其在目标辅助处理器上执行。由此,通过在另一辅助处理器上模拟命令并且确定命令在选定命令类型过滤模式下是无效的,并且因此不在目标辅助处理器上如请求那样执行来促进处理并且改进性能。

[0008] 在一个实施例中,拒绝包括将错误代码放置在中央位置以促进对错误代码的访问。使用独立于辅助处理器模式的中心位置来返回错误代码,有助于由程序定位错误代码,而不管是谁产生的错误(例如,使用命令类型过滤模拟的管理程序,在特定模式中的辅助处理器等)。

[0009] 在一个实施例中,基于获得所述命令对选定命令类型过滤模式有效的指示,将所述命令作为选定命令类型过滤模式命令添加到命令列表。命令列表将用于确定哪些命令对于在目标辅助处理器上的执行是有效的。进一步,在一个实施例中,基于获得命令对于选定命令类型过滤模式无效的指示,将命令作为有效的辅助处理器命令添加到命令列表。动态更新的命令列表通过促进确定哪些命令对于目标处理器有效来促进处理和改进性能。然而,命令列表是可选的,因为命令可在支持选定命令类型过滤模式的一个或多个辅助处理器上模拟。

[0010] 在一个实施例中,基于确定多个辅助处理器未被配置为支持选定命令类型过滤模式,拒绝命令。在一个实施例中,如果没有辅助处理器支持选定命令类型过滤模式,则不执行模拟;由此,促进处理,并且改进性能。

[0011] 在一个实施例中,基于确定目标辅助处理器未被配置为支持选定命令类型过滤模式并基于另一辅助处理器被配置为支持选定命令类型过滤模式,确定命令是否在命令列表上,命令列表用于确定命令是否将在目标辅助处理器上执行。基于确定命令不在命令列表上,将命令转发到另一辅助处理器用于处理。动态更新的命令列表通过促进确定哪些命令对于目标辅助处理器有效来促进处理和改进性能。

[0012] 在一个实施例中,基于命令在另一辅助处理器上的成功执行,将命令作为有效的选定命令类型过滤模式命令添加到命令列表。在一个实施例中,基于命令在另一辅助处理器上未成功执行,将命令作为有效辅助处理器命令添加到命令列表。

[0013] 作为示例,选定命令类型过滤模式是无状态命令过滤模式。进一步,作为示例,多个辅助处理器包括多个密码卡。

[0014] 在此还描述并要求保护与一个或多个方面有关的计算机实施的方法和系统。进一步,本文还描述并可要求保护与一个或多个方面有关的服务。

[0015] 通过在此描述的技术实现附加特征和优点。其他实施例和方面在本文中详细描述,并且被认为是所要求保护的方面的一部分。

附图说明

[0016] 一个或多个方面被特别指出并且被清楚地要求保护作为说明书结尾处的权利要求书中的示例。从下面结合附图的详细描述中,一个或多个方面的上述目标、特征以及优点显而易见,其中:

图1A示出了结合和使用本发明的一个或多个方面的计算环境的一个示例;

图1B示出了结合和使用本发明的一个或多个方面的计算环境的另一个示例;

图2A-2D示出了根据本发明的一个或多个方面的处理辅助处理器队列指令的示例;

图3A示出了根据本发明的一个或多个方面的辅助处理器命令请求消息的一个示例;

图3B示出了根据本发明的一个或多个方面的请求连接性编程请求块(CPRB)的一个示例;

图3C示出了根据本发明的一个或多个方面的辅助处理器命令回复消息的一个示例;

图3D示出了根据本发明的一个或多个方面的回复连接性编程请求块(CPRB)的一个示例;

图3E示出了根据本发明的一个或多个方面的图3C中的报头的字段的一个示例;

图4A示出了根据本发明的一个或多个方面的命令类型过滤过程的一个示例;

图4B示出了根据本发明的一个或多个方面的模拟命令类型过滤的流程的一个示例;

图5A-5B示出了根据本发明的一个或多个方面的与促进计算环境内的处理相关的方面一个实施例;

图6A示出了结合和使用本发明的一个或多个方面的计算环境的一个示例;

图6B示出了结合和使用本发明的一个或多个方面的计算环境的另一个示例;

图6C示出了根据本发明的一个或多个方面的图6B的存储器的进一步细节的一个示例;

图6D示出了根据本发明的一个或多个方面的图6B的存储器的进一步细节的另一示例;

图7A示出了结合和使用本发明的一个或多个方面的计算环境的另一个示例;

图7B示出了根据本发明的一个或多个方面的图7A的存储器的进一步细节;

图8示出了根据本发明的一个或多个方面的云计算环境的一个实施例;以及

图9示出了根据本发明的一个或多个方面的抽象模型层的一个示例。

具体实施方式

[0017] 在本发明的一个或多个方面中,提供过滤能力,其使诸如密码(加密)卡的辅助处理器能够以每一命令为基础动态地确定由辅助处理器获得的命令是否要由辅助处理器执行。例如,一个或多个每一命令过滤指示符(例如,选定命令类型过滤指示符)用于确定所接收的命令是否是如由每一命令过滤指示符指定的有效命令类型,并且因此将由辅助处理器执行。在一个实施例中,基于与命令的请求者相关联的计算策略,按每一命令设置一个或多个每一命令过滤指示符。因此,由一个请求者发出的命令可以是用于执行的有效命令类型,但是由另一个请求者发出的命令可以是无效的,如由基于请求者的计算策略设置的每一命令过滤指示符所指定的。

[0018] 在一个或多个方面,为了使辅助处理器参与每一命令过滤,至少一个过滤设施将被安装在辅助处理器上。可以安装不同的过滤设施,并且每个设施具有要在每一命令过滤中使用的至少一个相关联的过滤指示符(例如,选定命令类型过滤指示符)。过滤设施的一个示例是无状态命令过滤设施,其中选定命令类型(例如,无状态命令类型命令)对于执行是有效的。例如,如果辅助处理器支持例如无状态命令过滤设施,并且接收到的命令具有设置为选择值(例如,1)的无状态命令类型过滤指示符,则该命令将是要执行的无状态命令类型命令。如果命令是另一命令类型,甚至由辅助处理器的配置模式(例如,公共加密架构

(CCA) 模式;又名协处理器模式) 支持的命令类型,则它将被认为是无效的。然而,如果命令中的无状态命令类型过滤指示符被设置为另一值(例如,零),则该命令将是要执行的由辅助处理器的配置模式支持的任何命令类型。由此,在一个示例中,当支持过滤设施(例如无状态命令过滤设施)时,在一种模式(这里称为命令集模式)中配置的辅助处理器可以用于执行在配置的模式(例如协处理器模式)中支持的命令类型的全集或者命令类型的精简集(例如仅无状态命令类型命令)。

[0019] 虽然本文中作为一个示例描述了无状态命令过滤设施,但是可应用其他过滤设施或技术。例如,可以使用主密钥过滤设施,其中选定命令类型是主密钥管理密钥命令。作为另一示例,过滤可用策略施加的使用情况限制来实现。例如,如果选定命令访问的价格与通用密码命令访问的价格不同,则可以针对购买的使用情况施加过滤器。进一步的过滤级别可以基于性能服务协议,其中,基于所购买的性能,以高或低服务响应性能优先级来标注命令。也可以使用其他过滤设施或技术。在不针对另一模式重新配置辅助处理器的情况下,每个过滤设施的应用是可允许的。过滤设施可以彼此结合或分开使用。许多示例是可能的。

[0020] 在一个或多个方面,计算环境包括多个辅助处理器,并且辅助处理器中的一个或多个可能不支持命令类型过滤和/或特定命令类型过滤设施。因此,在一个实施例中,基于获得命令请求,确定请求的目标辅助处理器是否支持由请求指示的过滤设施(也称为命令类型过滤模式)。如果目标辅助处理器不支持所请求的设施,而另一辅助处理器支持,则根据本发明的方面,通过在另一辅助处理器上运行命令来模拟选定命令类型过滤模式的命令的操作。如果在另一辅助处理器上的命令的执行是有效的,则在目标处理器上执行该命令。

[0021] 参考图1A描述了结合和使用本发明的一个或多个方面的计算环境的一个实施例。在一个示例中,计算环境100包括至少一个中央处理单元102和至少一个辅助处理器(AP) 104,它们中的每一个耦合到存储器(被称为系统存储器106)的至少一部分。作为一个示例,系统存储器106包括硬件系统区域,其对在中央处理单元上执行的程序是间接可访问的和不可见的。(间接可访问在本文中用于意味着硬件系统区域或存储在其中的辅助处理器队列(以下描述)仅可由特定的有限指令访问而不能以其他方式访问(例如,不能加载到其中,程序不知道地址等))。位于系统存储器内的是一个或多个辅助处理器队列108。这些队列从用户程序不是直接可见的,而是被视为机器(即,包括中央处理单元、系统存储器和辅助处理器的机器)的一部分。中央处理单元通过例如发出将请求放置在队列上和/或从队列中移除回复的指令来访问系统存储器中的队列。然而,辅助处理器的确经由例如传输层110(例如,i390C0) 直接访问队列,并且负责将请求从队列取出、处理请求和将对请求的回复放置在队列上。

[0022] 参考图1B描述了结合和使用本发明的一个或多个方面的计算环境的另一个实施例。在此实施例中,机器包含虚拟支持,且存在包含多个访客152(例如,访客操作系统和/或访客程序)的至少一个主机中央处理单元150。主机中央处理单元耦合到存储器的至少一部分,称为系统存储器154。另外,存在至少一个辅助处理器156,其也经由例如传输层160耦合到系统存储器154。作为一个示例,系统存储器154包括硬件系统区域,并且位于系统存储器内的是一个或多个辅助处理器队列158。

[0023] 如所指示的,存在不同类型的辅助处理器,包括但不限于密码卡或适配器。密码卡的具体示例是由纽约州阿蒙克的国际商业机器公司提供的Crypto Express卡。尽管提供了

示例密码卡,但是由国际商业机器公司和/或其他公司提供的其他密码卡可以结合和/或使用本发明的一个或多个方面。进一步,其他类型的辅助处理器可以结合和/或使用本发明的一个或多个方面。

[0024] 在一个实施例中,辅助处理器(诸如密码卡(例如,Crypto Express卡))支持多种模式,包括但不限于协处理器模式、加速器模式和企业公钥加密标准(PKCS)模式(例如,XCP/EP11-企业PKCS#11),作为示例。另外,在其他示例中,可支持更少和/或其他模式。每个模式可具有其自己的AP消息结构和格式。

[0025] 作为示例,辅助处理器消息由多个数据段构成,并且数据段可以彼此不相邻;相反,一个或多个数据段可以交织。这些数据段被称为分散聚集数据段。在一个示例中,密码卡没有对入队的AP消息的直接访问,并且消息的一部分(例如,AP消息的底部)包含将由例如密码卡用于执行AP命令的数据。因此,AP命令传输层(例如,传输层110、160)复制来自AP命令请求消息的相关数据,将其打包成密码卡理解的格式(例如,密码卡的命令请求消息)并且将其发送到密码卡。类似地,在由密码卡执行AP命令之后,密码卡生成包括例如分组5和6的密码卡命令回复消息,并且将其发送到AP命令传输层,AP命令传输层将其重新封装到AP命令回复消息中。例如,传输层使用AP命令请求消息和加密卡的命令回复消息的不同部分来提供AP命令回复消息,包括报头、子报头和分组。然后,传输层将AP命令回复消息发送给AP队列,以便稍后由程序出队。以下描述AP命令请求消息和AP命令回复消息的进一步细节,包括根据本发明的一个或多个方面的命令类型过滤所使用的消息的方面。

[0026] 根据本发明的方面,设计了辅助处理器(例如,密码卡),其允许机器管理程序根据计算策略(例如,许可条款、准许和/或资源要求,诸如客户的高可用性要求等)来请求命令类型过滤。由于客户具有与其相关联的不同计算策略(例如,许可条款、准许和/或资源要求,诸如高可用性要求),并非所有类型的命令都可用于特定客户。由此,根据本发明的方面,提供命令类型过滤,使得选定辅助处理器(例如,被配置用于特定模式(例如,协处理器模式)的密码卡)能够用不同的计算策略并且因此不同的准许用于客户,而不需要辅助处理器被重新配置成不同的所支持的模式。

[0027] 作为示例,根据本发明的一个或多个方面,提供了AP命令类型过滤设施(APFT),该APFT允许基于一个或多个选定AP命令类型过滤设施基于每一命令对AP命令进行过滤。在一个示例中,一个或多个选定AP命令类型过滤设施包括无状态AP命令过滤设施(sAPCF)。本文中关于特定架构(例如,由纽约州阿蒙克的国际商业机器公司提供的z/Architecture®硬件架构)来描述AP命令类型过滤设施和无状态AP命令过滤设施的方面。z/Architecture(z/架构)硬件架构的一个实施例描述于2019年9月的IBM公开号SA22-7832-12第13版的“z/Architecture Principles of Operation(z/架构操作原理)”中,特此通过引用其全文结合在此。IBM和Z/ARCHITECTURE是国际商业机器公司在至少一个管辖区域中的注册商标。然而,z/Architecture硬件架构仅为一个示例架构。本发明的各方面还可基于其他架构,包括但不限于英特尔x86架构、国际商业机器公司的其他架构、和/或其他公司的架构。

[0028] 在一个示例中,当安装无状态AP命令过滤设施时,安装AP命令类型过滤设施。根据本发明的方面,为了确定是否安装了无状态AP命令过滤设施,使用处理辅助处理器队列指令。

[0029] 参考图2A描述处理辅助处理器队列(PQAP)指令的一个示例。如图所示,在一个示

例中,处理辅助处理器队列指令200包括指示辅助处理器队列的处理操作的操作代码(操作码)202(例如,32位指令的位0-15)。在一个实施例中,处理辅助处理器队列指令采用多个通用寄存器,包括通用寄存器0、1和2。根据通用寄存器0中指定的功能代码来处理由通用寄存器0中的AP队列号(APQN)指定的AP队列。下文进一步描述通用寄存器0、1和2的示例。

[0030] 参照图2B,在一个实施例中,通用寄存器0 (GR0) 210是例如64位寄存器,其包括例如指示要执行的选定功能的功能代码(FC) 212(例如,位32-39);用于指示在通用寄存器2中是否提供已安装设施的掩码的测试设施指示符(T) 214(例如,位40);以及识别辅助处理器队列(例如,AP队列108(图1A))的辅助处理器队列号(APQN) 216(例如,位48-63);根据功能代码处理的AP队列158(图1B))。

[0031] 基于下发处理辅助处理器队列指令,功能代码212将包括多个可接受代码中的一个,所述可接受代码的示例是代码00测试AP队列(TAPQ)。

[0032] 根据本发明的一个或多个方面,当计算环境处于例如z/Architecture架构模式中且安装APFT设施时,如果指定TAPQ功能代码(例如,在GR0中FC=00),那么将通用寄存器0的位40界定为TAPQ功能的测试设施位(T) 214。当T为1时,用所安装AP设施的掩码和其他相关信息替换通用寄存器2的位0-31,下文描述所述掩码的示例。当T为零时,指例如未安装APFT设施,通用寄存器2中的结果限于例如位位置32-63,且位位置0-31被忽略且不改变。在此情况下,AT和QD字段(下文描述)是有效的,且其他位位置存储为零。

[0033] 如所指示的,除了通用寄存器0之外,处理辅助处理器队列指令还使用通用寄存器1和2,本文进一步描述其中的每一个。

[0034] 参照图2C,在一个实施例中,通用寄存器1 (GR1) 220是例如包括例如辅助处理器队列状态字(APQSW) 222(例如,位32-63)的64位寄存器。在处理辅助处理器队列指令完成时,APQSW字段包含AP队列状态字,除非针对特定功能另外声明。AP队列状态字指例如在指令完成时AP队列的状态。

[0035] 此外,参照图2D,在一个实施例中,通用寄存器2 (GR2) 230是例如包括多个字段的64位寄存器。如本文中所描述,在一个实施例中,位位置0-31在经设置时包含所安装AP设施的掩码和其他相关信息。根据本发明的一个或多个方面的GR2的示例字段包括例如:

[0036] 模式232:当设置时,该字段(例如,位3-5)指示多个可能的AP模式设施。例如,当D(例如,位3)为1时,指定AP提供协处理器模式设施;当A(例如,位4)为1时,指定AP提供加速器模式设施;以及当X(例如,位5)为1时,指定的AP提供XCP模式设施;

[0037] SL234:当该字段(例如,位7)为1时,安装本发明的一个或多个方面的无状态AP命令过滤设施(SAPCF)。SAPCF设施例如是PCI-X(扩展外围组件互连)加密器件特征,并且在一个实施例中,其被安装在例如z/Architecture架构模式中;

[0038] 分类236:该字段(例如,位8至15)包含关于指定的辅助处理器(AP)的功能能力的信息。每个位表示结合由辅助处理器提供的设施的某个功能能力,如在寄存器的模式字段中所指示的(例如,位3-5)。如果将0存储到例如分类字段的位8至15,那么完整本机卡功能可用于指定AP。分类字段不是PCI-X密码器件特征并且不由系统固件设置。相反,其可选地由管理程序设置以基于访客的特权向其访客中的一个或多个提供完整的本机卡功能或完整的本机卡功能的一个或多个子集。作为示例,位8指示全AP命令集(FAPCS)设施。当位8被设置为一个值(例如,1)时,其指示完整的本机卡功能可用于指定的辅助处理器。当位8被设

置(例如,设置为1)时,将零(在一个示例中)存储在位9中。位9指示例如无状态AP命令(SAPC)设施。当位9被设置为一个值(例如,1)时,其指示仅无状态功能可用于指定的辅助处理器。当位9被设置(例如,设置为一)时,零(在一个示例中)被存储在位8中。在一示例中保留位10至15。

[0039] 可以由计算环境支持的与一个或多个设施有关的其他设施和/或信息可以由掩码的在例如位0-31中的一个或多个位来指示。

[0040] 辅助处理器类型(AT) 238:该字段(例如,位位置32-39)包括例如0-255范围内的指示不同辅助处理器类型的示例有效AP类型值;

[0041] AP队列条目数目(QD) 240:配置中每个AP队列上的队列条目数目。例如,QD是范围内(例如,0-31)的值,其表示所述范围内(例如,1-32十进制)的队列条目的数目。

[0042] 在一个示例中,通用寄存器2中返回的已安装设施信息应用于相同AP类型以及相同配置模式下(对于合并AP(例如,AP类型10或更高)而言)的所有AP。在一个示例中,所安装的设施信息至少持续到下一个子系统重置为止。可以同时添加设施。当AP类型的最后AP被解除配置时,设施可以或可以不同时移除。

[0043] 当TAPQ功能以例如条件代码0(成功完成)或条件代码3、响应代码例如02-05(非预期条件;例如,进行中的AP队列重置、AP解除配置、AP检查停止、AP忙碌)完成时,如所定义地修改通用寄存器2。否则,不修改通用寄存器2。

[0044] 虽然在本文的一个实施例中针对处理辅助处理器队列指令和其相关寄存器描述了特定字段、字段位置、字段大小、字段或位的位和值,但是在不脱离本发明一个或多个方面的精神的情况下,可以使用其他字段、字段位置、字段大小、字段或位的位和/或值。在一个实施例中,本文中未描述的通用寄存器中的每一者的字段和/或位可为空、具有预定义值(例如,零)和/或包括待忽略的值。存在许多可能性。

[0045] 根据一个或多个方面,辅助处理器(例如,加密卡)具有识别不同类型的命令的属性的逻辑。在一个实施例中,当一起考虑时,这些属性定义命令的集合和子集。在一个实施例中,不同类型的命令由管理程序提供。管理程序基于例如可从其接收命令请求的客户集确定例如命令类型标签集。例如,要由命令类型标签的集合表示的命令的类型是基于例如从其接收命令请求的客户的计算策略(例如,许可条款;准许;资源要求,诸如例如高可用性要求;等)。

[0046] 在一个示例中,命令具有与其相关联的表示命令的属性的标签集合(例如,策略或过滤标签),并且具有相同标签的命令可被视为一组。基于管理程序施加的命令类型标签的集合,相同的命令可以出现在多个命令类型集合中。例如,命令可以具有无状态命令类型标签以指示该命令是有效的无状态命令类型命令,可以具有主密钥命令类型标签以指示该命令是有效的主密钥命令类型命令,等等。存在命令类型、命令类型设施和命令类型命令的不同可能性,并且每个命令可具有与其相关联的一个或多个命令类型标签。

[0047] 由辅助处理器获得(例如,被提供、接收、检索等)命令类型标签的集合的指示。辅助处理器(例如,辅助处理器固件)基于可以由管理程序请求的命令类型标签的集合将预期命令分成不同的命令集合。例如,在一个特定示例中,辅助处理器接收命令类型标签的集合,包括用于安全密钥命令类型命令(例如,当由调用者请求时用于禁用安全密钥命令)的标签;以及用于无状态命令类型命令的标签。因此,辅助处理器使用每个命令的命令属性,

将使用加密密钥的命令(例如,安全密钥命令类型命令)认为是安全密钥命令类型命令集的一部分;并且剩余命令被认为是无状态命令类型命令集的一部分。在管理程序为其他过滤设施提供其他标签的其他实施例中,提供具有对应于其他标签的命令的其他命令集。许多类型的命令集是可能的。

[0048] 进一步,在一个实施例中,根据本发明的一个或多个方面,命令请求被配置为包括用于提供每一命令过滤的一个或多个过滤指示符,诸如一个或多个命令类型过滤指示符。参见图3A-3B描述关于包括在命令请求中的选定命令类型过滤指示符的进一步细节。

[0049] 参照图3A,在一个示例中,AP命令请求消息300包括报头302、子报头304以及多个数据分组306-312。在一个示例中,分组中的一个或多个(例如,分组-1308-310中的一个或多个)被配置成提供命令,并且分组中的一个或多个(例如,分组-2312)被配置成提供输入数据。根据本发明的一个方面,所述分组中的一个分组包括请求连接性编程请求块(CPRB)308,所述CPRB包括与命令类型过滤相关的一个或多个过滤指示符。

[0050] 例如,如图3B所示,请求CPRB 308包括AP命令过滤掩码320,该AP命令过滤掩码320包括一个或多个命令类型过滤指示符。命令类型过滤指示符的示例是无状态命令类型指示符322。该指示符指示所允许的命令集是用于无状态命令类型命令(例如,指示符322,诸如所选择的位,被设置为1)还是用于全命令集(例如,指示符322被设置为0)。其他指示符、标志、位等可被包括在请求CPRB 308中以指示可被过滤的其他类型的命令。例如,另一指示符可指示基于主密钥的过滤。许多其他示例是可能的。

[0051] 响应于消息,提供回复,并且在一个示例中,回复是AP命令回复消息的形式,其示例在图3C中描述。如图所示,AP命令回复消息330包括例如报头332、子报头334和多个分组336-340。根据本发明的方面,分组之一包括回复CPRB 336,该回复CPRB 336包括对请求的回复并且可以指示错误。

[0052] 例如,如图3D所示,回复CPRB 336包括错误指示。错误指示可包括错误代码350(例如,CPRB返回代码/原因代码)以报告客户请求的命令不被命令类型标签的定义集(例如,由管理程序或另一实体施加)所允许。

[0053] 在一个示例中,参照图3E,错误代码被转换成选定AP回复代码(例如,8B无效无状态命令)并且存储在回复代码字段352的报头332中。这提供了错误代码的中央位置。

[0054] 在一个实施例中,在AP命令请求消息进入进程内状态之后,如果安装了无状态AP命令过滤设施并且AP命令请求消息在CPRB中将无状态命令类型位(例如,无状态命令类型指示符322)设置为一但未指定无状态AP命令,或者如果未安装无状态AP命令过滤设施但安装了无状态AP命令设施并且AP命令请求消息未指定无状态AP命令,则命令请求的正常处理终止。作为一个示例,指定格式-1子报头的类型-86命令-回复消息与回复代码8B一起返回。

[0055] 在一个方面,命令请求消息的目标为特定辅助处理器,这里称为目标辅助处理器。因此,根据本发明的方面,确定目标辅助处理器是否能够运行命令。例如,如果命令请求包括指示仅允许请求者执行特定过滤设施或模式的命令的过滤指示符(例如,选定命令类型过滤指示符,诸如无状态命令类型指示符322),则确定目标辅助处理器是否支持命令类型过滤,具体地,是否支持由命令指示的特定过滤设施。在一个示例中,这经由处理辅助处理器队列指令或类似类型的指令来确定。如果目标辅助处理器不支持特定命令类型过滤模式,则根据本发明的方面,通过在支持特定命令类型过滤模式的另一辅助处理器上运行命

令、检查结果、然后如果结果指示用于选定命令类型过滤模式的有效命令、则在目标辅助处理器上运行命令来模拟命令。

[0056] 参考图4A至图4B描述了关于命令模拟的进一步细节。在图4A-4B的示例中,计算环境是云环境;然而,在其他实施例中,计算环境是非云环境。本发明的各方面不限于特定计算环境。进一步,在图4A-4B的示例中,辅助处理器是密码卡。然而,过滤可以由其他辅助处理器使用;密码卡仅是一个示例。

[0057] 参见图4A,在一个实施例中,管理程序(例如,下面描述的管理程序672(图6C);692(图6D))获得(例如,接收、被提供、检索、访问等)针对访客的请求策略402(例如,云请求策略),其基于账户配置404(例如,云账户配置),并且确定访客的操作模式(步骤400)。请求策略402包括例如基于由账户配置404提供的请求者的计算策略(例如,许可条款;资源需求,诸如高可用性需求;和/或准许;等等)。基于请求策略,管理程序在分类236中设置至少一个指示(例如,至少一个位)以指示用于配置的访客的能力。例如,如果访客被允许基于请求策略访问全AP命令集,则位8被设置为1并且位9被设置为零;然而,如果只允许访客访问选定的命令子集,例如无状态命令类型命令,那么位8被设置为零,位9被设置为一。其他位将用于其他类型的设施。位的设置应用于配置的所有辅助处理器,指示用于配置的访客的操作模式。作为示例,分类236的设置是在访客的初始程序加载(IPL)时、基于接收该请求来执行的,或者在对于一个或多个访客的另一时间执行,以反映每个访客的操作模式并保存(例如,针对每个访客的分类)。其他实施例是可能的。

[0058] 另外,管理程序获得(例如,接收、被提供、检索、访问等)要在模拟过程中使用的初始辅助处理器命令列表408,如本文所描述的。作为示例,管理程序基于从支持选定命令类型过滤设施(例如,无状态AP命令过滤设施)的密码卡获得的信息动态地生成AP命令列表,并且在模拟例如不支持选定命令类型过滤设施的目标密码卡上的无状态AP命令过滤操作时,使用命令列表,如下所述。在一个示例中,其用默认值初始化AP命令列表,诸如全零(空列表)或具有无状态AP命令指示符的已知无状态AP命令(或其他设施的命令)的列表。

[0059] 进一步,管理程序从访客获得(例如,接收、被提供、检索、访问等)AP命令请求消息406(例如,消息300),步骤405。作为示例,基于经由入队指令(诸如z/Architecture硬件架构的NQAP(入队辅助处理器队列)指令或另一架构的另一入队指令)将AP命令入队至目标AP队列的访客程序,在AP命令入队至目标AP队列之前,管理程序拦截来自访客的AP命令。

[0060] 管理程序确定访客是否被授权用于辅助处理器的配置的命令集模式(例如,协处理器全命令集),查询410。作为示例,管理程序通过检查基于请求策略402(其基于客户的计算策略)的分类236来确定访客是具有对命令的全集(例如,协处理器模式)还是对命令的精简集(例如,无状态命令过滤模式)的访问。如果访客被授权用于所配置的命令集模式,则管理程序将AP命令发送到目标辅助处理器,在目标辅助处理器(例如,加密卡)上执行AP命令,并且将结果返回到访客,步骤412。

[0061] 然而,如果访客未被授权用于所配置的命令集模式,查询410,而是被授权用于选定模式,诸如无状态命令过滤模式,则由例如管理程序做出关于在机器配置中是否存在支持选定命令类型过滤设施的密码卡的进一步确定,查询414。例如,确定无状态命令过滤设施是否被任何密码卡支持。这可以例如通过针对每个密码卡执行处理辅助处理器队列指令来确定。如果确定不存在支持选定命令类型过滤设施的密码卡,则管理程序拒绝AP命令,因

为不允许访客使用任何密码卡,步骤416。

[0062] 返回查询414,然而,如果存在支持选定命令类型过滤设施的至少一个密码卡,则由例如管理程序做出关于目标密码卡是否支持选定命令类型过滤设施的进一步确定,查询420。如果目标密码卡支持选定命令类型过滤设施,如由处理辅助处理器队列指令所指示的,则管理程序将命令请求中的过滤指示符、诸如选定命令类型过滤指示符设置为选择值(例如,1),并且向目标密码卡发送命令以用于处理,步骤422。例如,请求CPRB 308中的无状态命令类型指示符322被设置为1,然后,该请求被发送到目标密码卡进行处理。

[0063] 目标密码卡获得(例如,接收、被提供、检索等)命令请求消息且确定命令是否为用于选定命令类型过滤模式的有效命令,查询424。例如,命令是选定命令类型过滤设施的命令集的一部分?如果命令是选定命令类型过滤设施的命令集的一部分,那么命令由目标密码卡执行,并且结果被放置在密码卡的命令回复消息中,其被发送到例如AP传输层,步骤426。传输层将从密码卡接收的命令回复消息转换为AP命令回复消息(例如,消息330),该AP命令回复消息被返回至访客,步骤428。

[0064] 返回到查询424,如果命令不是有效的选定命令类型过滤命令(例如,其不在选定命令类型过滤设施的命令集中),那么目标密码卡将命令作为无效的选定命令类型过滤命令拒绝,且将此指示返回到传输层,步骤430。例如,将选定的错误代码(例如,错误代码350)包括在密码卡的回复消息的回复CPRB中,并且该回复消息被发送到传输层,作为示例。传输层转换从密码卡接收的回复消息,从而提供AP命令回复消息330,其包括回复CPRB 336的错误代码350以及报头332中的回复代码352。例如,传输层将CPRB中的选定错误代码转换为AP回复代码(例如,8B)并且将其放置在AP回复消息报头的AP回复代码字段中(例如,回复代码352)以促进回复代码的访问,步骤432。在步骤428,将回复消息发送至访客。

[0065] 返回到查询420,如果目标密码卡不支持选定命令类型过滤设施(例如,无状态命令过滤设施),则根据本发明的一方面,管理程序模拟选定命令类型过滤操作(例如,无状态命令过滤操作),如下所述,并且将操作的结果返回到访客,步骤450。参照图4B描述模拟选定命令类型过滤操作的进一步细节。

[0066] 参照图4B,在一个实施例中,管理程序检查所请求的命令的AP命令列表(例如,AP命令列表408),步骤452。例如,管理程序检查AP命令列表以查看目标AP命令是否包括在AP命令列表中。如果所请求的命令不在列表上,查询454,则将适当的过滤指示符(例如,选定命令类型过滤指示符,诸如无状态命令类型指示符322)设置为选择值,例如一,步骤456,并且将命令发送到支持选定命令类型过滤设施的密码卡之一。

[0067] 密码卡处理命令,并且管理程序检查结果,步骤458。如果结果指示用于选定命令类型过滤设施的有效命令,查询460,则管理程序将AP命令作为选定命令类型过滤命令(例如,作为无状态AP命令类型命令)添加到AP命令列表,步骤462。此外,在目标密码卡上执行AP命令,并且将结果返回至访客,步骤464。

[0068] 返回到查询460,如果结果经由例如错误代码指示用于选定命令类型过滤设施的无效命令,那么管理程序将命令作为有效AP命令(但不作为有效选定命令类型过滤命令)添加到命令列表,步骤466,且拒绝AP命令,步骤468。例如,管理程序通过在AP命令回复消息报头(例如,报头332)的AP回复代码字段(例如,回复代码352)中用新AP回复代码8B组成无效的无状态AP命令错误回复消息并且将组成的AP回复消息返回至将AP命令入队的访客以向

访客指示该命令不是选定AP命令类型命令,来将AP命令作为无效的选定命令类型过滤命令拒绝。

[0069] 返回到查询454,如果AP命令在AP命令列表上,则由例如管理程序做出关于命令是否是用于选定命令类型过滤设施的有效命令的进一步确定,查询470。如果命令对选定命令类型过滤设施有效,则处理继续到步骤464,在步骤464中,由管理程序将AP命令发送到目标密码卡,在目标密码卡上执行命令并将结果返回到访客。然而,如果AP命令对选定命令类型过滤设施无效,那么管理程序将AP命令作为对选定命令类型过滤设施的无效命令而拒绝,且将结果返回到访客,步骤468,如上所述。

[0070] 在一个实施例中,当访客程序经由例如出队指令(诸如z/Architecture硬件架构的出队辅助处理队列(DQAP)指令或另一架构的指令)将AP命令回复消息(例如,消息330)从AP队列出队时,其从密码卡(从管理程序模拟或加密卡)接收经处理的AP命令回复消息。访客程序在AP回复代码(例如,回复代码352)中看到相同的错误代码,例如,代码8B,而不管AP命令是被管理程序模拟拒绝还是被加密卡拒绝。然而,在一个实施例中,如果是密码卡处理AP命令而不是管理程序模拟,则访客程序将只看到命令回复消息的CPRB中的错误代码。因此,通过检查AP命令回复消息,CPRB错误代码可以用于确定错误的生成者。

[0071] 如本文所描述的,在一个实施例中,如果仅允许访客执行命令的子集(例如,无状态命令类型命令),但是管理程序的配置中的密码卡都不支持选定模式(例如,无状态AP命令过滤),则管理程序不独自模拟无状态AP命令过滤设施,并且不允许访客使用该密码卡。

[0072] 然而,根据本发明的方面,如果客户在选定命令类型过滤模式(例如,无状态AP命令过滤模式)下运行,但选定命令类型过滤设施未安装在目标密码卡上,那么管理程序通过模拟命令来检查以查看AP命令是否是选定命令类型过滤设施的命令。在一个示例中,这被执行而不是为其支持的每个密码卡类型保持选定命令的静态列表,为每个密码卡类型保持选定命令代静态列表是相当繁重的并且不容易及时获得以用于机器启动测试。其使用来自确实支持选定命令类型模式的其他密码卡之一的信息来在不支持选定命令类型模式设施的目标密码卡上模拟命令。AP命令回复消息由管理程序组成,且结果被发送至访客。

[0073] 如果客户在选定命令类型模式中运行并且对应于选定命令类型模式的选定AP命令类型过滤设施安装在目标密码卡上,则管理程序设置CPRB中的无状态命令类型指示符,并且将命令发送到目标密码卡以被执行。

[0074] 在一个实施例中,密码卡从管理程序接收命令请求消息(例如,AP命令请求消息300),基于CPRB中的管理程序施加的命令类型过滤指示符的集合来确定是否允许执行命令,如果基于管理程序施加的命令类型指示符的集合确定命令是有效的,则执行命令,并且将结果放置在命令回复消息中。命令回复消息被发送到例如AP命令传输层(例如,传输层110、160),并且AP命令传输层将命令回复消息转换为AP命令回复消息330。进一步,它将CPRB中的过滤错误代码(如果发现的话)转换成选定的AP回复代码,例如8B。传输层将回复代码放置在AP命令回复消息报头(例如,报头332)中的AP回复代码字段(例如,回复代码352)中并且将结果发送至访客。

[0075] 根据本发明的方面,在用于密码卡的AP命令回复消息的回复CPRB中的错误报告字段中定义错误代码(例如,无效无状态AP命令错误代码),以报告访客请求了管理程序施加的命令类型过滤指示符的集合不允许的AP命令。密码卡在AP命令回复消息的回复CPRB中的

错误报告字段中上报AP命令类型过滤错误代码。然而，CPRB中的密码代卡错误代码位于针对不同模式（例如，协处理器模式、EP11模式）的不同偏移处，并且其消息结构和格式不同。因此，提供独立于辅助处理器模式的用于返回AP错误代码（例如，AP回复代码）的中央位置，以便由管理程序以及访客容易地定位错误代码，而不管是谁产生的错误。结果，无效选择模式错误代码（例如，AP回复代码8B）被定义在AP命令回复消息报头的AP回复代码字段（例如，回复代码352）中以报告过滤的非无状态AP命令错误。AP回复代码是AP消息的公共错误报告字段，因为其有助于访客定位错误代码而不管谁生成错误（使用命令类型过滤模拟的管理程序、协处理器模式中的密码卡、XCP模式中的密码卡或加速器模式中的密码卡等）。然而，密码卡没有对AP回复代码字段的访问，并且因此，不将AP回复代码存储在AP命令回复消息报头中的AP回复代码中。AP命令回复消息的回复CPRB中的错误报告字段中存储的密码卡错误代码通常在AP架构的范围之外。因此，传输层被配置为在AP命令回复消息的回复CPRB中的错误报告字段中查找选择命令类型过滤模式错误代码，并且将CPRB中的错误代码转换成回复代码，例如，8B，并且将其放置在AP回复代码中。

[0076] 在AP命令回复消息的回复CPRB中的错误报告字段中具有无效选择模式命令错误代码对于调试目的是有用的，以确定AP回复代码是由密码卡还是由管理程序模拟生成，因为管理程序模拟不将无效选择模式命令错误代码存储在AP命令回复消息的回复CPRB中的错误报告字段中。

[0077] 本发明的一个或多个方面与计算机技术紧密联系并且促进计算环境内的处理（包括命令处理），从而改善其性能。参见图5A-5B描述与促进计算环境内的处理相关的一个实施例的进一步细节。

[0078] 参考图5A，在一个实施例中，确定计算环境的多个辅助处理器中的目标辅助处理器是否被配置为支持选定命令类型过滤模式（500），并且检查多个辅助处理器中的另一辅助处理器是否被配置为支持选定命令类型过滤模式（502）。

[0079] 基于确定目标辅助处理器未被配置为支持选定命令类型过滤模式，并且基于另一辅助处理器被配置为支持选定命令类型过滤模式，将命令转发到另一辅助处理器以供处理，以确定命令对于选定命令类型过滤模式是否有效（504）。基于在另一辅助处理器处的处理，获得关于命令对于选定命令类型过滤模式是否有效的指示（506）。

[0080] 基于获得命令对选定命令类型过滤模式有效的指示，将命令发送到目标辅助处理器以供执行（508）。

[0081] 在一个实施例中，基于获得命令对于选定命令类型过滤模式无效的指示，命令由于对于选定命令类型过滤模式无效被拒绝，并且制止在目标辅助处理器上执行该命令（510）。

[0082] 此外，在一个示例中，错误代码被放置在中央位置以促进对错误码的访问（512）。

[0083] 作为示例，选定命令类型过滤模式是无状态命令过滤模式（514），并且多个辅助处理器包括多个密码卡（516）。

[0084] 参考图5B，在一个实施例中，基于获得所述命令对选定命令类型过滤模式有效的指示，将所述命令作为选定命令类型过滤模式命令添加到命令列表（518）。命令列表将用于确定哪些命令对于在目标辅助处理器上执行是有效的（520）。进一步，在一个实施例中，基于获得命令对于选定命令类型过滤模式无效的指示，将命令作为有效辅助处理器命令添加

到命令列表(522)。

[0085] 在一个实施例中,基于确定多个辅助处理器未被配置为支持选定命令类型过滤模式,拒绝命令(524)。

[0086] 此外,在一个实施例中,基于确定目标辅助处理器未被配置为支持选定命令类型过滤模式,并且基于另一辅助处理器被配置为支持选定命令类型过滤模式,确定命令是否在命令列表上,命令列表用于确定命令是否将在目标辅助处理器上执行(526)。基于确定命令不在命令列表上,将命令转发到另一辅助处理器以供处理(528)。

[0087] 在一个实施例中,基于命令在另一辅助处理器上成功执行,将命令作为有效的选定命令类型过滤模式命令添加到命令列表(530)。此外,基于命令在另一辅助处理器上未成功执行,将命令作为有效辅助处理器命令添加到命令列表(532)。

[0088] 其他变型和实施例是可能的。

[0089] 本发明的一个或多个方面的命令类型过滤可结合在许多计算环境中并使用。参考图6A描述一个示例计算环境。作为示例,计算环境基于由纽约州阿蒙克的国际商业机器公司提供的z/Architecture®硬件架构。然而,z/Architecture硬件架构仅为一个示例架构。计算环境还可以基于其他架构,包括但不限于英特尔x86架构、国际商业机器公司的其他架构、和/或其他公司的架构。

[0090] 如图6A所示,计算环境600包括例如以通用计算设备的形式示出的计算机系统602。计算机系统602可以包括但不限于:经由一个或多个总线和/或其他连接610彼此耦合的一个或多个处理器或处理单元604(例如,中央处理单元(CPU))、存储器606(例如,系统存储器、主存储器、主存储、中央存储器或存储装置)、以及一个或多个输入/输出(I/O)接口608。

[0091] 总线610表示若干类型的总线结构中的任何一种或多种,包括存储器总线或存储器控制器、外围总线、加速图形端口、以及使用各种总线架构中的任一种的处理器或局部总线。作为示例而非限制,这样的体系结构包括工业标准体系结构(ISA)、微通道体系结构(MCA)、增强型ISA(EISA)、视频电子标准协会(VESA)局部总线和外围组件互连(PCI)。

[0092] 存储器606可包含(例如)高速缓存612,例如共享高速缓存,其可耦合到处理器604的本地高速缓存614。进一步,存储器606可包括一个或多个程序或应用616、至少一个操作系统618和一个或多个计算机可读程序指令620。计算机可读程序指令620可以被配置为执行本发明的方面的实施例的功能。

[0093] 在一个实施例中,存储器606(例如,存储器606的至少硬件系统区域)经由一个或多个辅助处理器总线623并且在一个或多个实施例中经由AP传输层耦合到一个或多个辅助处理器621。

[0094] 计算机系统602可以经由例如I/O接口608与一个或多个外部设备630、诸如用户终端、磁带驱动器、定点设备、显示器和一个或多个数据存储设备634等通信。数据存储设备634可以存储一个或多个程序636、一个或多个计算机可读程序指令638和/或数据等。该计算机可读程序指令可以被配置成用于执行本发明的多个方面的实施例的功能。

[0095] 计算机系统602还可以经由例如I/O接口608与网络接口632通信,网络接口632使计算机系统602能够与一个或多个网络通信,诸如局域网(LAN)、通用广域网(WAN)和/或公共网络(例如,互联网),提供与其他计算设备或系统的通信。

[0096] 计算机系统602可以包括和/或耦合到可移动/不可移动、易失性/非易失性计算机系统存储介质。例如,它可以包括和/或耦合到不可移动、非易失性磁介质(通常被称为“硬盘驱动器”)、用于从可移动、非易失性磁盘(例如,“软盘”)读取或向其写入的磁盘驱动器、和/或用于从可移动、非易失性光盘(如CD-ROM、DVD-ROM或其他光学介质)读取或向其写入的光盘驱动器。应当理解,其他硬件和/或软件组件可以与计算机系统602结合使用。示例包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器和数据归档存储系统等。

[0097] 计算机系统602可以与许多其他通用或专用计算系统环境或配置一起操作。适于与计算机系统602一起使用的众所周知的计算系统、环境和/或配置的示例包括但不限于个人计算机(PC)系统、服务器计算机系统、瘦客户机、厚客户机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机系统、大型计算机系统和包括以上系统或设备中的任一个的分布式云计算环境等。

[0098] 下面参照图6B描述结合和使用本发明的一个或多个方面的计算环境的另一个示例。作为示例,图6B的计算环境可基于由国际商业机器公司提供的z/Architecture®硬件架构。然而,z/Architecture硬件架构仅为一个示例架构。再次,计算环境还可以基于其他架构,包括但不限于英特尔x86架构、国际商业机器公司的其他架构、和/或其他公司的架构。

[0099] 在一个示例中,计算环境650包括中央电子复合体(CEC)652。CEC 652包括多个组件,例如,耦接到一个或多个处理器(又名,中央处理单元(CPU))656和输入/输出(I/O)子系统658的存储器654(又名,系统存储器、主存储器、主存储、中央存储、存储装置)。进一步,在一个实施例中,存储器654(例如,存储器654的至少硬件系统区域)经由一个或多个辅助处理器总线并且在一个或多个实施例中经由AP传输层耦合到一个或多个辅助处理器657。

[0100] I/O子系统658可以是中央电子复合体的一部分或与其分离。它引导主存储654与输入/输出控制单元660和连接到中央电子复合体的输入/输出(I/O)设备662之间的信息流。

[0101] 可以使用许多类型的I/O设备。一种特定类型是数据存储设备664。数据存储设备664可以存储一个或多个程序666、一个或多个计算机可读程序指令668、和/或数据等。该计算机可读程序指令可以被配置成用于执行本发明的多个方面的实施例的功能。

[0102] 中央电子复合体652可以包括和/或耦合到可移动/不可移动、易失性/非易失性计算机系统存储介质。例如,它可以包括和/或联接到不可移动、非易失性磁介质(通常被称为“硬盘驱动器”)、用于从可移动、非易失性磁盘(例如,“软盘”)读取和向其写入的磁盘驱动器、和/或用于从可移动、非易失性光盘(如CD-ROM、DVD-ROM或其他光介质)读取或向其写入的光盘驱动器上。应当理解,其他硬件和/或软件部件可以与中央电子复合体652结合使用。示例包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器和数据归档存储系统等。

[0103] 进一步,中央电子复合体652可以与许多其他通用或专用计算系统环境或配置一起操作。可以适用于中央电子复合体652的公知的计算系统、环境和/或配置的示例包括但不限于个人计算机(PC)系统、服务器计算机系统、瘦客户机、厚客户机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机系统、大型计算机系统和包括以上系统或设备中的任一个的分布式云计算环境等。

[0104] 在一个或多个实施例中,中央电子复合体652提供逻辑分区和/或虚拟化支持。在一个实施例中,如图6C所示,存储器654包括例如一个或多个逻辑分区670、管理逻辑分区的管理程序672和处理器固件674。管理程序672的一个示例是由纽约州阿蒙克的国际商业机器公司提供的处理器资源/系统管理器(PR/SM)。如本文所使用的,固件包括例如处理器的微代码。其包括例如在更高级机器代码的实现中使用的硬件级指令和/或数据结构。在一个实施例中,其包括例如通常作为微代码递送的专有代码,微代码包括可信软件或特定于底层硬件的微代码,并控制操作系统对系统硬件的访问。

[0105] 每个逻辑分区670能够用作单独的系统。即,每个逻辑分区可以独立地重置、运行访客操作系统676(诸如由纽约州阿蒙克的国际商业机器公司提供的z/OS®操作系统)或其他控制代码678(诸如耦合设施控制代码(CFCC))并且与不同的程序680一起操作。在逻辑分区中运行的操作系统或应用程序看起来可以访问完整和完全的系统,但实际上,只有其一部分是可用的。虽然提供z/OS作为示例,但是可以根据本发明的一个或多个方面使用其他操作系统。

[0106] 存储器654耦合到CPU 656(图6B),CPU 656是可以被分配给逻辑分区的物理处理器资源。例如,逻辑分区670包括一个或多个逻辑处理器,每个逻辑处理器表示可动态地分配给逻辑分区的物理处理器资源656的全部或共享。

[0107] 在又一实施例中,中央电子复合体提供虚拟机支持(有或者没有逻辑分区支持)。如图6D所示,中央电子复合体652的存储器654包括例如一个或多个虚拟机690、管理虚拟机的虚拟机管理器(诸如管理程序692)和处理器固件694。管理程序692的一个示例是由纽约州阿蒙克的国际商业机器公司提供的z/VM®管理程序。管理程序有时被称为主机。z/OS和z/VM是国际商业机器公司在至少一个管辖区域中的商标或注册商标。

[0108] CPC的虚拟机支持提供操作大量虚拟机690的能力,每个虚拟机能够与不同的程序696操作并运行访客操作系统698,例如Linux®操作系统。每个虚拟机690能够充当单独的系统。即,每个虚拟机可被独立地重置、运行访客操作系统、以及用不同程序来操作。在虚拟机中运行的操作系统或应用程序看起来能够访问完整和完全的系统,但实际上,只有其一部分是可用的。虽然提供z/VM和Linux作为示例,但是根据本发明的一个或多个方面可以使用其他虚拟机管理器和操作系统。注册商标Linux®是根据来自Linux基金会(Linus Torvalds)的专有被许可者,在全球基础上的标记的所有者)的子许可来使用的。

[0109] 参考图7A描述了结合和使用本发明的一个或多个方面的计算环境的另一个实施方式。在这个示例中,计算环境10包括例如经由例如一条或多条总线18和/或其他连接彼此耦合的本机中央处理单元(CPU)12、存储器14、以及一个或多个输入/输出设备和/或接口16。作为示例,计算环境10可以包括由纽约州阿蒙克的国际商业机器公司提供的PowerPC®处理器;由加利福尼亚州帕洛阿尔托的惠普公司提供的具有英特尔Itanium 11处理器的HP Superdome;和/或基于由国际商业机器公司、惠普公司、英特尔公司、甲骨文公司或其他公司提供的架构的其他机器。PowerPC是国际商业机器公司在至少一个管辖区域中的的商标或注册商标。Intel和Itanium是Intel公司或其子公司在美国和其他国家的商标或注册商标。

[0110] 本机中央处理单元12包括一个或多个本机寄存器20,诸如在环境内的处理期间使用的一个或多个通用寄存器和/或一个或多个专用寄存器。这些寄存器包括表示在任何特

定时间点的环境状态的信息。

[0111] 此外,本机中央处理单元12执行存储在存储器14中的指令和代码。在一个特定示例中,中央处理单元执行存储在存储器14中的仿真器代码22。该代码使得在一个架构中配置的计算环境能够仿真另一架构。例如,仿真器代码22允许基于除了z/Architecture硬件架构之外的架构的机器(诸如PowerPC处理器、HP Superdome服务器或其他)仿真z/Architecture硬件架构,并且执行基于z/Architecture硬件架构开发的软件和指令。

[0112] 参照图7B描述与模拟器代码22相关的进一步细节。存储在存储器14中的访客指令30包括经开发以在不同于本机CPU 12的架构的架构中执行的软件指令(例如,与机器指令相关)。例如,访客指令30可能已被设计成在基于z/Architecture硬件架构的处理器上执行,但取而代之的是在本机CPU 12上仿真,本机CPU 12可以是例如Intel Itanium 11处理器。在一个示例中,仿真器代码22包括指令提取例程32,以从存储器14获得一个或多个访客指令30,并且可选地提供对所获得的指令的本地缓冲。其还包含指令转换例程34,以确定已获得的访客指令的类型,且将访客指令转换为一或多个对应本机指令36。该转换包括,例如,识别要由访客指令执行的功能并选择执行该功能的本机指令。

[0113] 进一步,仿真器代码22包括仿真控制例程40以使本机指令被执行。仿真控制例程40可致使本机CPU 12执行仿真一个或多个先前获得的访客指令的本机指令的例程,且在此执行结束时,将控制返回到指令提取例程以仿真下一访客指令或一组访客指令的获得。本机指令36的执行可包含将数据从存储器14加载到寄存器中;将数据从寄存器存储回到存储器;或执行如由转换例程确定的某一类型的算术或逻辑操作。

[0114] 例如,每一例程以软件实施,所述软件存储在存储器中且由本机中央处理单元12执行。在其他示例中,例程或操作中的一个或多个以固件、硬件、软件或其某种组合来实现。可使用本机CPU的寄存器20或通过使用存储器14中的位置来仿真所仿真处理器的寄存器。在各实施例中,访客指令30、本机指令36和仿真器代码22可驻留在同一存储器中或可分布在不同存储器设备之间。

[0115] 进一步,在一个实施例中,计算环境10包括耦合到存储器14的一个或多个辅助处理器15。一个或多个辅助处理器在一个架构中被定义并且被配置为仿真另一架构。例如,辅助处理器获得被仿真的架构的访客命令,将访客命令转换为一个架构的本机命令并执行本机命令。

[0116] 上文所描述的计算环境仅为可使用的计算环境的示例。可以使用其他环境,包括但不限于非分区环境、分区环境、云环境和/或模拟环境;实施例不限于任何一个环境。尽管本文描述了计算环境的不同示例,但本发明的一个或多个方面可与许多类型的环境一起使用。本文提供的计算环境仅为示例。

[0117] 每个计算环境能够被配置成包括本发明的一个或多个方面。例如,根据本发明的一个或多个方面,每个可以被配置用于每一命令类型过滤。

[0118] 如本文中所描述,在一个或多个方面中,提供基于每一命令的命令类型过滤。可使用许多过滤技术,包含许多命令类型过滤技术。在一个特定示例中,提供无状态命令类型过滤。利用该过滤,在一个示例中,如果无状态命令过滤设施被设置为例如零,则不安装无状态命令过滤设施,并且辅助处理器(例如,密码卡)允许执行由辅助处理器支持的命令;否则,安装无状态命令过滤设施,并且辅助处理器是否执行命令至少取决于命令请求中的管

理程序施加的命令类型过滤指示符的集合的值。下面描述在命令请求消息中包括无状态命令类型指示符的示范性实施例：

[0119] 如果无状态命令类型指示符(例如,指示符322)在命令请求消息(例如,消息300)中被设置为零,则密码卡允许由该密码卡支持的所有命令被执行。如果无状态命令类型指示符(例如,指示符322)在命令请求消息(例如,消息300)中被设置为一,则密码卡不允许密码卡所支持的所有命令被执行。如果命令请求消息中的命令为无状态命令类型命令,则执行该命令。如果命令请求消息中的命令不是无状态命令类型命令,则在命令回复消息(例如,消息330)的CPRB(例如,回复CPRB 336)中以错误代码拒绝该命令。

[0120] 在一个或多个方面,密码卡的配置模式(例如,协处理器模式)可用于提供无状态命令过滤(也称为非安全密钥过滤模式;例如,仅处理无状态命令类型命令)或具有精简命令集的另一过滤模式,而不将密码卡配置为新的加密卡模式,例如,加速器模式。过滤技术可用于过滤命令集,诸如在其他示例中的无状态命令类型命令或其他命令类型命令,诸如主密钥管理命令等。这减少了要购买和管理的辅助处理器的数量。

[0121] 此外,本发明的一个或多个方面提供针对每一命令动态地切换命令类型过滤模式的能力;命令类型过滤是基于每一命令进行的。因此,每一命令在命令处理时间处可基于命令类型旗标值(例如,命令类型过滤指示符)而有效或无效。程序不必在各种加密卡模式之间切换以执行不同的过滤命令集。因此,管理和使用密码卡的数量复杂性保持相同,而不管所支持的过滤模式的数量如何。程序复杂性的降低还增加了更高效的代码并且提高了代码执行时间和性能。

[0122] 在另一方面中,使用来自支持选定命令类型过滤设施的辅助处理器(例如,较新版本)的信息来模拟目标辅助处理器(例如,较旧版本)不支持的过滤设施。

[0123] 在一个或一个以上方面中,管理程序基于访客的需要(例如,云环境客户的集合)确定AP命令类型过滤模式的集合、AP命令类型集合和AP命令类型标志。管理程序基于云环境来宾允许的AP命令集来设置AP命令集模式,并且通过拦截来宾发出的AP命令并采取适当动作来实施该操作模式。管理程序通过使用在客户配置中配置的加密卡上的相应硬件的AP命令集过滤模式设施,向其云环境客户提供AP命令集过滤模式支持。如果允许客户机例如仅执行AP命令的无状态子集,但是管理程序的配置中的加密卡都不支持无状态AP命令类型过滤(硬件)设施,则管理程序不允许客户机使用加密卡。然而,如果至少一个加密卡支持无状态命令过滤,则如果客户机在无状态AP命令模式下运行但无状态AP命令类型过滤(硬件)设施未安装在目标加密卡上,则管理程序自己模拟例如无状态AP命令类型过滤操作。

[0124] 管理程序模拟通过使用来自确实支持无状态AP命令类型过滤(硬件)设施(或其他过滤设施)的密码卡之一的信息来在不支持无状态AP命令类型过滤(硬件)设施的目标密码卡上模拟无状态AP命令类型过滤操作,来保证例如功能等效的硬件过滤操作。在一个实施例中,AP命令传输层(例如,i390C0)被增强以提供不管错误的发起者如何做出统一故障响应并且允许管理程序内的软件实现与加密卡一致的方式。

[0125] 在一个或多个方面中,可使用相同密码卡模式(例如,协处理器或EP11模式)来提供全AP命令集模式、无状态AP命令模式或具有减少的命令集的另一过滤模式,而不将密码卡配置在另一密码卡模式(例如,加速器模式)中。客户不需要购买用于加密卡过滤模式的附加卡。管理程序可通过例如将相同加密卡模式的不同加密域专用于具有不同AP命令类型

过滤要求的不同来服务具有不同AP命令类型过滤要求的不同客户。管理程序可以使用软件模拟和硬件过滤能力的组合来将非密码卡类型配置转换成对称密码卡类型配置以支持其来宾。使用使用公共接口的硬件和软件过滤的组合对于多个密码卡类型配置是有用的,其中一个或多个密码卡类型不提供任何硬件过滤设施或不提供所有所支持的硬件过滤设施(例如,非对称密码卡类型)。

[0126] 在一个方面,管理程序不需要为其支持用于模拟的每个加密卡类型维护每个过滤模式的AP命令的静态列表。针对管理程序支持的每个密码卡类型和模式维护每个过滤模式的AP命令的最新静态列表是繁重的并且不容易及时获得用于机器启动测试。因此,管理程序不能通过为其支持的每个加密卡类型维护每个过滤模式的AP命令的静态列表来保证软件AP命令类型过滤在功能上等同于硬件AP命令类型过滤。

[0127] 在一个方面,程序不必在各种加密卡模式之间切换以执行不同的过滤命令集。因此,管理和使用加密卡的复杂性保持相同,而不管所支持的过滤模式的数量如何。程序复杂性的这种降低还增加了更高效的代码并且提高了代码执行时间和性能。进一步,在一个方面中,管理程序不需要检查由客户程序提供的CPRB中的命令类型标志的正确设置。其基于客户机所允许的AP命令集,而非产生AP命令请求消息的客户机程序,在AP命令请求消息的CPRB中插入命令类型标志。结果,如果命令设置违反客户机所允许的命令类型过滤设置,则管理程序不需要设置(也不重置)CPRB中的命令类型标志或拒绝命令。

[0128] 在使用硬件和软件过滤技术两者的一个方面中,使用公共接口对于多个密码卡类型配置是有用的,其中一个或多个密码卡类型不提供任何硬件过滤设施或不提供所有所支持的硬件过滤设施(例如,非对称密码卡类型)。例如,如果管理程序配置由具有多个密码卡类型但不是所有密码卡类型的单个机器构成,以支持选定命令类型过滤设施(例如,无状态命令过滤设施),则管理程序可以在它自己在不支持选定命令类型过滤设施的密码卡类型上模拟选定命令类型过滤设施,以在所有可用的密码卡上提供相同的选定命令类型过滤设施。类似地,如果管理程序配置由具有不同模型的多个机器构成,并且客机可以被重新定位在那些机器模型中的任何一个上,但不是所有模型都支持,例如,选定命令类型过滤设施,则管理程序可以在其自己在不支持选定命令类型过滤设施的机器模型上模拟无状态命令过滤设施,以在所有可用的机器模型上提供相同的选定命令类型过滤设施。这允许管理程序使用软件和硬件能力的组合将非对称密码卡类型配置变成对称密码卡类型配置并且为其来宾提供命令类型过滤设施支持。该技术还可用于支持多个硬件过滤设施。其他变化也是可能的。

[0129] 此外,硬件过滤设施例如提供针对每一命令动态地切换过滤模式的能力;命令类型过滤是在每一命令的基础上完成的。因此,每一命令可基于命令类型旗标值在命令处理时间处有效或无效。因此,该技术允许管理程序与具有不同AP命令类型过滤要求的多个来宾共享相同的加密域。此外,程序不必在各种加密卡模式之间切换以执行不同的过滤命令集。因此,管理和使用密码卡的数量的复杂性保持相同,而不管所支持的过滤模式的数量如何。程序复杂性的这种降低还增加了更高效的代码并且提高了代码执行时间和性能。

[0130] 在一个或多个实施例中,管理程序可以是主机(如逻辑分区管理程序)、操作系统(如z/VM®)或设备驱动器。z/VM可使用同一加密卡来服务具有不同策略的多个客户机。在诸如Linux环境的某些环境中,可以使用密码设备驱动器来代替操作系统,以检索经处理的

AP消息。密码设备驱动器可以服务于多个用户,例如docker容器或具有不同策略的不同应用。管理器(诸如z/VM管理器)或加密设备驱动器可逐命令地从一个过滤模式(诸如一个命令类型过滤模式)切换到另一过滤模式。在一个示例中,如果至少一个客户机仅执行单个加密命令,则管理器或加密设备驱动器切换到下一个客户机,并且下一个客户机从不同过滤模式执行其加密命令。

[0131] 虽然本文描述了各种实施例,但是在不脱离本发明的方面的情况下,许多变化和其他实施例是可能的。应注意,除非另外不一致,否则本文所述的每个方面或特征及其变体可与任何其他方面或特征组合。

[0132] 一个或多个方面可涉及云计算。

[0133] 应当理解,虽然本公开包括关于云计算的详细描述,但是本文所引用的教导的实现不限于云计算环境。相反,本发明的实施例能够结合现在已知的或以后开发的任何其他类型的计算环境来实现。

[0134] 云计算是服务交付的模型,用于使得能够方便地、按需地网络访问可配置计算资源(例如,网络、网络带宽、服务器、处理、存储器、存储、应用、虚拟机和服务)的共享池,所述可配置计算资源可以以最小的管理努力或与所述服务的提供者的交互来快速供应和释放。该云模型可以包括至少五个特性、至少三个服务模型和至少四个部署模型。

[0135] 特性如下:

[0136] 按需自助服务:云消费者可以单方面地根据需要自动地提供计算能力,诸如服务器时间和网络存储,而不需要与服务的提供者的人类交互。

[0137] 广泛的网络接入:能力可通过网络获得并且通过标准机制接入,该标准机制促进异构瘦客户机平台或厚客户机平台(例如,移动电话、膝上型计算机和PDA)的使用。

[0138] 资源池:提供者的计算资源被池化以使用多租户模型来服务于多个消费者,其中不同的物理和虚拟资源根据需要动态地指派和重新指派。存在位置独立性的感觉,因为消费者通常不具有对所提供的资源的确切位置的控制或了解,但可能能够以较高抽象级别(例如,国家、州或数据中心)指定位置。

[0139] 快速弹性:能够快速和弹性地提供能力,在一些情况下自动地快速缩小和快速释放以快速放大。对于消费者而言,可用于供应的能力通常显得不受限制并且可以在任何时间以任何数量购买。

[0140] 测量的服务:云系统通过在适合于服务类型(例如,存储、处理、带宽和活动用户账户)的某个抽象级别处利用计量能力来自动控制和优化资源使用。可以监视、控制和报告资源使用,为所利用的服务的提供者和消费者提供透明度。

[0141] 服务模型如下:

[0142] 软件即服务(SaaS):提供给消费者的能力是使用在云基础设施上运行的提供者的应用。可通过诸如web浏览器(例如,基于web的电子邮件)之类的瘦客户端接口从不同客户端设备访问应用。消费者不管理或控制包括网络、服务器、操作系统、存储或甚至单独的应用能力的底层云基础设施,可能的例外是有限的用户特定应用配置设置。

[0143] 平台即服务(PaaS):提供给消费者的能力是将消费者创建的或获取的使用由提供商支持的编程语言和工具创建的应用部署到云基础设施上。消费者不管理或控制包括网络、服务器、操作系统或存储的底层云基础设施,但是对所部署的应用和可能的应用托管环

境配置具有控制。

[0144] 基础设施即服务(IaaS):提供给消费者的能力是提供处理、存储、网络 and 消费者能够部署和运行任意软件的其他基本计算资源,所述软件可以包括操作系统和应用。消费者不管理或控制底层云基础设施,而是具有对操作系统、存储、所部署的应用的控制以及对所选联网组件(例如,主机防火墙)的可能受限的控制。

[0145] 部署模型如下:

[0146] 私有云:云基础架构仅为组织运作。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0147] 社区云:云基础架构被若干组织共享并支持共享了关注(例如,任务、安全要求、策略、和合规性考虑)的特定社区。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0148] 公共云:使云基础架构对公众或大型行业组可用,并且由出售云服务的组织拥有。

[0149] 混合云:云基础架构是两个或更多个云(私有、社区或公共)的组合,这些云保持唯一实体但通过使数据和应用能够移植的标准化或专有技术(例如,云突发以用于云之间的负载平衡)绑定在一起。

[0150] 云计算环境是面向服务的,集中于无状态、低耦合、模块化和语义互操作性。云计算的核心是包括互连节点网络的基础设施。

[0151] 现在参见图8,描述了说明性云计算环境50。如图所示,云计算环境50包括云消费者使用的本地计算设备可以与其通信的一个或多个云计算节点52,本地计算设备诸如例如个人数字助理(PDA)或蜂窝电话54A、台式计算机54B、膝上型计算机54C和/或汽车计算机系统54N。节点52可彼此通信。它们可以物理地或虚拟地分组(未示出)在一个或多个网络中,诸如如上所述的私有云、社区云、公共云或混合云、或其组合。这允许云计算环境50提供基础设施、平台和/或软件作为云消费者不需要为其维护本地计算设备上的资源的服务。应当理解,图8中所示的计算设备54A-N的类型仅旨在是说明性的,并且计算节点52和云计算环境50可通过任何类型的网络和/或网络可寻址连接(例如,使用网络浏览器)与任何类型的计算机化设备通信。

[0152] 现在参见图9,示出了由云计算环境50(图8)提供的一组功能抽象层。提前应当理解,图9所示的组件、层和功能仅仅是说明性的,本发明的实施例不限于此。如所描述,提供以下层和对应功能:

[0153] 硬件和软件层60包括硬件和软件组件。硬件组件的示例包括:大型机61;基于RISC(精简指令集计算机)架构的服务器62;服务器63;刀片服务器64;存储设备65;以及网络和联网组件66。在一些实施例中,软件组件包括网络应用服务器软件67和数据库软件68。

[0154] 虚拟化层70提供抽象层,从该抽象层可以提供虚拟实体的以下示例:虚拟服务器71;虚拟存储72;虚拟网络73,包括虚拟专用网络;虚拟应用和操作系统74;以及虚拟客户端75。

[0155] 在一个示例中,管理层80可以提供以下描述的功能。资源供应81提供用于在云计算环境内执行任务的计算资源和其他资源的动态采购。计量和定价82在云计算环境内利用资源时提供成本跟踪,并为这些资源的消费开账单或发票。在一个示例中,这些资源可以包括应用软件许可证。安全性为云消费者和任务提供身份验证,以及为数据和其他资源提供

保护。用户门户83为消费者和系统管理员提供对云计算环境的访问。服务水平管理84提供云计算资源分配和管理,使得满足所需的服务水平。服务水平协议(sLA)规划和履行85提供根据SLA预期未来需求的云计算资源的预安排和采购。

[0156] 工作负载层90提供可以利用云计算环境的功能的示例。可以从该层提供的工作负荷和功能的示例包括:地图和导航91;软件开发和生命周期管理92;虚拟课堂教育交付93;数据分析处理94;事务处理95;以及命令类型过滤处理96。

[0157] 本发明的各个方面可以是任何可能的技术细节集成度的系统、方法和/或计算机程序产品。计算机程序产品可包括其上具有用于使处理器执行本发明的各方面的计算机可读程序指令的计算机可读存储介质(或多个介质)。

[0158] 计算机可读存储介质可为可保留和存储供指令执行装置使用的指令的有形装置。计算机可读存储介质可以是,例如但不限于,电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备、或者上述的任意合适的组合。计算机可读存储介质的更具体示例的非穷尽列表包括以下各项:便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式紧凑盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、诸如穿孔卡之类的机械编码设备或具有记录在其上的指令的槽中的凸出结构、以及上述各项的任何合适的组合。如本文所使用的计算机可读存储介质不应被解释为暂时性信号本身,例如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如,穿过光纤电缆的光脉冲)或通过电线发射的电信号。

[0159] 本文中所描述的计算机可读程序指令可以经由网络(例如,互联网、局域网、广域网和/或无线网络)从计算机可读存储介质下载到相应的计算/处理设备,或者下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输纤维、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配器卡或网络接口接收来自网络的可读程序指令,并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0160] 用于执行本发明的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据、或以一种或多种程序设计语言的任何组合编写的源代码或目标代码,这些程序设计语言包括面向对象的程序设计语言(诸如Smalltalk、C++等)和过程程序设计语言(诸如“C”程序设计语言或类似程序设计语言)。计算机可读程序指令可以完全地在用户计算机上执行、部分在用户计算机上执行、作为独立软件包执行、部分在用户计算机上部分在远程计算机上执行或者完全在远程计算机或服务器上执行。在后一种情况下,远程计算机可通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接至用户计算机,或者可连接至外部计算机(例如,使用互联网服务提供商通过互联网)。在一些实施例中,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来使电子电路个性化来执行计算机可读程序指令,以便执行本发明的各方面。

[0161] 这里参照根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述了本发明的各个方面。应当理解,流程图和/或框图的每个方框以及流程图和/

或框图中各方框的组合,都可以由计算机可读程序指令实现。

[0162] 这些计算机可读程序指令可被提供给计算机或其他可编程数据处理装置的处理器以产生机器,使得经由计算机或其他可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或框图的或多个框中指定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中,这些指令使得计算机、可编程数据处理装置、和/或其他设备以特定方式工作,从而,其中存储有指令的计算机可读存储介质包括包含实现流程图和/或框图中的或多个方框中规定的功能/动作的方面的指令的制造品。

[0163] 也可以把计算机可读程序指令加载到计算机、其他可编程数据处理装置、或其他设备上,使得在计算机、其他可编程装置或其他设备上执行一系列操作步骤,以产生计算机实现的处理,使得在计算机、其他可编程装置或其他设备上执行的指令实现流程图和/或框图中的或多个方框中规定的功能/动作。

[0164] 附图中的流程图和框图示出了根据本发明的不同实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。对此,流程图或框图中的每个框可表示指令的模块、段或部分,其包括用于实现指定的逻辑功能的一个或多个可执行指令。在一些备选实现中,框中标注的功能可以不按照图中标注的顺序发生。例如,连续示出的两个方框实际上可以作为一个步骤完成,同时、基本上同时、以部分或完全时间上重叠的方式执行,或者方框有时可以以相反的顺序执行,这取决于所涉及的功能。也要注意的,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作或执行专用硬件与计算机指令的组合的专用的基于硬件的系统来实现。

[0165] 除了上述之外,一个或多个方面可由提供客户环境的管理的服务提供商提供、提供、部署、管理、服务等。例如,服务提供商可为一个或多个客户创建、维护、支持等执行一个或多个方面的计算机代码和/或计算机基础设施。作为回报,作为示例,服务提供商可以根据订阅和/或费用协议从客户接收支付。另外或可替代地,服务提供商可以从向一个或多个第三方销售广告内容来接收支付。

[0166] 在一个方面,可以部署用于执行一个或多个实施例的应用。作为一个示例,应用的部署包括提供可操作以执行一个或多个实施例的计算机基础设施。

[0167] 作为又一方面,可以部署计算基础设施,包括将计算机可读代码集成到计算系统中,其中代码与计算系统组合能够执行一个或多个实施例。

[0168] 作为又一方面,可提供一种用于集成计算基础设施的过程,所述过程包括将计算机可读代码集成到计算机系统中。计算机系统包括计算机可读介质,其中计算机介质包括一个或多个实施例。代码与计算机系统组合能够执行一个或多个实施例。

[0169] 尽管以上描述了各种实施例,但这些实施例仅是示例。例如,其他架构的计算环境可以用于合并和使用一个或多个实施例。进一步,可以使用不同的指令、命令或操作。另外,可以指定不同类型的指示或标签,以及不同类型的过滤模式和/或辅助处理器。许多变化是可能的。

[0170] 本文描述了各个方面。此外,在不背离本发明的各方面的精神的情况下,许多变化是可能的。应注意,除非另外不一致,否则本文所述的每个方面或特征及其变体可与任何其他方面或特征组合。

[0171] 进一步,其他类型的计算环境可有益并被使用。作为示例,适合于存储和/或执行

程序代码的数据处理系统是可用的,其包括通过系统总线直接或间接地耦合到存储器元件的至少两个处理器。存储器元件包括例如在程序代码的实际执行期间使用的本地存储器、大容量存储器和高速缓冲存储器,该高速缓冲存储器提供至少一些程序代码的临时存储以便减少在执行期间必须从大容量存储器检索代码的次数。

[0172] 输入/输出或I/O设备(包括但不限于键盘、显示器、定点设备、DASD、磁带、CD、DVD、拇指驱动器和其他存储介质等)可以直接地或通过中间的I/O控制器耦合到系统。网络适配器也可以耦合到系统,以使得数据处理系统能够通过居间的私有或公共网络耦合到其他数据处理系统或远程打印机或存储设备。调制解调器、电缆调制解调器和以太网卡仅是一些可用类型的网络适配器。

[0173] 本文中使用的术语仅用于描述具体实施方式的目的,而并非旨在进行限制。如本文中使用的,除非上下文另有明确指示,否则单数形式“一”、“一个”和“该”旨在也包括复数形式。还应当理解,当在本说明书中使用术语“包括(comprises)”和/或“包含(comprising)”时,其指定所述特征、整体、步骤、操作、元件和/或部件的存在,但不排除一个或多个其他特征、整体、步骤、操作、元件、部件和/或其组合的存在或添加。

[0174] 以下权利要求中的所有装置或步骤加上功能元件的对应结构、材料、动作和等效物(如果有的话)旨在包括用于结合如具体要求保护的其他要求保护的元件来执行所述功能的任何结构、材料或动作。已经出于说明和描述的目的呈现了一个或多个实施例的描述,但并不旨在是详尽的或限于所公开的形式。对于本领域普通技术人员而言,许多修改和变化将是显而易见的。选择和描述实施例以便最好地解释各个方面和实际应用,并且使本领域的其他普通技术人员能够理解具有适合于预期的特定用途的不同修改的不同实施例。

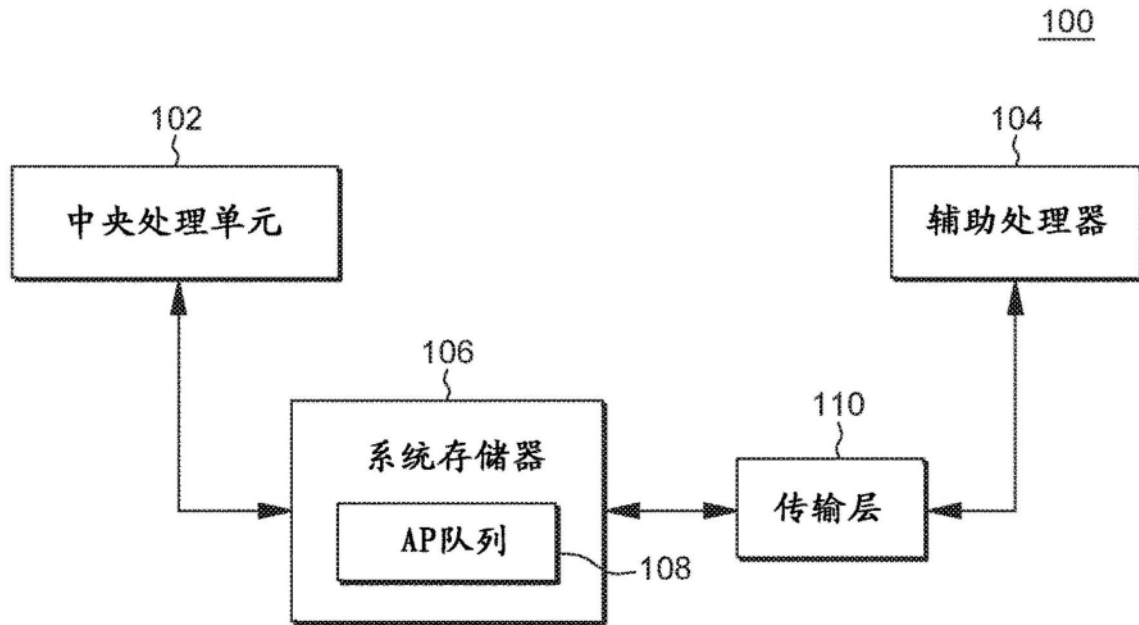


图1A

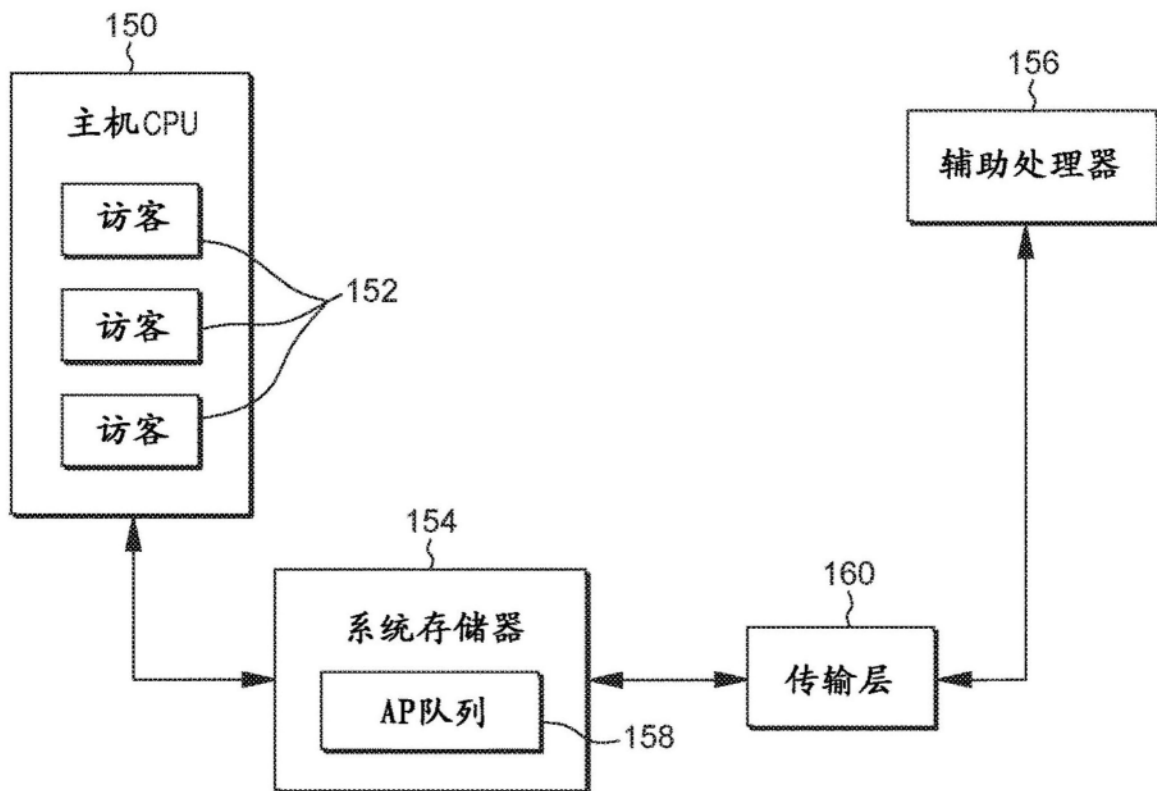


图1B

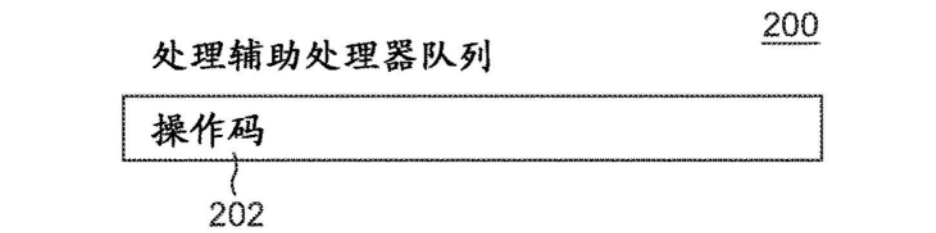


图2A

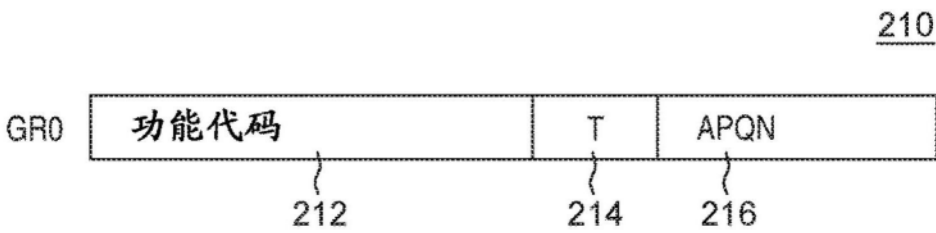


图2B

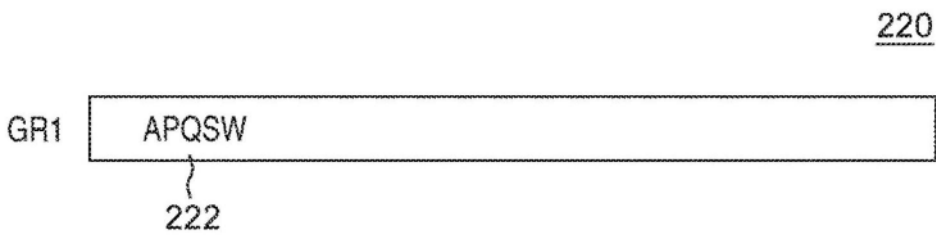


图2C

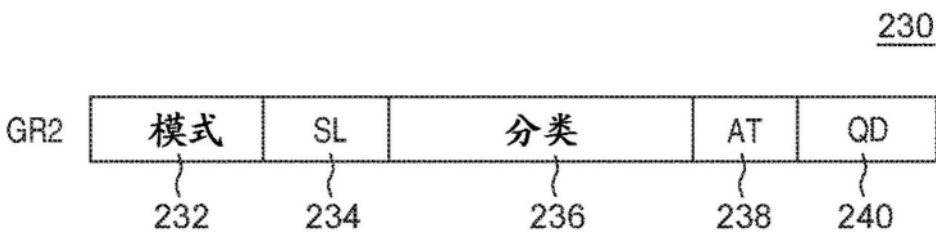


图2D



图3A

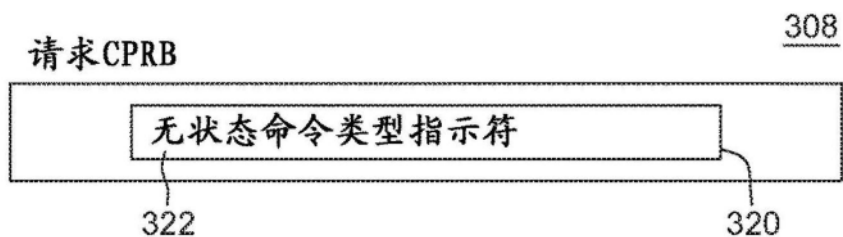


图3B



图3C

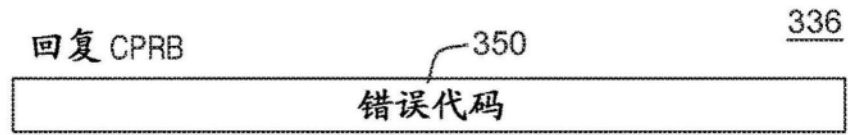


图3D

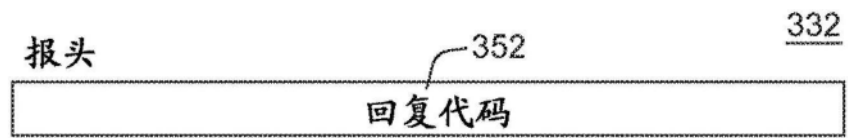


图3E

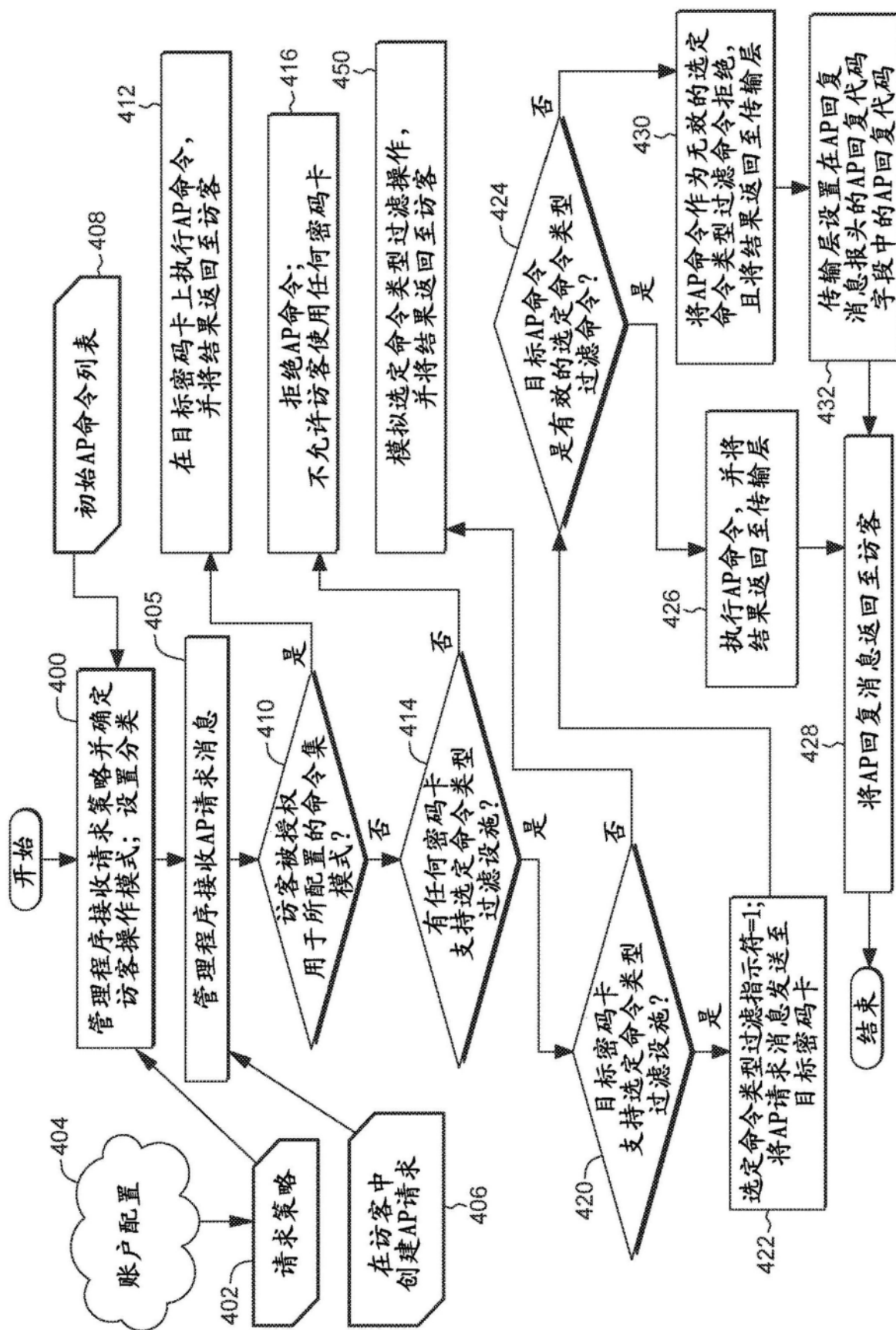


图4A

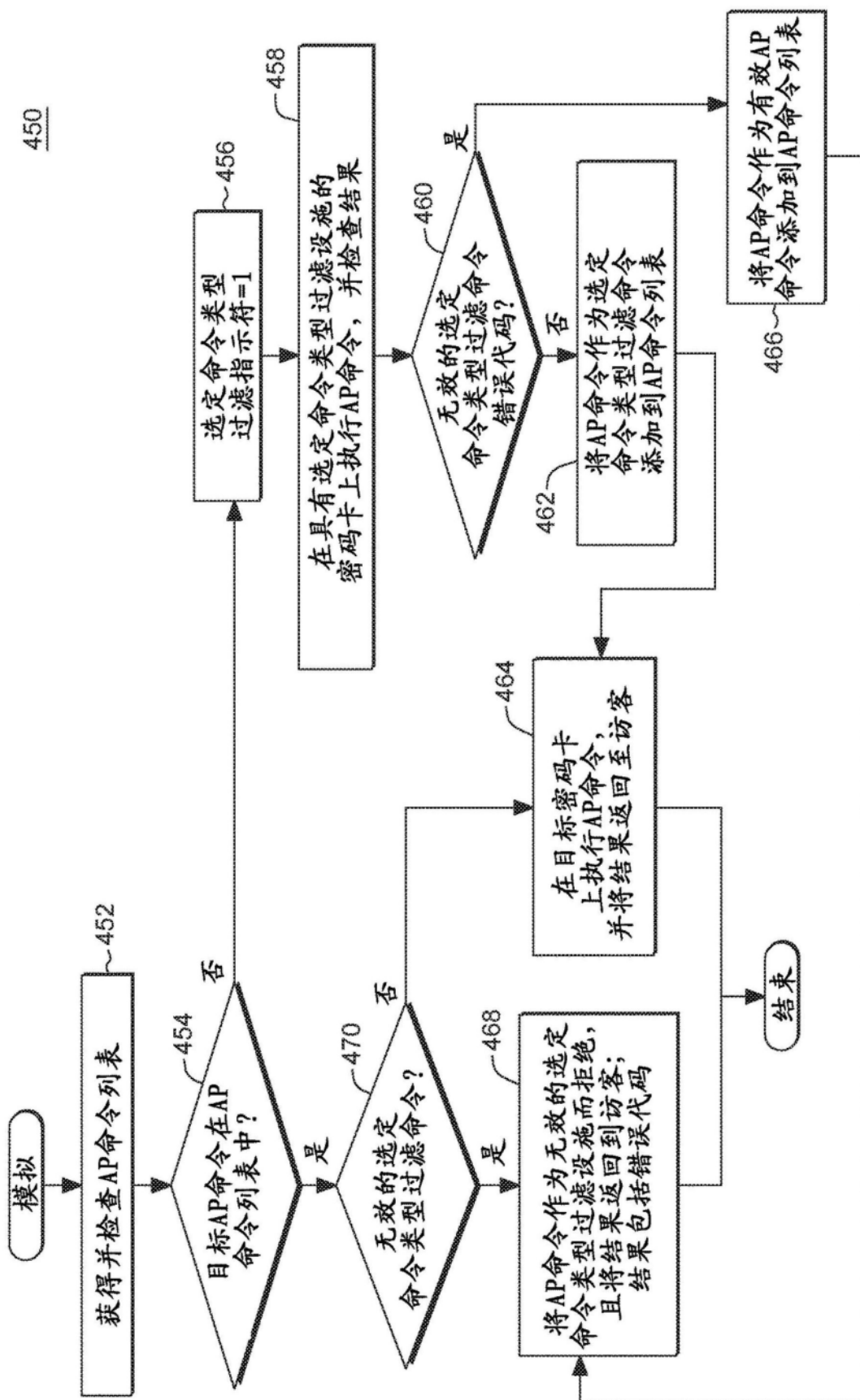


图4B

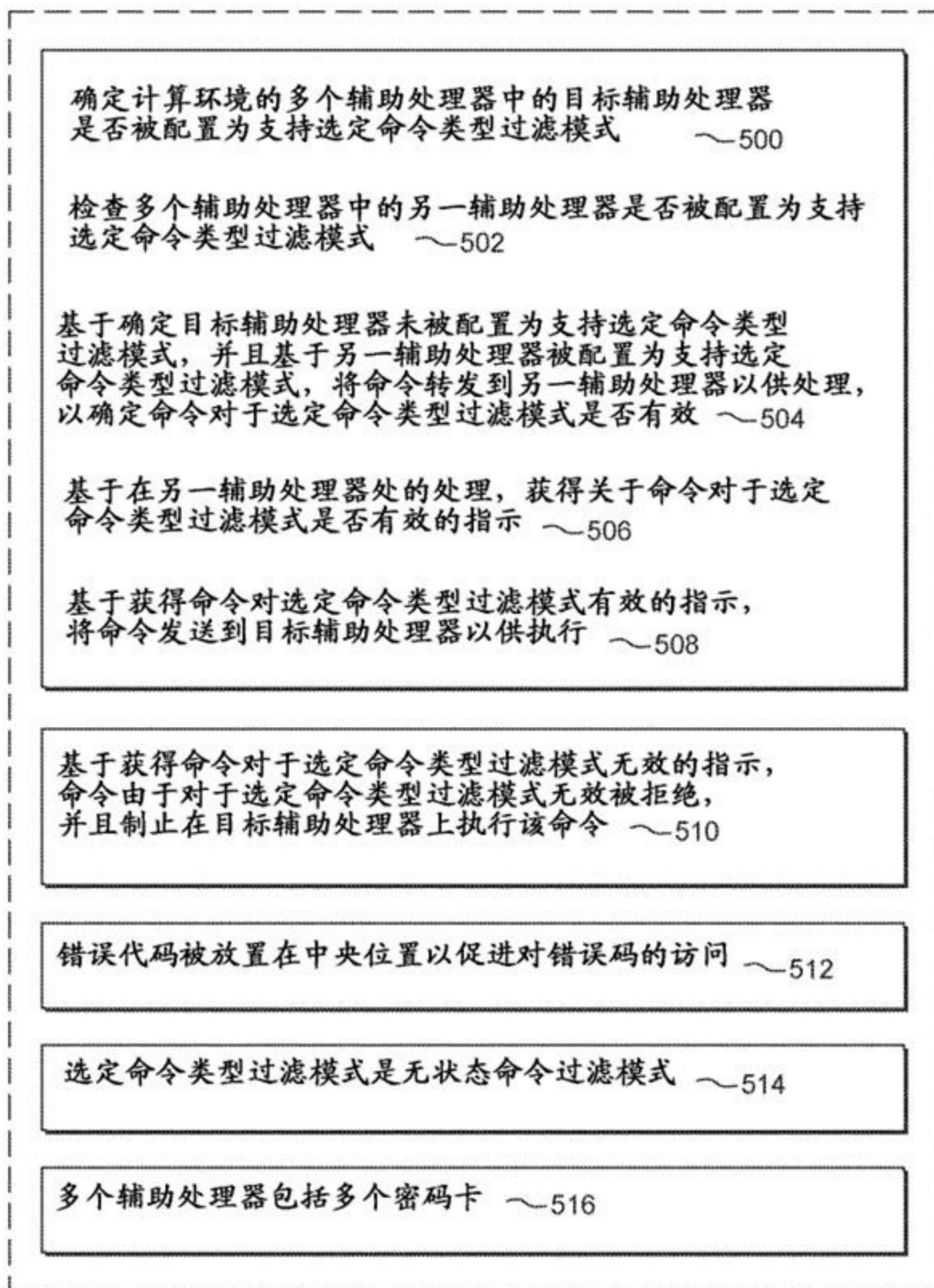


图5A

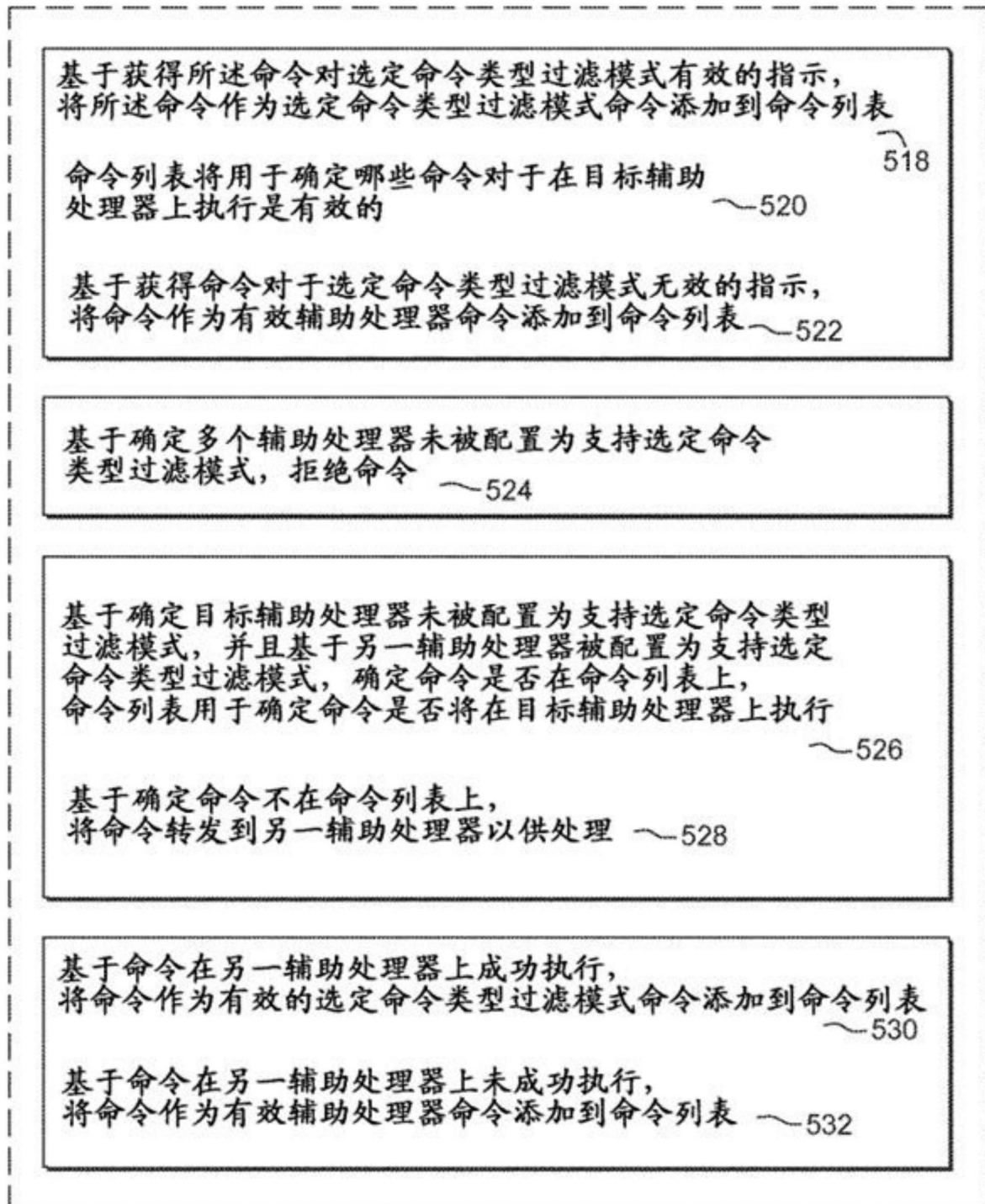


图5B

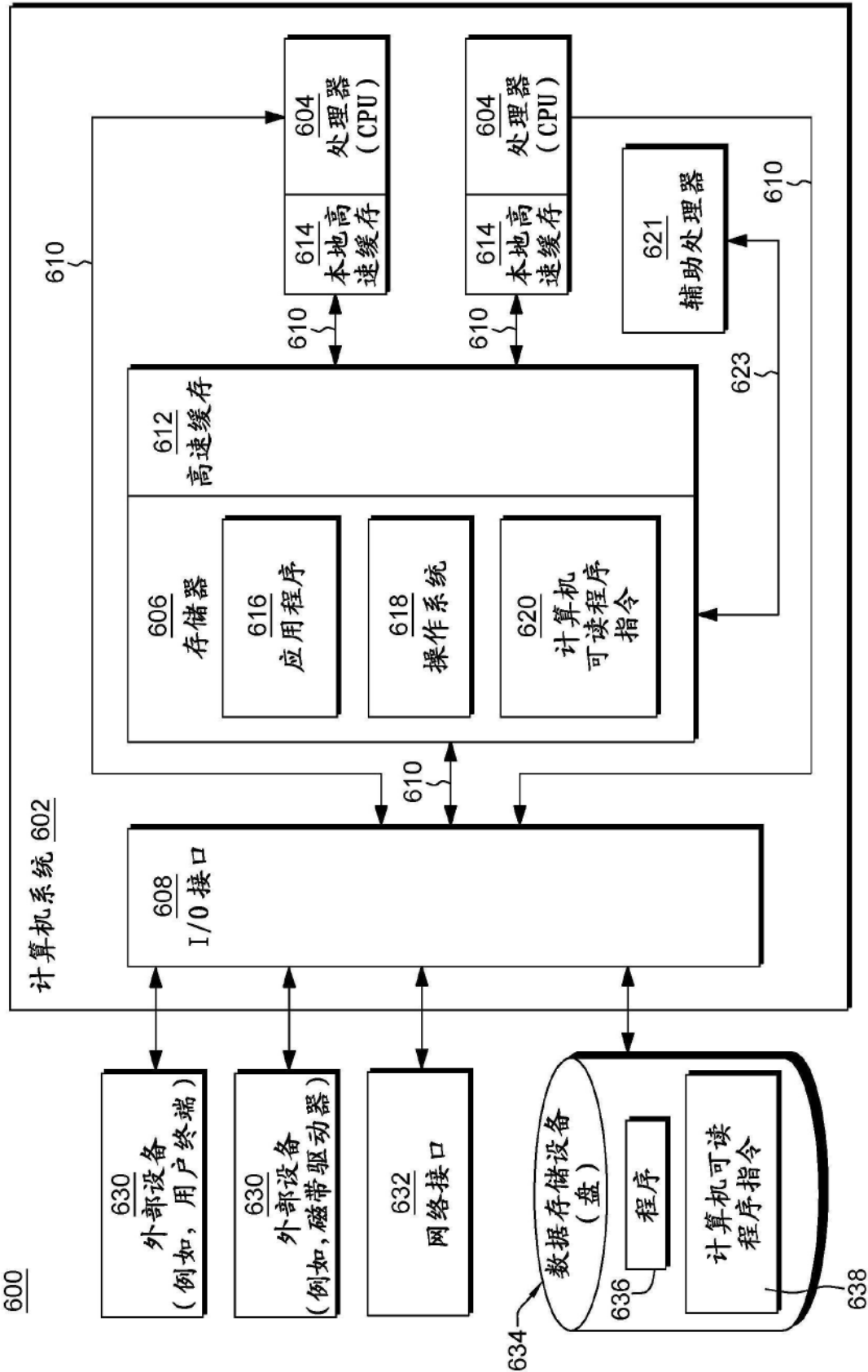


图6A

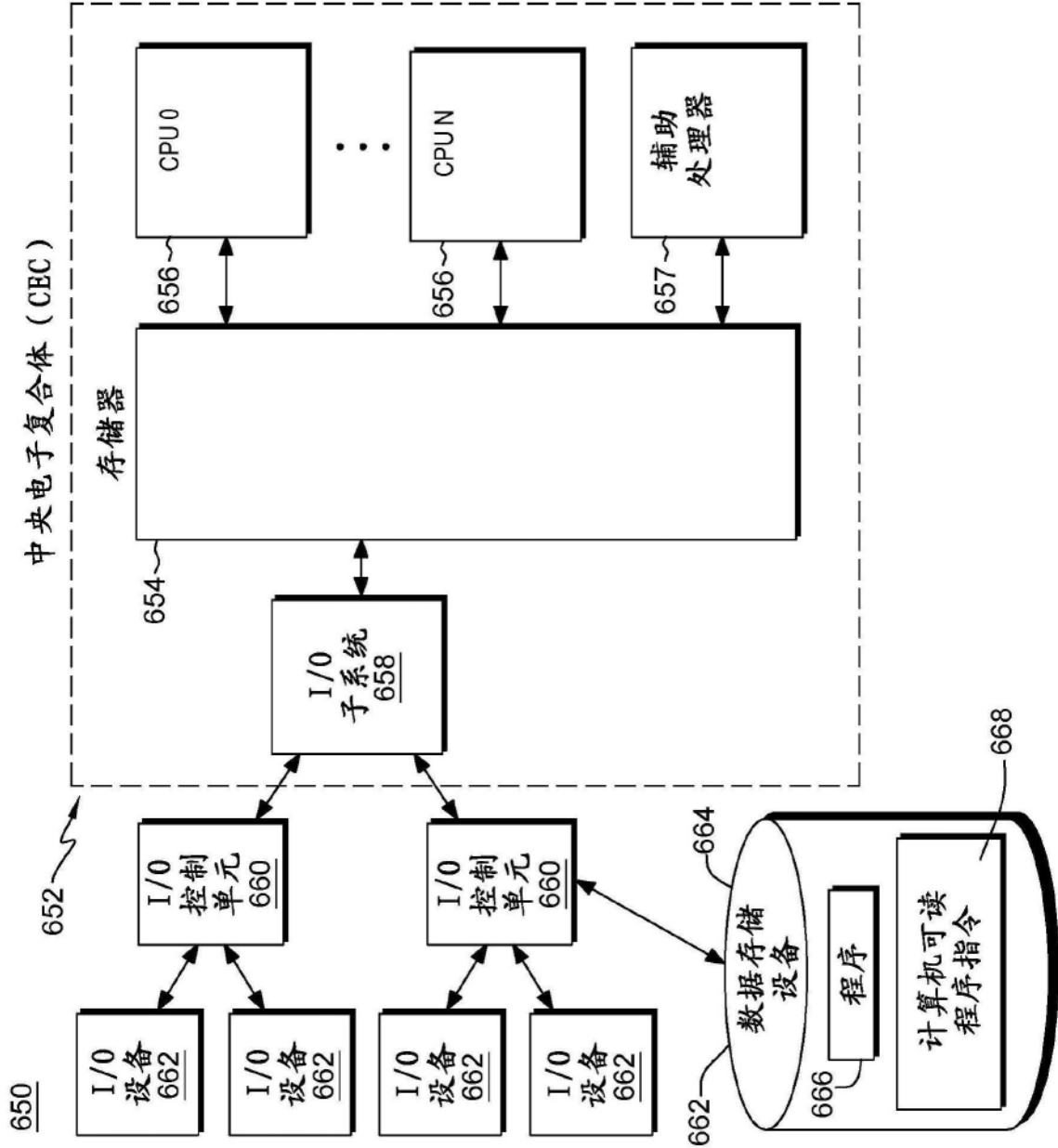


图6B

652

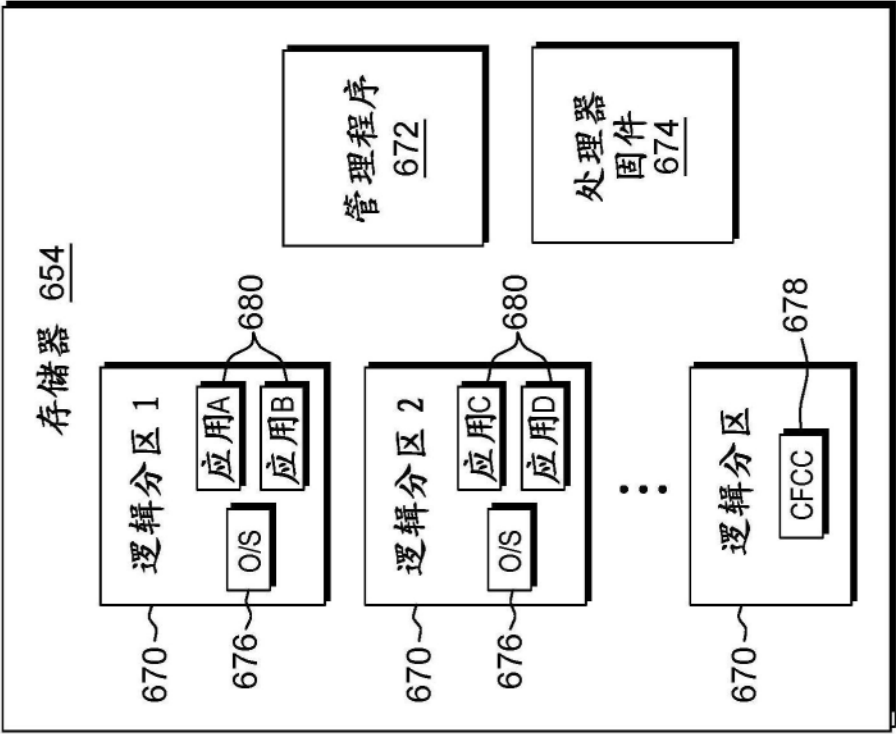


图6C

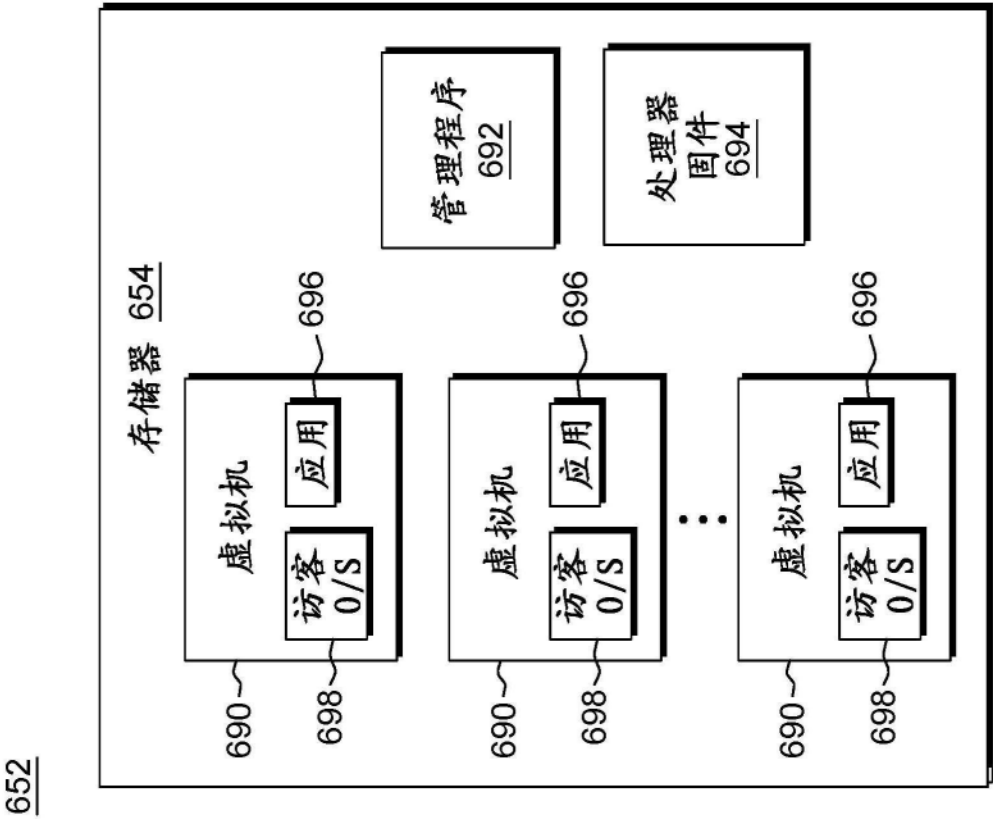


图6D

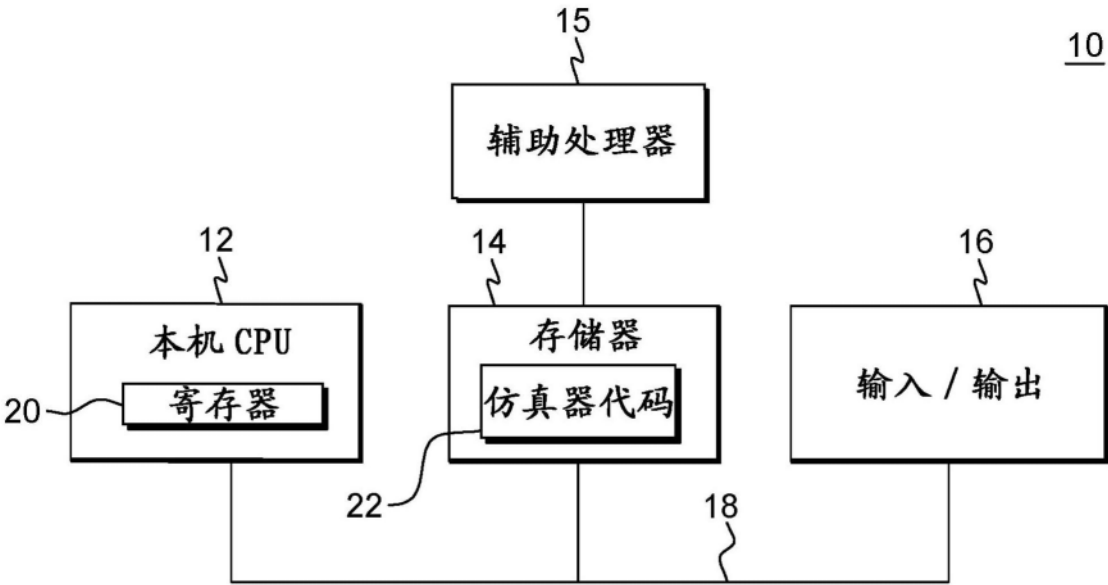


图7A

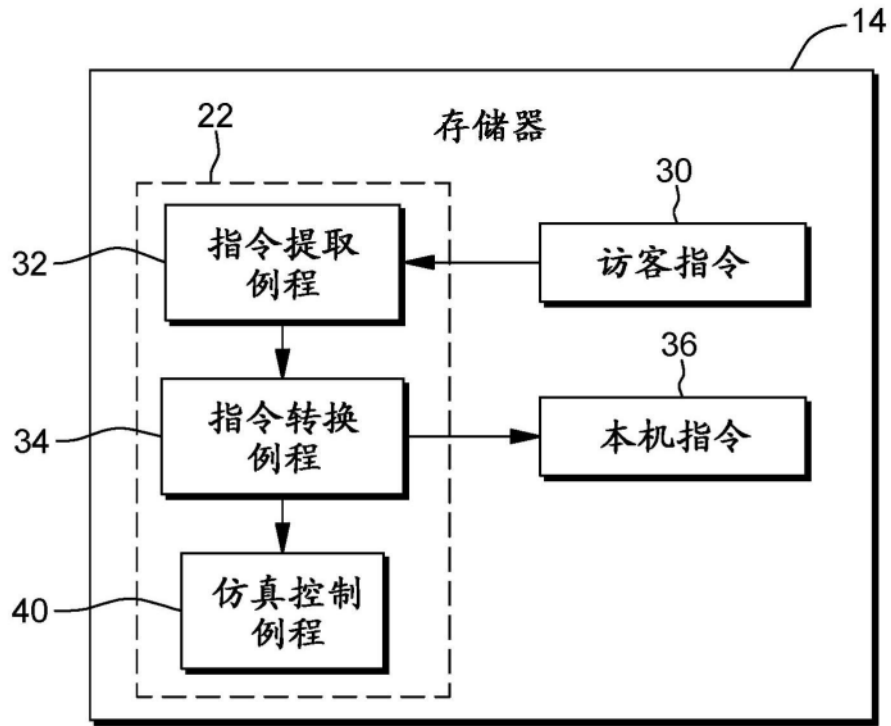


图7B

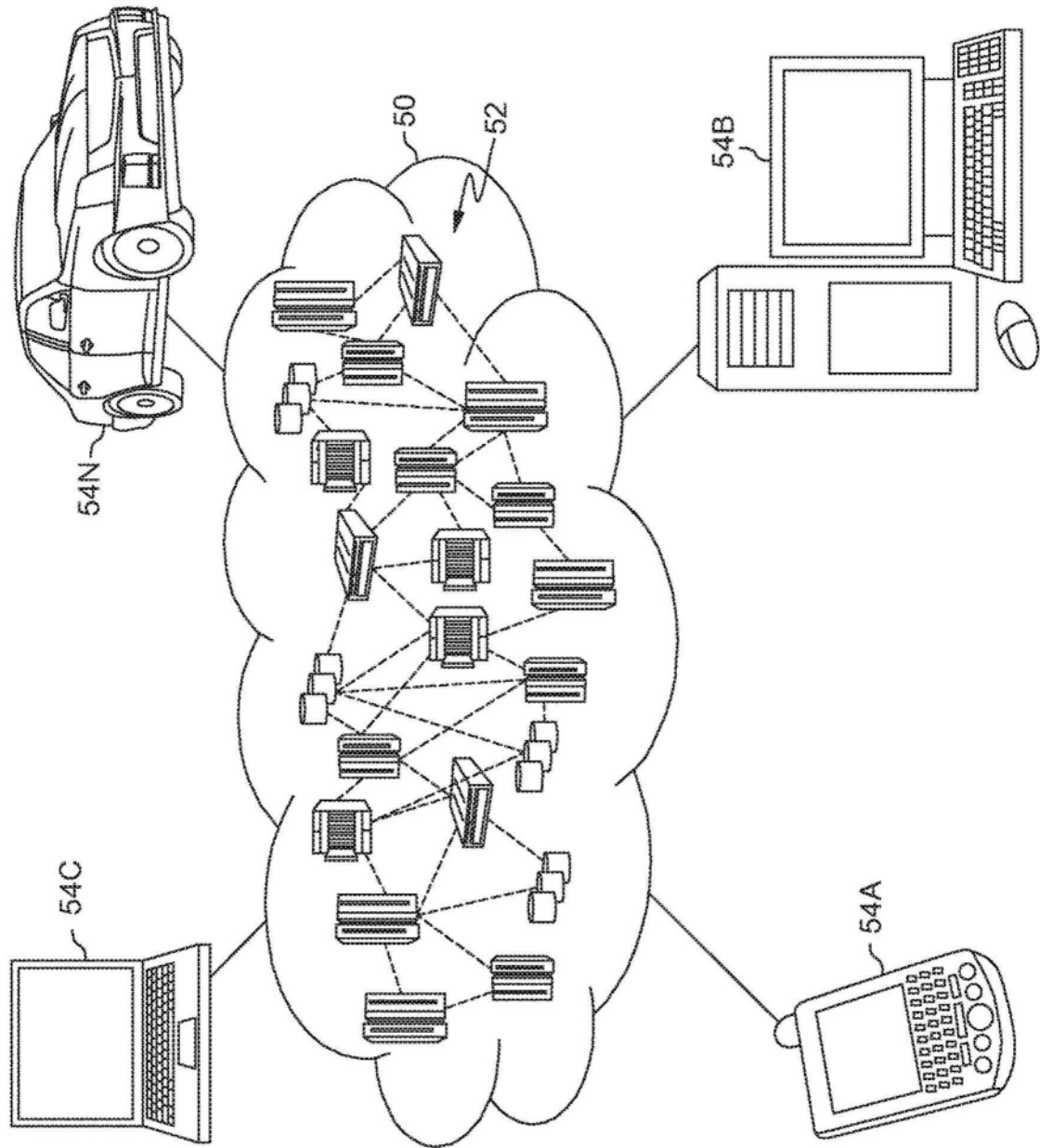


图8

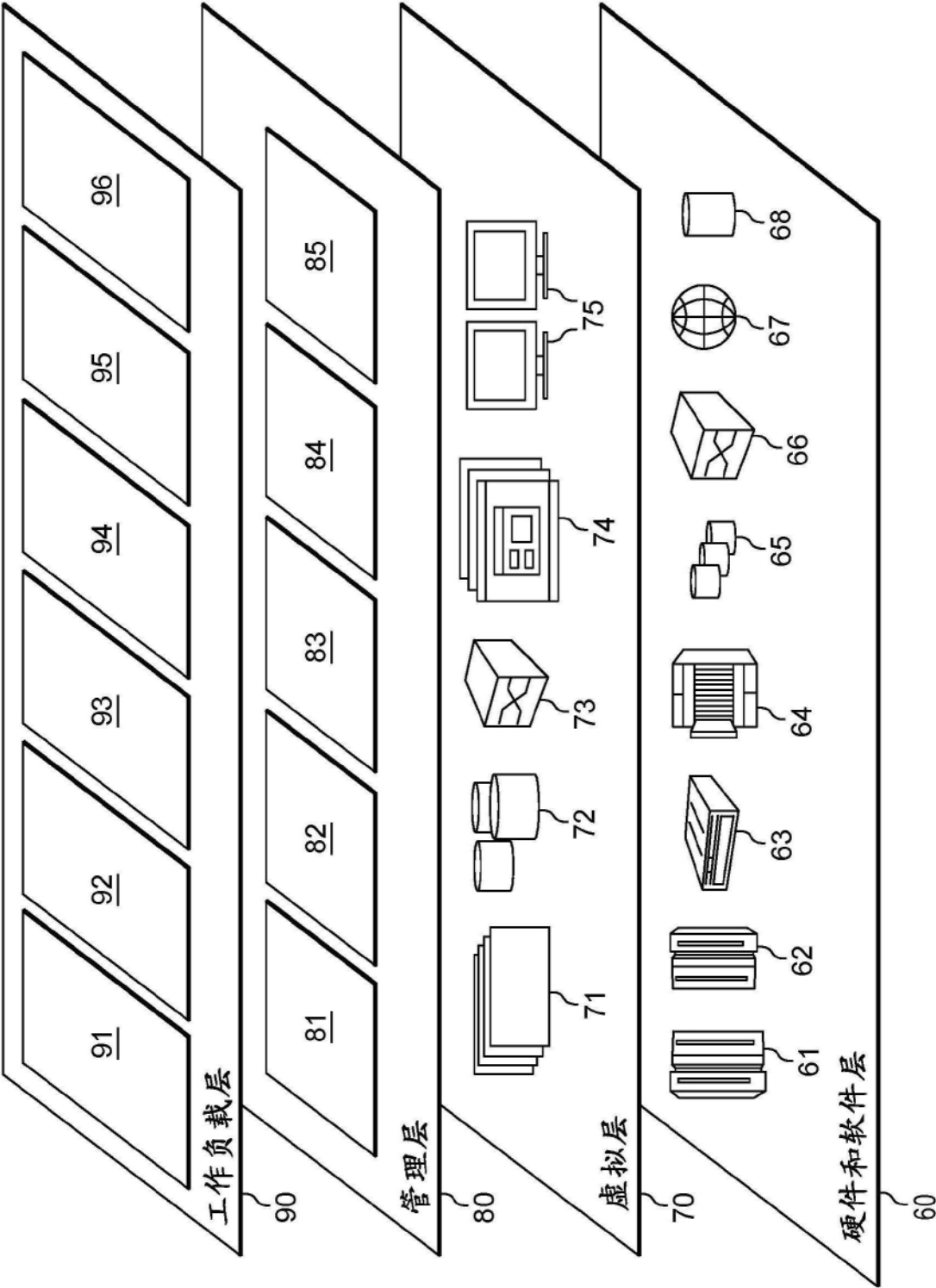


图9