(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116636191 A
(43)申请公布日 2023.08.22

(21)申请号 202180084756.7
(22)申请日 2021.12.17
(30)优先权数据
2020904728 2020.12.18 AU
(85)PCT国际申请进入国家阶段日
2023.06.15
(86)PCT国际申请的申请数据
PCT/AU2021/051515 2021.12.17
(87)PCT国际申请的公布数据
WO2022/126200 EN 2022.06.23
(71)申请人 达尔IP私人有限公司
地址 澳大利亚维多利亚州
(72)发明人 T·S·胡贝尔万阿森拉德
(74)专利代理机构 北京世峰知识产权代理有限公司 11713
专利代理师 卓霖 许向彤
(51)Int.Cl.
H04L 61/2567(2006.01)

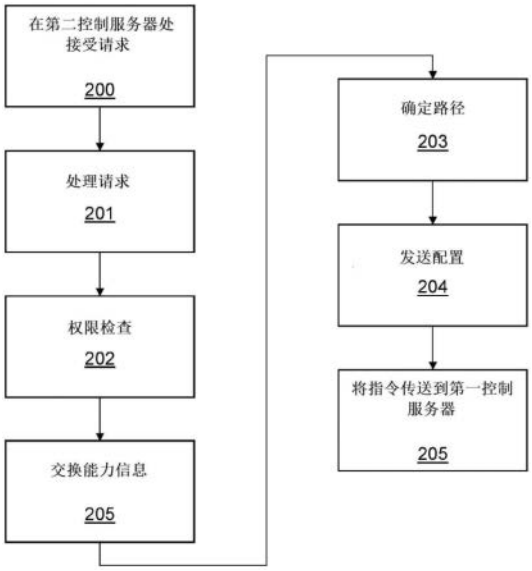
权利要求书5页 说明书16页 附图10页

(54)发明名称

用于在网络之间建立可信数据通信的方法

(57)摘要

一种用于在请求者和目标之间创建数据通信的方法，其中：请求者与第一群组和第一控制代理相关联；并且目标与第二群组和第二控制代理相关联，所述方法包括以：在第一控制代理处接收来自请求者的连接到目标的意图；识别第二控制代理并生成请求；将所述请求传送到第二控制代理；从第二控制代理接收外部配置指令；根据所接收的外部配置指令，选择一个或多个可配置的第一联网代理，以创建所述数据通信；至少部分地根据所接收的外部配置指令，为第一联网代理中的每一个确定第一联网配置指令；和将所述指令传送到所述第一联网代理，从而创建用于连接到由所述第二控制代理创建的第二节段的第一节段。



CN 116636191 A

1.一种用于在请求者和目标之间创建数据通信的方法,其中:所述请求者与第一群组和第一控制代理相关联;并且所述目标与第二群组和第二控制代理相关联,所述方法包括以下步骤:

在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图;

将所述第二控制代理标识为与所述目标相关联,并生成请求;

将所述请求从所述第一控制代理传送到所述第二控制代理;

从所述第二控制代理接收外部配置指令;

至少部分地根据所接收的外部配置指令,选择需要配置的所述第一群组的一个或多个可配置的第一联网代理,以便创建所述数据通信;

至少部分地根据所接收的外部配置指令,为一个或多个可配置的第一联网代理中的每一个第一联网代理确定第一联网配置指令;和

将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理,从而创建第一节段,所述第一节段用于连接到由所述第二控制代理创建的第二节段。

2.根据权利要求1所述的方法,其中,所述数据通信至少部分地通过诸如因特网的数据网络。

3.根据权利要求1所述的方法,其中,所述数据通信经由被所述请求者和所述目标共享的存储器。

4.根据权利要求1至3中任一项所述的方法,其中,所述请求包括适合于由所述第二控制代理处理的预定义数据结构。

5.根据权利要求1至4中任一项所述的方法,其中,所述请求者也是可配置的联网代理,并且被标识为是创建所述数据通信所需要的。

6.根据权利要求1至5中任一项所述的方法,其中,所述外部配置指定用于传出通信的IP地址和/或端口。

7.根据权利要求6所述的方法,其中,所述请求者是可配置的联网代理,并且被配置成将传出数据包寻址到所述IP地址和/或端口。

8.根据权利要求6所述的方法,其中,至少一个可配置的联网代理被配置成将传出数据包寻址到所述IP地址和/或端口。

9.根据权利要求1至8中任一项所述的方法,其中,至少一个可配置的联网代理包括安全协议,并且所述第一联网配置指令包含配置所述安全协议。

10.根据权利要求1至9中任一项所述的方法,其中,至少一个可配置的联网代理被配置成与汇聚点服务器通信,并且所述第一联网配置指令包含用于使能与所述汇聚点服务器的通信以便于建立所述数据通信的指令。

11.根据权利要求1至10中任一项所述的方法,其中,至少一个可配置的联网代理包括防火墙,并且所述第一联网配置指令包含用于配置所述防火墙以使来自所述目标的通信能够到达所述请求者的信息。

12.根据权利要求1至11中任一项所述的方法,其中,至少一个可配置的联网代理包括NAT,并且所述第一联网配置指令包含用于配置所述NAT以使来自所述目标的通信能够到达所述请求者的信息。

13.根据权利要求1至12中任一项所述的方法,其中,至少一个可配置的联网代理包括

用于记录在所述请求者和所述目标之间传输的数据的记录器，并且所述第一联网配置指令包含配置所述记录器的信息。

14.根据权利要求1到13中任一项所述的方法，进一步包括以下步骤：所述第一控制代理与所述第二控制代理交换能力信息。

15.根据权利要求14所述的方法，其中，至少部分地基于所交换的能力信息来选择所述一个或多个可配置的第一联网代理和/或确定所述第一联网配置指令。

16.根据权利要求1到15中任一项所述的方法，进一步包括以下步骤：检查与所述意图相关联的权限，并响应于确定所述权限不满足权限要求而停止所述数据通信的创建。

17.一种用于在请求者和目标之间创建数据通信的方法，其中：所述请求者与第一群组和第一控制代理相关联；并且所述目标与第二群组和第二控制代理相关联，所述方法包括以下步骤：

在所述第二控制代理处接收来自所述第一控制代理的请求，其中，所述请求用于创建所述数据通信；

确定需要配置的所述第二群组的一个或多个可配置的第二联网代理，以便创建所述数据通信；

为一个或多个可配置的第二联网代理中的每一个第二联网代理确定第二联网配置指令；

将所述第二联网指令传送到所述一个或多个可配置的第二联网代理，从而创建第二节段；

确定外部配置指令，所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段；和

将所述外部配置指令传送到所述第一控制代理。

18.根据权利要求17所述的方法，其中，所述数据通信至少部分地通过诸如因特网的数据网络。

19.根据权利要求17所述的方法，其中，所述数据通信经由由所述请求者和所述目标共享的存储器。

20.根据权利要求17至19中任一项所述的方法，其中，所述请求包括适合于由所述第二控制代理处理的预定义数据结构。

21.根据权利要求17至20中任一项所述的方法，其中，所述目标也是可配置的联网代理，并且被标识为是创建所述数据通信所需要的。

22.根据权利要求17至21中任一项所述的方法，其中，所述外部配置指定用于传出通信的IP地址和/或端口。

23.根据权利要求22所述的方法，其中，所述目标是可配置的联网代理，并且被配置成在特定IP地址和/或端口上接收传入数据包。

24.根据权利要求17至23中任一项所述的方法，其中，至少一个可配置的联网代理包括安全协议，并且所述第一联网配置指令包含配置所述安全协议。

25.根据权利要求17至24中任一项所述的方法，其中，至少一个可配置的联网代理被配置成与汇聚点服务器通信，并且所述第二联网配置指令包含用于使能与所述汇聚点服务器的通信以便于建立所述数据通信的指令。

26.根据权利要求17至25中任一项所述的方法，其中，至少一个可配置的联网代理包括防火墙，并且所述第二联网配置指令包含用于配置所述防火墙以使来自所述请求者的通信能够到达所述目标的信息。

27.根据权利要求17至26中任一项所述的方法，其中，至少一个可配置的联网代理包括NAT，并且所述第二联网配置指令包含用于配置所述NAT以使来自所述请求者的通信能够到达所述目标的信息。

28.根据权利要求17至27中任一项所述的方法，其中，至少一个可配置的联网代理包括用于记录在所述请求者和所述目标之间传输的数据的记录器，并且所述第一联网配置指令包含用于配置所述记录器的信息。

29.根据权利要求17至28中任一项所述的方法，其中，至少部分地基于所接收的请求来选择所述一个或多个可配置的第二联网代理和/或确定所述第二联网配置指令。

30.根据权利要求17到29中任一项所述的方法，进一步包括以下步骤：所述第二控制代理与所述第一控制代理交换能力信息。

31.根据权利要求30所述的方法，其中，至少部分地基于所交换的能力信息来选择所述一个或多个可配置的第二联网代理和/或确定所述第二联网配置指令。

32.根据权利要求17到31中任一项所述的方法，进一步包括以下步骤：检查与所述请求相关联的权限，并响应于确定所述权限不满足权限要求而停止所述数据通信的创建。

33.一种用于在请求者和目标之间创建数据通信的方法，其中：所述请求者与第一群组和第一控制代理相关联；并且所述目标与第二群组和第二控制代理相关联，所述方法包括以下步骤：

在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图；

由所述第一控制代理将所述第二控制代理标识为与所述目标相关联，并生成请求；

将来自所述第一控制代理的所述请求从所述第一控制代理传送到所述第二控制代理，其中，所述请求用于创建所述数据通信；

在所述第二控制代理处接收来自所述第一控制代理的所述请求，

由所述第二控制代理确定需要配置的所述第二群组的一个或多个可配置的第二联网代理，以便创建所述数据通信；

由所述第二控制代理为一个或多个可配置的第二联网代理中的每一个第二联网代理确定第二联网配置指令；

由所述第二控制代理将所述第二联网指令传送到所述一个或多个可配置的第二联网代理，从而创建第二节段；

由所述第二控制代理确定外部配置指令，所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段；和

将所述外部配置指令从所述第二控制代理传送到所述第一控制代理；

在所述第一控制代理处接收来自所述第二控制代理的所述外部配置指令；

由所述第一控制代理至少部分地根据所接收的外部配置指令来选择需要配置的所述第一群组的一个或多个可配置的第一联网代理，以便创建所述数据通信；

由所述第一控制代理至少部分地根据所接收的外部配置指令来为一个或多个可配置的第一联网代理中的每一个第一联网代理确定第一联网配置指令；和

将所述指令从所述第一控制代理传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理，从而创建第一节段，所述第一节段用于连接到由所述第二控制代理创建的第二节段。

34.根据权利要求32所述的方法，进一步包括以下步骤：

通过使用与所创建的第一节段和第二节段相对应的路径来在所述请求者和所述目标之间进行通信。

35.一种用于在请求者和目标之间创建数据通信的方法，其中：所述请求者与第一群组和第一控制代理相关联；并且所述目标与第二群组和第二控制代理相关联，所述方法包括以下步骤：

在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图；

将不同于所述第二控制代理的另外的控制代理标识为与所述目标相关联，并生成请求；

将所述请求从所述第一控制代理传送到所述另外的控制代理；

从所述另外的控制代理接收外部配置指令；

至少部分地根据所接收的外部配置指令，选择需要配置的所述第一群组的一个或多个可配置的第一联网代理，以便创建所述数据通信；

至少部分地根据所接收的外部配置指令，为一个或多个可配置的第一联网代理中的每一个第一联网代理确定第一联网配置指令；和

将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理，从而创建第一节段，所述第一节段用于连接到由所述第二控制代理创建的第二节段。

36.一种用于在请求者和目标之间创建数据通信的方法，其中：所述请求者与第一群组和第一控制代理相关联；并且所述目标与第二群组和第二控制代理相关联，所述方法包括以下步骤：

在所述第二控制代理处接收来自另外的控制代理的请求，其中，所述请求用于在所述目标和请求者之间创建所述数据通信，其中，所述另外的控制代理不同于所述第一控制代理；

确定需要配置的所述第二群组的一个或多个可配置的第二联网代理，以便创建所述数据通信；

为一个或多个可配置的第二联网代理中的每一个第二联网代理确定第二联网配置指令；

将所述第二联网指令传送到所述一个或多个可配置的第二联网代理，从而创建第二节段；

确定外部配置指令，所述外部配置指令被配置成使得所述另外的控制代理能够创建另外的节段以连接到所述第二节段；和

将所述外部配置指令传送到所述第一控制代理。

37.一种控制代理，所述控制代理被配置成实施根据权利要求1和17中任一项或两项所述的方法和/或根据权利要求35和36中任一项或两项所述的方法。

38.一种系统，包括：

第一控制代理，其定义包括至少一个第一计算机的第一群组；和

第二控制代理,其定义包括至少一个第二计算机的第二群组,

其中,所述第一控制代理和第二控制代理被配置成在彼此之间交换数据,

其中,所述第一控制代理被配置成:

从请求者接收连接到目标的意图,其中,所述请求者与所述第一群组的第一计算机相关联,并且所述目标与所述第二群组的第二计算机相关联;

将所述第二控制代理标识为与所述目标相关联,并生成请求;并且

将所述请求传送到所述第二控制代理,

其中,所述第二控制代理被配置成:

从所述第一控制代理接收所述请求;

确定需要配置的所述第二群组的一个或多个可配置的第二联网代理,以便创建所述数据通信;

为一个或多个可配置的第二联网代理中的每一个第二联网代理确定第二联网配置指令;

将所述第二联网指令传送到所述一个或多个可配置的第二联网代理,从而创建第二节段;确定外部配置指令,所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段;并且

将所述外部配置指令传送到所述第一控制代理,

并且其中,所述第一控制代理被进一步配置成:

接收所述外部配置指令;

至少部分地根据所接收的外部配置指令,选择需要配置的所述第一群组的一个或多个可配置的第一联网代理,以便创建所述数据通信;

至少部分地根据所接收的外部配置指令,为一个或多个可配置的第一联网代理中的每一个第一联网代理确定第一联网配置指令;并且

将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理,从而创建用于连接到所述第二节段的第一节段,从而创建路径。

39.根据权利要求38所述的系统,进一步包括所述一个或多个第一联网代理和所述一个或多个第二联网代理。

40.根据权利要求37或权利要求38所述的系统,其中,所述请求者和所述目标是在其相应计算机上运行的应用,并且其中,所述请求者和目标被配置成根据所创建的路径进行数据通信。

41.一种包括代码的计算机程序,所述代码被配置成当所述代码被计算机执行时,使所述计算机实施根据权利要求1至36中任一项所述的方法。

42.一种计算机可读存储介质,包括根据权利要求41所述的计算机程序。

用于在网络之间建立可信数据通信的方法

技术领域

[0001] 本发明总体上涉及用于经由网络的数据通信、例如可配置的网络通信的方法和系统。

背景技术

[0002] 网络隧道是已知的，其中，两个专用网络可以经由公共网络虚拟连接。然而，这种隧道方法通常缺乏灵活性和通用性。这限制了延迟、吞吐量、可靠性、覆盖范围和潜在的新能力。此外，目前的隧道技术通常需要集中式控制器来限制数据包，其中防火墙只允许经授权的通信。这可能导致性能(例如，延迟)方面的限制，并可能产生中心故障点。

发明内容

[0003] 根据本发明的一个方面，提供了一种用于在请求者和目标之间创建数据通信的方法，其中：所述请求者与第一群组和第一控制代理相关联；并且所述目标与第二群组和第二控制代理相关联，所述方法包括以下步骤：在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图；将所述第二控制代理标识为与所述目标相关联，并生成请求；将所述请求从所述第一控制代理传送到所述第二控制代理；从所述第二控制代理接收外部配置指令；至少部分地根据所接收的外部配置指令，选择需要配置的所述第一群组的一个或多个可配置的第一联网代理，以便创建所述数据通信；至少部分地根据所接收的外部配置指令，为一个或多个可配置的第一联网代理中的每一个确定第一联网配置指令；和，将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理，从而创建用于连接到由所述第二控制代理创建的第二节段的第一节段。

[0004] 在一个实施例中，所述数据通信至少部分地在诸如因特网的数据网络上进行。在另一个实施例中，所述数据通信经由由所述请求者和所述目标共享的存储器。

[0005] 通常，所述请求包括适合于由所述第二控制代理处理的预定义数据结构。

[0006] 所述请求者也可以是可配置的联网代理，并且被标识为是创建所述数据通信所需要的。

[0007] 在一个实施例中，所述外部配置指定用于传出通信的IP地址和/或端口。所述请求者可以是可配置的联网代理，并且可以被配置成将传出数据包寻址到所述IP地址和/或端口。至少一个可配置的联网代理可以被配置成将传出数据包寻址到所述IP地址和/或端口。

[0008] 至少一个可配置的联网代理可以包括安全协议，并且所述第一联网配置指令可以包含配置所述安全协议。

[0009] 至少一个可配置的联网代理可以被配置成与汇聚点服务器通信，并且所述第一联网配置指令可以包含用于使能与所述汇聚点服务器的通信以便于建立所述数据通信的指令。

[0010] 至少一个可配置的联网代理可以包括防火墙，并且所述第一联网配置指令可以包含用于配置所述防火墙以使来自所述目标的通信能够到达所述请求者的信息。

[0011] 至少一个可配置的联网代理可以包括NAT,并且所述第一联网配置指令可以包含用于配置所述NAT以使来自所述目标的通信能够到达所述请求者的信息。

[0012] 至少一个可配置的联网代理可以包括用于记录在所述请求者和所述目标之间传输的数据的记录器,并且所述第一联网配置指令可以包含用于配置所述记录器的信息。

[0013] 所述方法可以进一步包括以下步骤:所述第一控制代理与所述第二控制代理交换能力信息。选择所述一个或多个可配置的第一联网代理和/或确定所述第一联网配置指令可以至少部分地基于所交换的能力信息。

[0014] 所述方法可以进一步包括以下步骤:检查与所述意图相关联的权限,并响应于确定所述权限不满足权限要求而停止所述数据通信的创建。

[0015] 根据本发明的另一个方面,提供了一种用于在请求者和目标之间创建数据通信的方法,其中:所述请求者与第一群组和第一控制代理相关联;并且所述目标与第二群组和第二控制代理相关联,所述方法包括以下步骤:在所述第二控制代理处接收来自所述第一控制代理的请求,其中,所述请求用于创建所述数据通信;确定需要配置的所述第二群组的一个或多个可配置的第二联网代理,以便创建所述数据通信;为一个或多个可配置的第二联网代理中的每一个确定第二联网配置指令;将所述第二联网指令传送到所述一个或多个可配置的第二联网代理,从而创建第二节段;确定外部配置指令,所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段;和,将所述外部配置指令传送到所述第一控制代理。

[0016] 在一个实施例中,所述数据通信至少部分地通过诸如因特网的数据网络。在另一个实施例中,所述数据通信经由被所述请求者和所述目标共享的存储器。

[0017] 所述请求可以包括适合于由所述第二控制代理处理的预定义数据结构。

[0018] 所述目标也可以是可配置的联网代理,并且被标识为是创建所述数据通信所需要的。

[0019] 所述外部配置可以指定用于传出通信的IP地址和/或端口。

[0020] 所述目标可以是可配置的联网代理,并且被配置成在特定IP地址和/或端口上接收传入数据包。

[0021] 至少一个可配置的联网代理可以包括安全协议,并且所述第一联网配置指令可以包含配置所述安全协议。

[0022] 至少一个可配置的联网代理可以被配置成与汇聚点服务器通信,并且所述第二联网配置指令可以包含用于使能与所述汇聚点服务器的通信以便于建立所述数据通信的指令。

[0023] 至少一个可配置的联网代理可以包括防火墙,并且所述第二联网配置指令可以包含用于配置所述防火墙以使来自所述请求者的通信能够到达所述目标的信息。

[0024] 至少一个可配置的联网代理可以包括NAT,并且所述第二联网配置指令可以包含用于配置所述NAT以使来自所述请求者的通信能够到达所述目标的信息。

[0025] 至少一个可配置的联网代理可以包括用于记录在所述请求者和所述目标之间传输的数据的记录器,并且所述第一联网配置指令可以包含用于配置所述记录器的信息。

[0026] 选择所述一个或多个可配置的第二联网代理和/或确定所述第二联网配置指令可以至少部分地基于所接收的请求。

[0027] 所述方法可以进一步包括以下步骤:所述第二控制代理与所述第一控制代理交换能力信息。

[0028] 选择所述一个或多个可配置的第二联网代理和/或确定所述第二联网配置指令可以至少部分地基于所交换的能力信息。

[0029] 所述方法可以进一步包括以下步骤:检查与所述请求相关联的权限,并响应于确定所述权限不满足权限要求而停止所述数据通信的创建。

[0030] 根据本发明的另一个方面,提供了一种用于在请求者和目标之间创建数据通信的方法,其中:所述请求者与第一群组和第一控制代理相关联;并且所述目标与第二群组和第二控制代理相关联,所述方法包括以下步骤:在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图;由所述第一控制代理将所述第二控制代理标识为与所述目标相关联,并生成请求;将来自所述第一控制代理的所述请求从所述第一控制代理传送到所述第二控制代理,其中,所述请求用于创建所述数据通信;在所述第二控制代理处接收来自所述第一控制代理的所述请求,由所述第二控制代理确定需要配置的所述第二群组的一个或多个可配置的第二联网代理,以便创建所述数据通信;由所述第二控制代理为一个或多个可配置的第二联网代理中的每一个确定第二联网配置指令;由所述第二控制代理将所述第二联网指令传送到所述一个或多个可配置的第二联网代理,从而创建第二节段;由所述第二控制代理确定外部配置指令,所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段;和将所述外部配置指令从所述第二控制代理传送到所述第一控制代理;在所述第一控制代理处从所述第二控制代理接收所述外部配置指令;由所述第一控制代理至少部分地根据所接收的外部配置指令来选择需要配置的所述第一群组的一个或多个可配置的第一联网代理,以便创建所述数据通信;由所述第一控制代理至少部分地根据所接收的外部配置指令来为一个或多个可配置的第一联网代理中的每一个确定第一联网配置指令;和将所述指令从所述第一控制代理传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理,从而创建用于连接到由所述第二控制代理创建的第二节段的第一节段。

[0031] 所述方法可以进一步包括以下步骤:通过使用与所创建的第一节段和第二节段相对应的路径来在所述请求者和所述目标之间进行通信。

[0032] 根据本发明的另一个方面,提供了一种用于在请求者和目标之间创建数据通信的方法,其中:所述请求者与第一群组和第一控制代理相关联;并且所述目标与第二群组和第二控制代理相关联,所述方法包括以下步骤:在所述第一控制代理处接收来自所述请求者的连接到所述目标的意图;将不同于所述第二控制代理的另外的控制代理标识为与所述目标相关联,并生成请求;将所述请求从所述第一控制代理传送到所述另外的控制代理;从所述另外的控制代理接收外部配置指令;至少部分地根据所接收的外部配置指令,选择需要配置的所述第一群组的一个或多个可配置的第一联网代理,以便创建所述数据通信;至少部分地根据所接收的外部配置指令,为一个或多个可配置的第一联网代理中的每一个确定第一联网配置指令;和将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理,从而创建用于连接到由所述第二控制代理创建的第二节段的第一节段。

[0033] 根据本发明的另一个方面,提供了一种用于在请求者和目标之间创建数据通信的方法,其中:所述请求者与第一群组和第一控制代理相关联;并且所述目标与第二群组和第

二控制代理相关联，所述方法包括以下步骤：在所述第二控制代理处接收来自另外的控制代理的请求，其中，所述请求用于在所述目标和请求者之间创建所述数据通信，其中，所述另外的控制代理不同于所述第一控制代理；确定需要配置的所述第二群组的一个或多个可配置的第二联网代理，以便创建所述数据通信；为一个或多个可配置的第二联网代理中的每一个确定第二联网配置指令；将所述第二联网指令传送到所述一个或多个可配置的第二联网代理，从而创建第二节段；确定外部配置指令，所述外部配置指令被配置成使得所述另外的控制代理能够创建另外的节段以连接到所述第二节段；和将所述外部配置指令传送到所述第一控制代理。

[0034] 根据本发明的另一个方面，提供了一种控制代理，所述控制代理被配置成实施上述方法中的任何一种或多种。

[0035] 根据本发明的另一个方面，提供了一种系统，包括：第一控制代理，其定义包括至少一个第一计算机的第一群组；和第二控制代理，其定义包括至少一个第二计算机的第二群组，其中，所述第一控制代理和第二控制代理被配置成在彼此之间交换数据，其中，所述第一控制代理被配置成：从请求者接收连接到目标的意图，其中，所述请求者与所述第一群组的第一计算机相关联，并且所述目标与所述第二群组的第二计算机相关联；将所述第二控制代理标识为与所述目标相关联，并生成请求；并且将所述请求传送到所述第二控制代理，其中，所述第二控制代理被配置成：从所述第一控制代理接收所述请求；确定需要配置的所述第二群组的一个或多个可配置的第二联网代理，以便创建所述数据通信；为一个或多个可配置的第二联网代理中的每一个确定第二联网配置指令；将所述第二联网指令传送到所述一个或多个可配置的第二联网代理，从而创建第二节段；确定外部配置指令，所述外部配置指令被配置成使得所述第一控制代理能够创建第一节段以连接到所述第二节段；并且将所述外部配置指令传送到所述第一控制代理，并且其中，所述第一控制代理被进一步配置成：接收所述外部配置指令；至少部分地根据所接收的外部配置指令，选择需要配置的所述第一群组的一个或多个可配置的第一联网代理，以便创建所述数据通信；至少部分地根据所接收的外部配置指令，为一个或多个可配置的第一联网代理中的每一个确定第一联网配置指令；并且将所述指令传送到所述可配置的第一联网代理或每个所述可配置的第一联网代理，从而创建用于连接到所述第二节段的第一节段，从而创建路径。

[0036] 所述系统可以进一步包括所述一个或多个第一联网代理和所述一个或多个第二联网代理。所述请求者和所述目标可以是在其相应计算机上运行的应用，并且所述请求者和目标可以被配置成根据所创建的路径进行数据通信。

[0037] 根据本发明的另一个方面，提供了一种包括代码的计算机程序，所述代码被配置成当所述代码被计算机执行时，使所述计算机实施上述方法中的任何一种。

[0038] 根据本发明的另一个方面，提供了一种包括上述计算机程序的计算机可读存储介质。

[0039] 如本文使用的，词语“包括(comprise)”或其变型(comprises/comprising)以包含性意义使用，即指定所述特征的存在，但不排除本发明的各个实施例中的另外的特征的存在或添加。

附图说明

[0040] 为了更清楚地理解本发明,现在将参考附图通过举例的方式描述实施例,在附图中:

[0041] 图1示出了根据实施例的通信系统;

[0042] 图2示出了根据一个实施例的在实体和群组之间的关系;

[0043] 图3示出了示例性计算机的示意图;

[0044] 图4示出了路径的组件的示意图;

[0045] 图5示出了由第一控制代理采用的用于促成在第一群组的第一计算机和第二群组的第二计算机之间的路径的方法;

[0046] 图6示出了由第二控制代理采用的用于促成在第一群组的第一计算机和第二群组的第二计算机之间的路径的方法;

[0047] 图7示出了包括作为可配置的联网代理的防火墙的一个实施例;

[0048] 图8示出了包括作为可配置的联网代理的NAT的一个实施例;

[0049] 图9示出了对图6的方法的修改,包含能力交换步骤;

[0050] 图10A和10B涉及利用另外的节段的一个实施例;并且

[0051] 图11涉及图10的实施例的用例。

具体实施方式

[0052] 图1示出了代表本文所述的实施例的通信系统10。系统10包含与网络15进行数据通信的多个计算机11。网络15应被理解为代表能够在计算机11之间进行通信的任何数据互连——通常,网络15的至少一部分将包括诸如因特网的公共网络。数据通信可以至少部分地基于因特网协议(IP)。然而,可以包含其它形式的数据通信,例如,部分数据通信可以包括诸如蓝牙或USB的协议。在另一种形式中,数据通信可以在同一主机上运行的进程之间进行,例如经由存储器管道。

[0053] 出于本公开的目的,计算机11被认为对应于具有用于与一个或多个其它计算机11进行数据通信(例如,本文假设经由网络15,除非另有说明)的设施的任何合适的计算装置——存在这种计算机11的多个实施方案,例如独立的计算硬件(例如,台式或膝上型计算机)、独立的服务器、分布式计算布置、例如智能手机和平板电脑的移动装置、以及其它装置。计算机11可以例如对应于在服务器环境内实施的虚拟计算机,其可以是云服务,例如Amazon Web Services™。因此,两个计算机11可以对应于在同一服务器基础设施内实施的多个虚拟计算机。

[0054] 图1示出了被分组到第一群组30a中的多个计算机11a(在本文中被称为“第一”计算机11a)和被分组到第二群组30b中的多个计算机11b(在本文中被称为“第二”计算机11b)。每个群组30与控制代理13相关联(例如,第一控制代理13a与第一群组30a相关联,而第二控制代理13b与第二群组30b相关联)。尽管出于图示目的而分开地示出了控制代理13,但是所述控制代理可以被认为是其相应群组30的一部分。控制代理13可以是例如在群组30a、30b之一的计算机11a、11b上运行的程序,或者可以在物理上或逻辑上不同的专用服务器(未具体示出)中实施。更一般地说,群组30可以与在计算机11上运行的特定应用程序相关联,使得特定计算机11可以取决于所考虑的特定应用程序而与不同的群组30相关联。并

且,同一计算机11,或者更一般地说,同一应用程序可以与多个群组30(因此,多个控制代理13)相关联。

[0055] 在第一群组30a中,第一计算机11a被示出为与网络15进行直接数据通信——例如,每个第一计算机11a可以具有可从网络15直接寻址的IPv6地址(例如,经由因特网)。在第二群组30b中,第二计算机11b被示出为与网络地址转换(NAT)服务器14进行数据通信,所述服务器自身与网络15进行数据通信。因此,每个单独的第二计算机11b不可经由网络15直接寻址,而是必须经由NAT服务器14寻址,所述服务器可从网络15直接寻址。NAT服务器14通常是可使用端口转发技术配置的,以允许传入数据包被寻址到特定的第二计算机11b。所示出的群组30a、30b的实例纯粹是示例性的——通常,群组30可以具有可经由网络15直接寻址的一部分计算机11和/或不可直接寻址的一部分计算机。群组30可以对应于本地内联网或本地内联网的子集。

[0056] 参考图2,群组30也可以与一个或多个实体31相关联。实体31是在特定群组30内的一个或多个计算机11的用户。术语“实体”用于意指任何合适的用户概念——例如,个人或组织、或在组织内的群组(例如,IT服务台)。实体31由此利用计算机11。如图所示,实体31a与群组30a相关联,而实体31b与群组30b相关联。

[0057] 参考图3,一般来说,计算机11包括与存储器21和网络接口22接口连接的处理器20。所示出的处理器20实际上可以对应于单个CPU、多个CPU、在分开的硬件中实施的多个CPU的功能互连网络、微控制器等。存储器21通常包括易失性存储器和非易失性存储器。存储器21被配置成存储可由处理器20执行的程序指令,并且用于提供数据空间以存储程序指令所使用的数据。

[0058] 网络接口22被配置成使处理器20能够通过网络15传送数据并经由网络15接收数据。图1中示出的网络15应被解释为多个装置的任何互连——包含计算装置以及诸如路由器和交换机的网络节点。这些连接可以利用有线电连接、光连接和无线连接(通常是这些连接中的一些的组合)。相关地,数据通信通常由一个或多个协议定义——例如,因特网上的通信所常用的TCP/IP堆栈。网络15可以包括公共网络,例如因特网。计算机11还可以包括可移动介质端口23,其被配置成使得计算机11能够向可移动数据存储(未示出)读取和写入数据。根据本文所述的实施例,这个功能性可以实现数据通信。

[0059] 返回参考图1,示出了第一控制代理13a(其与第一群组30a相关联)。实际上,数据通信可以经由任何合适的信道——对于本公开来说,假设数据通信也经由网络15,但这可能不是必需的。每个控制代理13a、13b被配置成将请求传送到另一个控制代理13a、13b(在一个变型中,可能是以下情况:一个控制代理13可以被配置成仅接收请求)。通常,选择并配置一个预定义通信协议,以能够实现在控制代理13a、13b之间的通信。在一个实施例中,通信经由消息服务,例如电子邮件。在另一个实施例中,通信经由文件传输协议。在另一个实施例中,控制代理13a、13b运行用于实现所需的通信的专门配置的应用程序。还设想可以利用“离线”通信信道,例如经由利用可移动介质端口23的便携式固态存储装置的传输。通常,可以利用任何合适的通信系统。

[0060] 图4至6涉及示出了在第一群组30a的第一计算机11a和第二群组30b的第二计算机11b之间创建数据连接的示例性方法。图4示出了在请求者33和目标34之间的路径32的组件的示例性示意图。请求者33是与第一计算机11a相关联的应用程序,其需要通向目标34的数

据通信路径。目标34是在第二计算机11b上运行的应用程序。在这两种情况下，根据一个实施例，术语“应用”(应用程序)应被理解为具有宽泛的范围——例如，一个应用程序可以对应于多个应用，或者实际上，对应于计算机11本身。

[0061] 路径32还包含第一群组30a的一个或多个第一联网代理35a和第二群组30b的一个或多个第二联网代理35b。联网代理35a、35b包括以某种能力参与发起和/或维护在请求者33和目标34之间的数据通信路径的联网进程。联网代理35a、35b可以被实施为在与请求者33和目标34相同的计算机11a、11c上运行的进程，或在另外的计算机11上运行的进程(通常，可以存在在与请求者33和目标34相同的计算机11a、11b上以及在不同的计算机11上操作的联网代理35a、35b的混合体)。

[0062] 联网代理35a、35b中的至少一个是可配置的——通常，至少一个第一联网代理35a是可配置的，并且至少一个第二联网代理35b是可配置的。这里，“可配置”意指：在可配置的联网代理35a、35b的节段40内的操作至少部分地可由其相关联的控制代理13a、13b配置——例如，可配置的第一联网代理35a至少部分地可由第一控制代理13a配置，并且可配置的第二联网代理35b至少部分地可由第二控制代理13b配置。在附图中，路径32包括与第一群组30a相关联的第一节段40a和与第二群组30b相关联的第二节段40b。第一节段40a包括第一联网代理45，且第二节段40b包括第二联网代理40b。

[0063] 出于本公开的目的，节段40被描述为连接到另一个节段40和/或请求者33或目标34。例如，第一节段40a将请求者33连接到第二节段40b，并且相对应地，第二节段40b将目标34连接到第一节段40a。如本文所述，在一些实施例中，可以利用除第一节段40a和第二节段40b之外的另外的节段40。以这种方式，节段40链接以在请求者33和目标34之间创建路径32。

[0064] 在一个实施例中，目标34可以是可寻址的，使得可以将数据包向其定向。例如，目标34可以被配置(或者实际上，可以是可动态配置的)以在特定端口(例如，TCP或UDP)上接收数据包。在一个实施例中，目标34可以是间接可寻址的——例如，经由提供地址转换功能的联网代理35a、35b。

[0065] 在一个实施例中，一个或多个节段40可以利用在本申请人的PCT申请号PCT/AU2020/050244(2020年3月14日提交，2021年5月6日公布为WO 2021/081575 A1，此文件的全部公开内容通过引用并入本文)中描述的数据通信方法。此外，在控制代理13之间的通信可以经由根据本申请人的早期PCT申请的通信方法预先创建的连接。

[0066] 参考图5，描述了一种方法，其中，第一实体31a(即，与第一群组30a相关联)向其相关联的第一控制代理13a传送指示期望与第二群组30b的目标34进行数据通信的意图。

[0067] “意图”包括可以由接收控制代理13(即，本实例中的第一控制代理13a)接收和处理的预定义数据结构。数据结构通常被预定义成例如适合于由特定控制代理13处理——因此，当与不同的控制代理13通信时，可以使用不同的预定义数据结构。

[0068] 在步骤100，将意图从第一计算机11a传送到第一控制代理13a。第一实体31a在概念上可以是第一计算机11a的用户——因此，其可以是在输入到第一计算机11a中时的用于将实体与计算机11相关联的用户的凭证。应理解，可以将意图传送到第一控制代理13a，而不需要显式用户动作——例如，所述意图的生成可以是自动化的。在一个变型中，不需要与第一控制代理13a的显式通信——例如，所述要求可以是对数据通信的周期性要求，并且第

一控制代理13a被自动化以进行所述方法的动作，而无需明确地接收意图。

[0069] 在一个实施例中，第一实体经由在相关联的第一计算机11a和第一控制代理13a之间的数据信道(例如通过使用两者都位于其上的内联网)与第一控制代理13a通信。可以设想，在另一个实施例中，第一实体可以使用其它手段与第一控制代理13a通信——例如经由实体(用户)与第一控制代理13a的系统操作者(另一个用户)以言语方式通信——然后，系统操作者能够将意图的相关细节输入到控制代理13a中。第一计算机11a和第一控制代理13a可以包括在同一硬件上运行的分开的进程——在这种情况下，数据信道可以对应于共享存储器管线或共享存储器工作空间。

[0070] 根据一个实施例，在步骤101，第一控制代理13a然后将处理意图，以便标识第二控制代理13b与目标34相关联(例如，根据请求确定)。以这种方式，第一控制代理13a也标识第二群组30b。例如，所述请求可以明确地指定第二群组30或第二控制代理13b。在另一个实例中，第一控制代理13a可能已经被预先提供了控制代理相互参考信息，使得能够在目标34和其相关联的控制代理13b之间进行相互参考。例如，第一控制代理13a可以维护用于将特定目标34与特定控制代理13相关联的表格或其它数据库结构(“控制代理相互参考数据库”)。

[0071] 在一个实施例中，第一控制代理13a可以与第二控制代理13b进行数据通信，例如以接收相互参考信息的改变——例如，当第二控制代理13b对相互参考信息进行改变时，这可以通过数据通信而传播到第一控制代理13a。可以向第一控制代理13a提供对由第二控制服务器13b保持的仅相互参考信息的子集；例如仅被授权由第一控制服务器13a使用的相互参考信息的访问权。

[0072] 在步骤102，第一控制代理13a然后可以确定用于向第二控制代理13b提出请求的请求格式，并生成请求。请求是用于在第一控制代理13a和第二控制代理13b之间的通信的预定义数据结构。请求格式可以是用于所有控制代理13的标准格式，或者可以是用于特定第二控制代理13b的专用格式。请求格式定义了必须是请求的一部分的某些数据项，并且在一个实施例中定义了某些任选的数据项。由此，请求格式应确保所述请求适合于标识所述目标34——在一个实施例中，所述请求包含适合于使第二控制代理13b能够确定正确的目标34的目标ID。

[0073] 在步骤103，第一控制代理13a然后将请求传送到第二控制代理13b。例如，经由因特网(例如，作为网络15的一部分)传送所述请求，但也可以设想其它通信手段(例如，经由便携式固态存储装置)。第一控制代理13a和第二控制代理13b实际上可以对应于在同一硬件上运行的分开的进程——在这种情况下，数据信道可以对应于共享存储器管线或共享存储器工作空间。

[0074] 作为图5的示例性方法的结果，请求由与请求者33相关联的第一控制代理13a传送到与目标34相关联的第二控制代理13b。

[0075] 图6示出了由第二控制代理13b相关于由第一控制代理13a发送的请求所实施的方法。在步骤200，第二控制代理13b经由预定义信道接收请求。

[0076] 在步骤201，第二控制代理13b然后处理请求，以标识与请求相关联的目标34。在一个实施方案中，目标ID可以通过参考其上运行所述目标34的特定第二计算机11b来具体地定义目标34。在另一个实施方案中，要求第二控制代理13b基于目标ID来确定与目标34相关联的正确的第二计算机11b。例如，目标ID可以包括用户标识符，在这种情况下，要求第二控

制代理13b标识当前与用户标识符相关联的第二计算机11b(例如,当用户使用在不同位置的不同的计算机11时,这可能会有所不同)。在另一个实例中,目标ID可以包括临时标识符,例如已经提供给第一实体31a的临时标识符——这在第一实体31a是IT支持专业人员或类似人员并且仅需要对于特定目标的临时访问权的情况下可能特别有用。

[0077] 根据一个实施例,在步骤202,第二控制代理13b应用权限检查来确定请求是否满足预定义要求——仅在响应于确定了预定义要求被满足时,第二控制代理13b将继续到步骤203——即,继续在目标和请求者33之间创建路径32。权限检查可以基于在所述请求内存在的信息。权限检查可以包含对第一实体31a、第一计算机11a和/或第一群组30a的考虑。

[0078] 在一个实施例中,权限检查可以包含主动检查,其中,在第二控制代理13b接收请求之后,所定义的授权实体31被要求提供权限。例如,批准请求被发送到被授权提供对创建路径32的批准的实体31,例如经理。这可以以任何合适的方式传送,例如经由电子邮件。在一个特定实例中,授权实体31可能已经在装置(例如,智能电话)上接收通知——所述通知可以为授权实体31提供设施以提供批准(其被传送到第二控制代理13b),从而满足权限检查的至少一部分。

[0079] 在步骤203,第二控制代理13b然后确定第二节段40b——即,与第二群组30b相关联的路径32的部分,用于实现在请求者33(在第二群组30b外部)和目标34之间的通信,如前所讨论的,所述目标与第二计算机11b相关联。

[0080] 返回参考图6,在步骤204,第二控制代理13b然后向第二节段40b的所述一个或多个可配置的第二联网代理35b发送内部配置指令。所述配置指令被配置成使所述一个或多个第二联网代理35b能够有效地创建第二节段40b。

[0081] 根据一个实施例,在步骤205,第二控制代理13b向第一控制代理13a发送外部配置指令。外部配置指令被配置成使得能够创建与第一群组30b相关联的第一节段40a。例如,外部配置可以提供合适的指令,以使第一节段40a能够正确地连接到第二节段40b。换句话说,外部配置指令适合于使得第一计算机11a能够成功地与第二计算机11b通信。例如,所述配置指令可以指定目标IP地址和/或目标端口。在一个实施例中,可以使第二控制代理13b能够将所述配置指令直接传送到第一计算机11a(即,绕过第一控制代理13a)。例如,在步骤102生成的请求可以包含通信信息,以使第二控制代理13b能够与第一计算机11a直接通信。

[0082] 根据图5和图6的方法,使第一控制服务器13a和第二控制服务器13b能够在不同群组30中(因此,例如,在不同的内联网上)的计算机11之间动态地创建特定点对点数据连接。所述方法还可以用于实现在同一内联网上的不同子网中的计算机11之间的特定点对点数据连接。这些数据连接可以有利地是应用程序特定的——因此,固有地应用最小访问权限。例如,所述数据连接被配置成用于与特定应用程序的通信(例如,通过注册特定的UDP或TCP端口),并且任选地,将另外的联网代理35配置成用于所述特定通信。

[0083] 图4示出了联网代理35a、35b。特别地,包含一个或多个可配置的联网代理35a、35b(优选地,每个节段40包含至少一个)。通过配置这些一个或多个可配置的联网代理35a、35b来创建路径32——没有所述配置的话,在请求者33和目标34之间的数据通信就无法实现。本文所述的实施例允许满足这一要求的多种可配置的联网代理35a、35b。以这种方式,本文所述的实施例可以有利地提供用于在请求者33和目标34之间的有针对性的数据通信的手段。下面描述了包括示例性的可配置的联网代理35a、35b的多个实施例。

[0084] 参考图7,在一个实施例中,可配置的第二联网代理35b是第二群组30b的防火墙14b。在一个实例中,可以指示第二计算机11b允许在与目标34相关联的特定端口(例如,VNC端口)上通信——这可以通过配置在第二计算机11b上运行的防火墙应用程序(相关的可配置的第二联网代理35b)来实现。在另一个实例中,目标应用程序34自身被配置成在特定的定义端口上监听——在这种情况下,目标34也是可配置的第二联网代理35b。在另一个实例中,防火墙由独立于第二计算机11b的硬件(或独立于第二计算机的虚拟计算机)实施,并且可被配置成允许源自第一计算机11a的数据包(例如与特定端口相关联的数据包)通向第二计算机11b。

[0085] 参考图8,在一个实施例中,与第二群组30b相关联的NAT服务器14b可以被配置成对从第一计算机11a具体地接收的、寻址到特定端口的数据包实施端口转发,使得从网络15接收的定向至所述端口的数据包被转发到第二计算机11b。

[0086] 在一个实施例中,可配置的第二联网代理35b对应于认证协议。此协议的目的是要求与第一计算机11a相关联的实体31a进行认证程序(例如,双因素认证)。本实施例的优点可以是:对于特定的群组30,而不是对于每个计算机11,仅需要一个认证协议。授权协议可以被配置成向相关控制代理13、第二计算机11b、和/或另一个计算机11提供反馈,以确认成功的认证。然后,这可以使接收反馈的装置实施其在所述路径中的部分(使得所述路径仅在成功认证之后完成)。

[0087] 在一个实施例中,节段40a、40b配置有互补的加密协议(例如,AES)。因此,作为应用程序,请求者33和目标34自身不需要实施安全性——这作为路径32的一部分来解决。本实施例是在第一节段40a和第二节段40b中都需要的配置动作的一个实例——这是通过内部配置指令(用于配置第二节段40b的指令)和外部配置指令(用于配置第一节段40a的指令)来实现的。

[0088] 在一个实施例中,节段40a、40b可以使用外部汇聚点服务器(未示出)来链接。例如,这可以适用于请求者33和/或目标34位于不能被显式配置成允许通信的防火墙16或NAT服务器14之后的情况。在这种情况下,汇聚点服务器可以为请求者33和目标34两者提供传出会合点——一旦两者都与汇聚点服务器连接,就可以促成连接(所述汇聚点服务器不一定参与进一步后续的通信)。此过程的一个实例是在PCT/AU2020/050244中描述的“连接服务器”实施例。

[0089] 根据一个实施例,路径32具有时限或关于其存在的其它限制(例如,路径32可以被取消)。也就是说,路径32的可配置特征被配置成使得在达到时限或限制之后,它们将不再从第一计算机11a向第二计算机11b传递数据包。例如,第二控制代理13b可以将可配置的第二联网代理35b中的一个或多个配置成仅在到达时限之前允许通信。在另一个实例中,第二控制代理13b自身可以监视时限,并向第二联网代理35b发送另外的内部配置指令,以停止允许通信。

[0090] 根据一个实施例,路径32可以经由在任一控制代理13处接收的命令来取消——例如,与控制代理13相关联的系统操作者可以选择取消所述路径。在另一个实例中,与计算机11之一相关联的实体31可以与其相关联的控制代理13通信(例如,经由由计算机11或另一个装置发送的命令)以请求取消所述路径32——作为响应,控制代理13取消所述路径32。当控制代理13采取动作以取消路径32时,它可以经由数据通信通知另一个控制代理13。控制

代理13采取的动作可以包含向其关联的联网代理35a、35b中的一个或多个发送配置指令，以使路径32停止。

[0091] 根据一个实施例，在创建路径32之前，第一控制代理13a和第二控制代理13b在它们自身之间传送能力信息。例如，在第一群组30a和/或第二群组30b的情景中，多个节段40可以是可能的。此外，可以是仅可能节段40的子集适合于创建路径32——例如，第一节段40a和/或第二节段40b可以受限于可用的网络协议。通过共享此信息，第二控制代理13b可以生成外部配置指令，例如以与第一群组30a的能力兼容。此外，还生成内部配置指令以确保在节段40a、40b之间的兼容性。

[0092] 参考图9(它是图6的改型)，任选的附加步骤206实现了能力信息的交换。然而，在另一个实施例中，控制代理13a、13b进行能力信息的交换，作为独立于任何单独路径生成的进程。例如，当能力改变时，控制代理13a、13b可以向彼此发送更新的能力信息。

[0093] 本文所述的实施例可以有利地提供一种简化的进程，用于将使能在不同组织之间(或者甚至单个组织内的子网之间)的通信的商业协议与这种连接的技术要求相匹配。这是通过使控制代理13能够负责实施各个技术要求而不是要求预先配置每个单独的计算机11来实现的。

[0094] 例如，达成以下协议：第一群组30a的实体31a被授予访问在第二群组30b的一个或多个计算机11b上运行的特定应用(即，特定目标34)的权限。例如，在技术支持的情景中，特定应用可以是远程桌面或VNC服务器。由于实体30a可以是能够使用第一群组30a的不同计算机11a的人，因此针对此连接来配置每个计算机11a可能是困难的。类似地，将第二群组30b的每个计算机11b配置成接受来自这个实体的连接可能也是困难的——尤其是当所述连接可能来自不同的计算机11a时。

[0095] 本文所述的实施例可以有利地用于使控制代理13的系统操作者能够实施由群组管理员做出的策略决定。这里，群组管理员与特定群组30相关联，并且是被授权决定策略(例如，在不同群组30的群组管理员之间的协议)的决策者。系统操作者可以通过对相关联的控制代理13进行配置来实施策略，例如配置成定义可以访问相关联群组30的特定目标34的其它群组30的授权实体31。例如，可以在控制代理13内定义针对特定实体或实体类别的特定访问权限和特定目标34。此外，可以使系统操作者能够确保由相关联的控制代理13创建的节段40包含所需的联网代理35a、35b——例如，以确保安全性匹配策略。在另一个实例中，控制代理13可以被配置成确保传入连接等等的适当记录。

[0096] 现有技术可以向实体31a提供VPN登录细节或类似内容。然而，这种现有技术需要复杂的认证和权限管理，因为它们可以在提供对内联网的广泛访问权的基础上进行操作，而这种访问权在随后必须受到限制。本文所述的实施例提供了基于需求的对在特定计算机11上操作的特定目标34(例如，应用)的有针对性的访问权。这种方案可以是固有安全的，因为无需为了避免更广泛的访问权而对访问权进行限制。

[0097] 本文所述的实施例的另一个潜在优点是，与群组30相关联的内联网(举例来说)可以被修改，同时仍然能够在与不同群组30相关联的计算机11之间进行直接的点对点通信。例如，仅与发生改变的特定群组30相关联的控制代理13需要被更新——其它群组30不需要更新。

[0098] 另一个潜在的优点是，基础数据传输机制可以是任意的——即，实体31、特定请求

者33和/或目标34可以不需要具有传输机制的任何知识。相反，控制代理13在逐个情况的基础上创建合适的路径32(经由单独的节段40)来实现连接——这些可以在一个实例中使用IPv6，而在另一个实例中使用IPv4。类似地，可以在一个实例中使用TCP，而在另一个实例中使用UDP。由于每个路径32因此可以在需要时被动态地创建，所以对底层协议或网络基础设施的任何改变都可以被隐藏。例如，所实施的特定安全协议(作为联网代理35)可以取决于所述连接是否包括公共无线网络。

[0099] 本文所述的实施例的另一个潜在优点可以是降低的安全复杂性——例如，不需要复杂的防火墙或NAT规则来处理所有可能的传入连接，防火墙和/或NAT服务器14按需被配置成使能在与不同群组30a、30b相关联的计算机11a、11b之间的连接，从而降低欺诈性连接的风险。

[0100] 类似地，一个优点可以在于，控制代理13(而不是请求者33和目标34应用程序)负责实施安全协议。这可以有利地帮助确保遵守组织安全规则。

[0101] 在一个实施例中，控制代理13被配置成维护目标相互参考数据库(“目标数据库”)。目标数据库被配置成使控制代理13能够在所接收的目标ID和其群组30内的特定计算机11之间进行相互参考。然后，可以更新目标数据库，以反映在与特定目标ID相关联的计算机11中的变化。例如，在用户接收新的计算机11或使用一个以上计算机11的情况下。控制代理13可以手动更新——例如，由IT经理在向另一个雇员提供新计算机11时更新。控制代理13也可以或者替代地自动更新——例如，在用于连接到企业网络的登录过程期间，消息被传送到控制代理13以使其更新目标ID。在一个实施例中，目标ID仅仅是网络用户的用户名。然而，可以设想，可以利用其它代码。控制代理13可以在它们自身之间传送更新的目标信息，从而使第一控制代理13a能够维护在第二控制代理13b处的目标34的目标数据库。

[0102] 在一个实施例中，目标ID是动态生成的——例如，针对特定的用例。在这种情况下，例如，计算机11可以向其控制代理13传送创建临时目标ID的需求。然后，这可以被提供给另一个群组30的实体，以促成通信。

[0103] 根据一个实施例，参考图10A和10B，一个实施例利用一个或多个另外的控制代理13c来帮助形成在请求者33和目标34之间的路径32。根据本实施例，第二控制代理13b可以被配置成接收对于目标34的请求，其中，与目标34相对应的应用程序(以及例如相对应的计算机11)不在相对应的群组30内。这种目标34可以被称为代理目标——这些可以被存储在控制代理13b可访问的合适的数据结构中。然而，第一控制代理13a还确定所述请求应被发送到另外的控制代理13c，而不是与第二群组30c相关联的第二控制代理13b。用于将另外的控制代理13c指示为请求接收者的信息可以存储在第一控制代理13a可访问的存储器中。然而，第一控制代理13a可以替代地被配置成将另外的控制代理13c确定为接收者——例如，通过查询第二控制代理13b并接收将另外的控制代理13c标识为目标的信息。

[0104] 在这种情形下，另外的控制代理13c被预先配置成例如将目标34标识为另外的控制代理13c的代理目标。可能不一定要求第一控制代理13a有权访问将第二控制代理13b标识为与目标34相关联的信息——即，第一服务器13a可以被配置成将另外的控制代理13c视为与目标相关联。

[0105] 根据一个实施例，第一控制代理13a进行本文所述的方法来形成第一节段40a，以连接到另外的控制代理13c的第三节段40c。然而，连接的第一节段40a和第三节段40c的形

成不一定创建通向目标34的完整路径32。

[0106] 另外的控制代理13c向第二控制代理13b提出请求——用于标识另外的控制代理13c的代理目标的信息可以将第二控制代理13b指定为与实际目标34相关联，从而使另外的控制代理13c能够标识第二控制代理13b。

[0107] 根据一个实施例，另外的控制代理13c然后进行本文所述的方法来形成第二节段40b——在概念上，这可以被认为是连接到第三节段40c。因此，请求者33现在经由包括三个节段40a、40b、40c的路径32而有效地与目标34进行数据通信。节段40a和40c可以被认为是“相邻的”(并且节段40b和40c也可以被认为是“相邻的”)。在本实施例中，节段40a和40b是“不相邻的”——因为它们在路径32中由节段40c连接。

[0108] 根据本实施例，第三群组30c的可配置的另外的联网代理35c可以继续参与在请求者33和目标34之间的通信。然而，在另一个实施例中，另外的控制代理13c仅参与在请求者33和目标34之间建立数据连接，并且实际上不参与后续的通信。

[0109] 本实施例可以扩展到进一步包含另外的控制代理13c——实际上，由此可以创建节段40的链。

[0110] 图10的实施例可以有利地实现权限的委托。例如，与另外的控制代理13c相关联的第三实体30c可以和与第二控制代理13b相关联的第二实体30b达成协议——例如，关于对资源(例如，数据库)或应用(例如，VNC服务器)的访问权。因此，第二控制代理13b和另外的控制代理13c被配置成在彼此之间建立路径32，以实现对资源或应用的访问。然而，第三实体30c可能期望能够委托与第一控制代理13a相关联的实体30a。本实施例可以有利地实现这种委托，同时确保任何网络连接规则(例如，安全性、记录等)根据在第二实体30b和第三实体30c之间的协议是正确的。在特定的委托实例中，在协议中可以要求允许委托。

[0111] 根据这些实施例，内部配置指令和外部配置指令可以指定用于创建路径的要求，所述路径适用于在相邻的控制代理13之间，以及在非相邻的控制代理之间——例如，在安全性的情况下，在请求者33和目标34之间的数据通信一旦形成，就可能需要端到端加密。此信息经由另外的控制代理13c(其不属于任一群组30a、30b)在第一群组30a和第二群组30b之间共享。

[0112] 图11示出了图10的实施例的用例，其中，第一节段40a与第一群组30a相关联，第二节段40b与第二群组30b相关联，并且另外的节段可以是：在第一节段40a和第三节段40c以及第三群组30c之间使用通信协议的第一组合(第三节段40c可以被认为是“另外的节段40c”，因为它与另外的控制代理13c相关联)。

[0113] 这种布置的一个优点可以是：第三群组30c和第二群组30b定义某些通信协议(例如，安全性、封装、寻址、NAT遍历等)，而第三群组30c和第一群组30a定义不同的通信协议。因此，当第一计算机11a试图创建与目标34(其可以是代理目标)的连接时，它根据其与第三群组13c的协定进行通信——第一计算机11a不需要“知道”在第二群组13b和第三群组13c之间的通信要求。类似地，第二计算机11b不需要“知道”在第一群组13a和第三群组13c之间的通信要求。因此，例如在委托布置中，所述实施例可以有利地允许第三群组13c管理不同的通信要求。例如，在需要汇聚服务器的情况下，这可以仅在第一群组13a和第三群组13c之间(或者，仅在第二群组13b和第三群组13c之间)。

[0114] 在一个实施例中，一个或多个控制代理13被配置成向其它控制代理13发布可用目

标信息，从而使接收者控制代理13能够标识与发布控制代理13相关联的一个或多个可用目标34。目标信息可以任选地定义发布有效时间，以指示接收者控制代理13认为所发布的信息有效所经过的时间段。接收者控制代理13可以被配置成部分地或全部地更新或覆写先前接收的由特定控制代理13发布的目标信息。因此，目标信息可以对应于先前提到的控制代理相互参考信息，并且在相关实施方案中，可以用于更新控制代理相互参考数据库。

[0115] 在一个实施方案中，使控制代理13能够以通常可由一个或多个其它控制代理13访问的方式发布目标信息——所述目标信息例如由非秘密统一资源标识符(URI)定义，所述统一资源标识符可以是统一资源定位符(URL)。其它实例包含在DNS TXT记录中存储合适的信息，并提供已知的电子邮件地址，所述电子邮件地址向查询自动回复目标信息。目标信息可以以能够实现对目标信息内容的受控访问的方式发布。例如，可以使用已知的技术对目标信息进行编码，使得每个控制代理13仅能够对其有权访问的目标信息的部分进行解码。在一个事件中，可以指示特定控制代理13访问公共目标信息(例如，通过被定向到已知的URL)，所述公共目标信息然后被解析以标识与特定控制代理13相关的目标信息的部分(其可以是目标信息的子集，或者如果未被控制的话，则可以是整个目标信息)，所述特定控制代理然后更新其控制代理相互参考信息。在另一个实例中，控制代理13可以响应于来自特定控制代理13的请求，选择性地传送部分目标信息，所述部分是根据请求控制代理13的标识确定的。以这种方式，使特定控制代理13能够从其它控制代理13获得合适的相互参考信息。

[0116] 在一个实施例中，其可以适用于例如利用另外的控制代理13c(如参考图10A、10B和11所描述)的实施例，使特定控制代理13能够发布另一个控制代理13的目标信息。例如，在图11中，第二群组30b的第二控制代理13b可以向第三群组30c的另外的控制代理13c提供与其相关联的一个或多个目标34相关联的目标信息。第三控制代理13c然后可以发布与第二群组30b相关联的目标信息，其可由第一群组13a的第一控制代理13a访问。有利地，第一控制代理13a可能不需要“知道”在第二群组30b和第三群组30c之间的关系本身，相反，它知道第二群组30b的一个或多个目标34可经由第三群组30c的另外的控制代理13c访问。另一个优点可以是，所述另外的控制代理13c可以有效地提供目标信息转发功能。

[0117] 在一个实施方案中，系统10被布置成使得特定控制代理13通常被禁止发布其目标信息，并且只能经由与授权的其它控制代理13的通信来这样做——例如，在图11中，第二控制代理13c被禁止直接向第一控制代理13a(或者实际上，任何其它未授权的控制代理13)发布，并且必须代之以向授权的另外的控制代理13c提供目标信息，这在发布所接收的目标信息之前应用其自己的规则(这可以例如通过添加关于哪些群组30和/或特定计算机11或请求者可以有权访问某些目标34的条件来限制如此发布的目标信息)。有利地，这种实施方案可以允许专用控制代理13发布目标信息，从而可以提供额外的安全性和/或实施与可以发布哪些目标信息以及可以发布到哪些控制代理13相关的商业规则的便利性。

[0118] 可以从其相关联的控制代理13向群组30的特定计算机11或请求者33提供可用的目标信息，所述可用的目标信息源自被提供给控制代理13的目标信息，但是基于条件规则被进一步限制。例如，某个计算机11或请求者33可能仅有权访问另一个群组30的目标34的子集，并且其控制代理13通过限制所述特定计算机11或请求者33可用的可用目标信息来管理所述子集。实际上，第一群组30a可以具有对第二群组30b的目标34的受限访问权，如由第

一群组30a的第一控制代理13a可用的目标信息部分所定义的，并且第一群组30a的特定请求者33可以具有对第二群组30b的目标34(仅在从第一控制代理13a传送到请求者33的可用目标信息中所存在的目标)的进一步受限访问权。因此，有利地，第二控制代理13b和第一控制代理13a都通过限制来控制可用于第一群组30a的特定计算机11或请求者33的第二群组30b的可用目标34。实际上，第三控制代理13c也可以如上所述限制可用目标34。这些限制可以至少部分地涉及将特定权限授予有权访问特定群组30的目标的特定请求者33、计算机11和/或群组30。例如，可以经由认证程序来授予权限，目标信息通过所述认证程序被确定为可用于特定请求者33、计算机11和/或群组30。

[0119] 返回参考图5，在一个实施例中，当传送到第一控制代理13a的意图直接标识与预期目标33相关联的特定第二控制代理13b时，如果第一控制代理13a不具有与第二控制代理13b相关联的控制代理相互参考信息，则它可以向第二控制代理13b请求目标信息(经由在所述意图中的用于标识第二控制代理13b的信息)或者可以寻找发布的信息(例如，通过访问如上所述的合适的URL)。如果适用的话，目标信息实际上可以从适当授权的第三控制代理13c中寻找。以这种方式，当需要时，群组30可以被“添加”到第一控制代理13a(也就是说，用于标识相应的其它控制代理13的信息可以被存储以供控制代理13将来使用)——由此，第一控制代理13a有效地建立了可用的控制代理13及其相对应的群组30和目标34的数据库。

[0120] 尽管本文的讨论已经假设请求者33与第一计算机11a相关，并且目标34与物理上或逻辑上不同的第二计算机11b相关，但是在一个实施例中，请求者33和目标34可以是在逻辑上相同的计算机11上(即，在相同的操作环境内，而不是作为不同的虚拟服务器)运行的应用程序。因此，所需的一个或多个节段40可能不需要经由外部网络15的数据通信(尽管在某些境况下，数据通信可以包含外部网络15)——然而，由于所述应用程序的性质或其上运行所述应用程序的计算机11的配置，需要由相应控制代理11管理的经由一个或多个节段40的通信。在这种情况下，第一控制代理11a和第二控制代理11b可以在与请求者33和目标34相同的计算机11上操作，虽然它们中的一个或两个可以在外部计算机11上实施。

[0121] 应当理解，本文使用的标签“第一”、“第二”等等旨在在描述由相关特征实施的特定作用和过程时对所述特征进行区分。然而，应当理解，这些实施方案可以在不同的时间呈现不同的作用——例如，特定控制代理13可以在实际操作期间进行第一控制代理13a和第二控制代理13b的所述动作，这取决于特定的境况。

[0122] 在不脱离本说明书的精神和范围的情况下，可以进行进一步的修改。

[0123] 例如，本文中的某些实施例可以扩展为包含与同一群组30相关联的请求者33和目标34，并且因此，第一控制代理13a和第二控制代理13b实际上是相同的；这些可以理解为与“公共”控制代理13相关。在这种情况下，公共控制代理13被配置成在请求者33和目标34之间创建路径32；也就是说，公共控制代理13可以将配置指令传送到一个或多个可配置的联网代理35。由于控制代理13是公共的，所以配置指令可以被认为既是内部的又是外部的——也就是说，在概念上，从请求者33的“角度”来看，某些配置指令可以是外部配置指令，而从目标34的“角度”来看，所述某些配置指令可以是内部配置指令。类似地，在概念上，从请求者33的“角度”来看，某些配置指令可以是内部配置指令，而从目标34的“角度”来看，所述某些配置指令可以是外部配置指令。在这种改型中，尽管请求者33和目标34在同一群

组30内,但一个或多个另外的控制代理13c也可能与路径32有关连;这仅仅是意指在请求者33和目标34之间的通信涉及被定向到包括请求者33和目标34的特定群组30之外的通信。

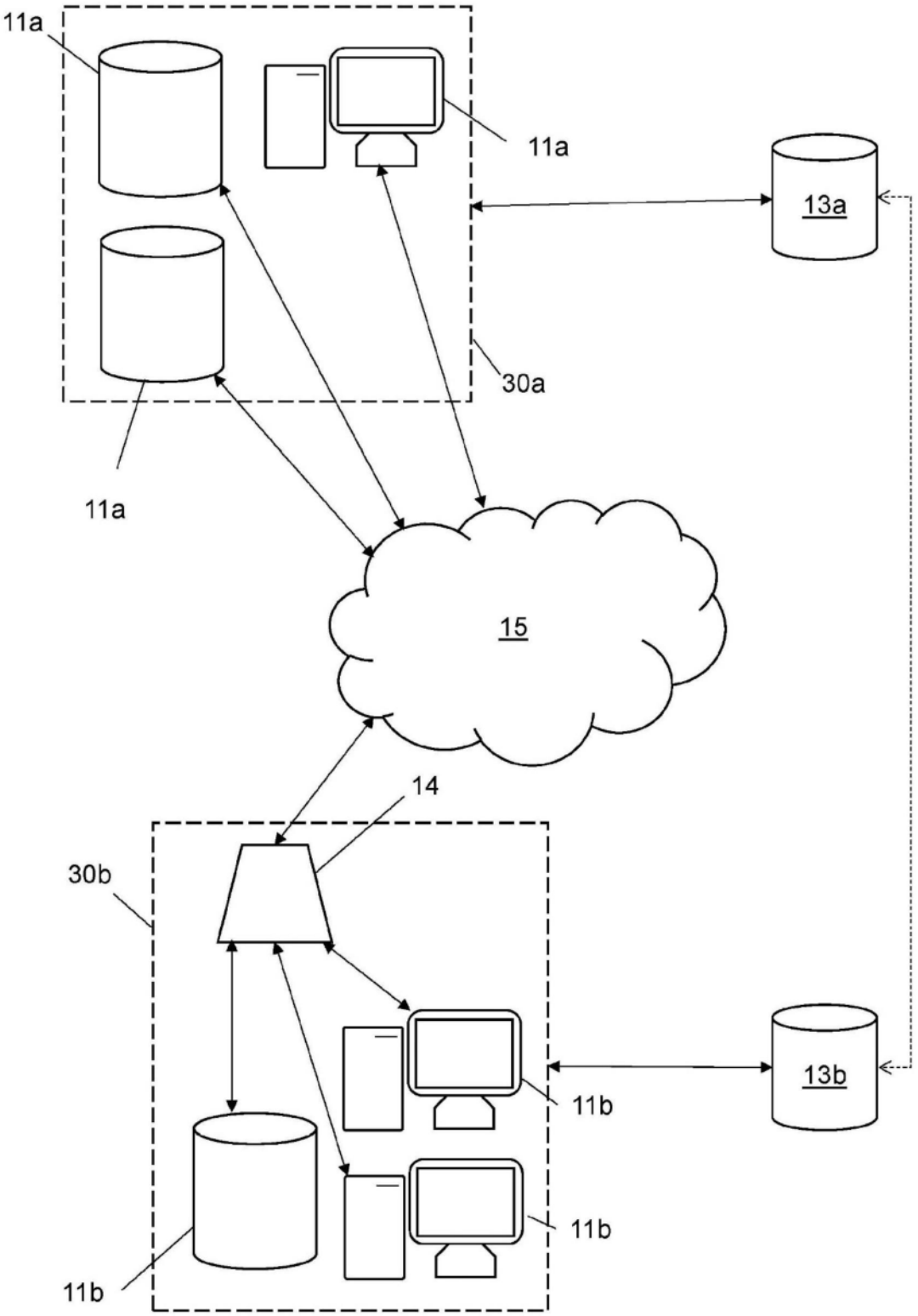
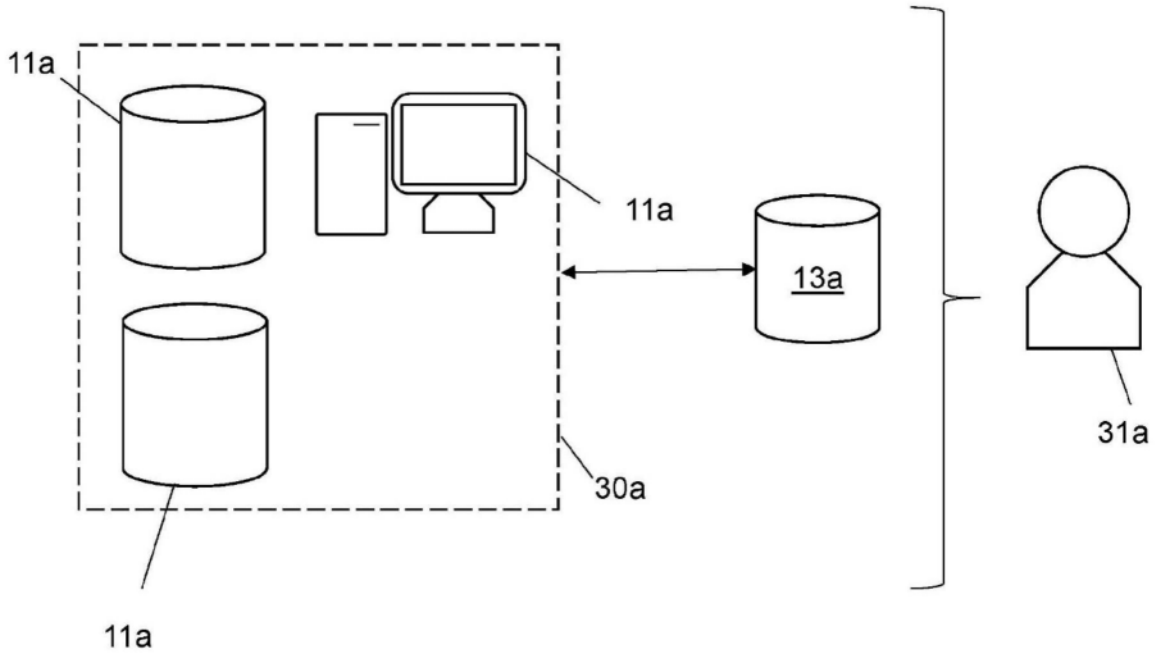


图1



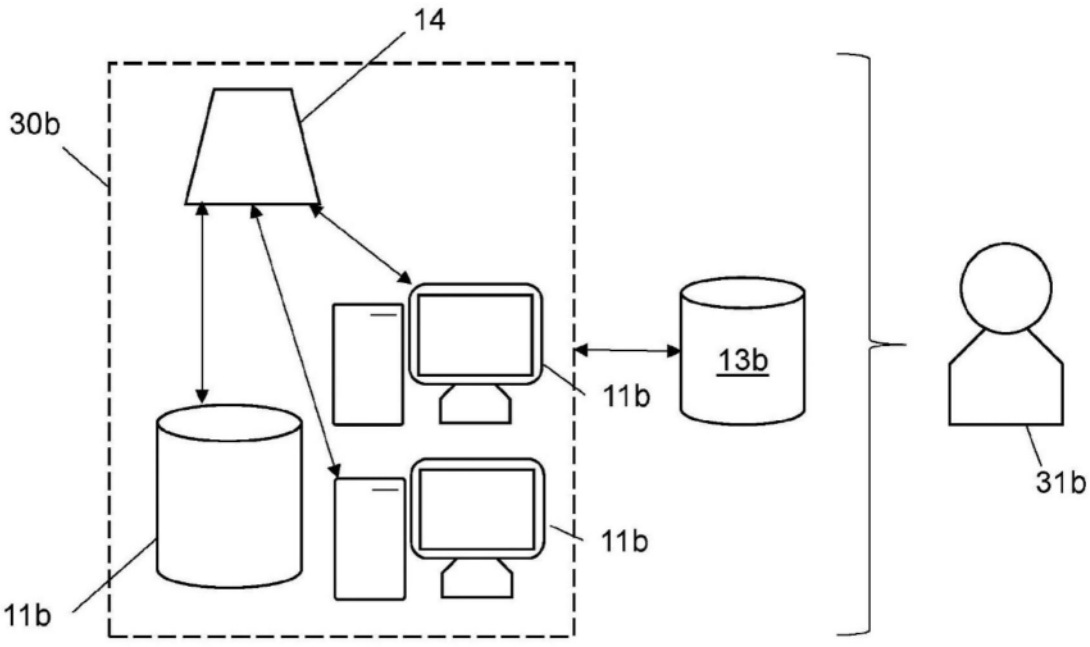


图2

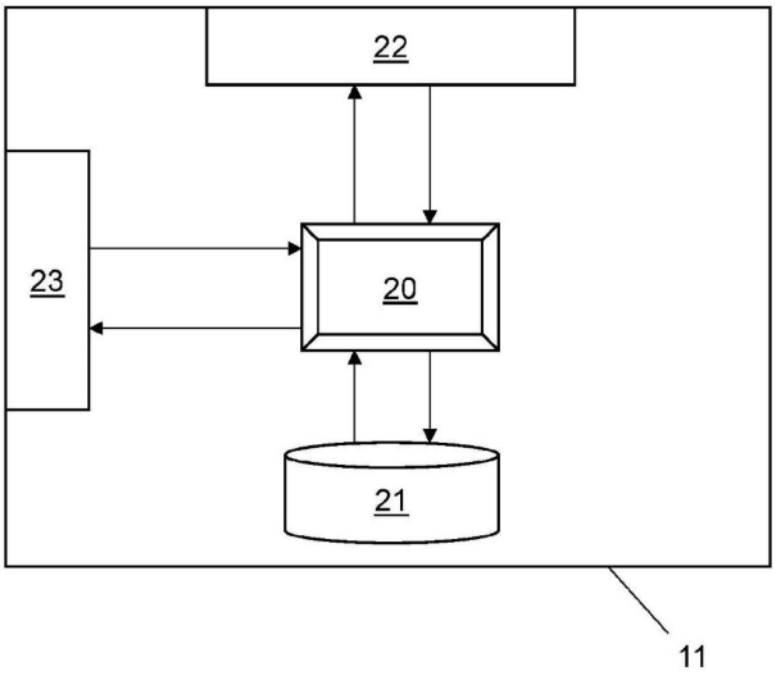


图3

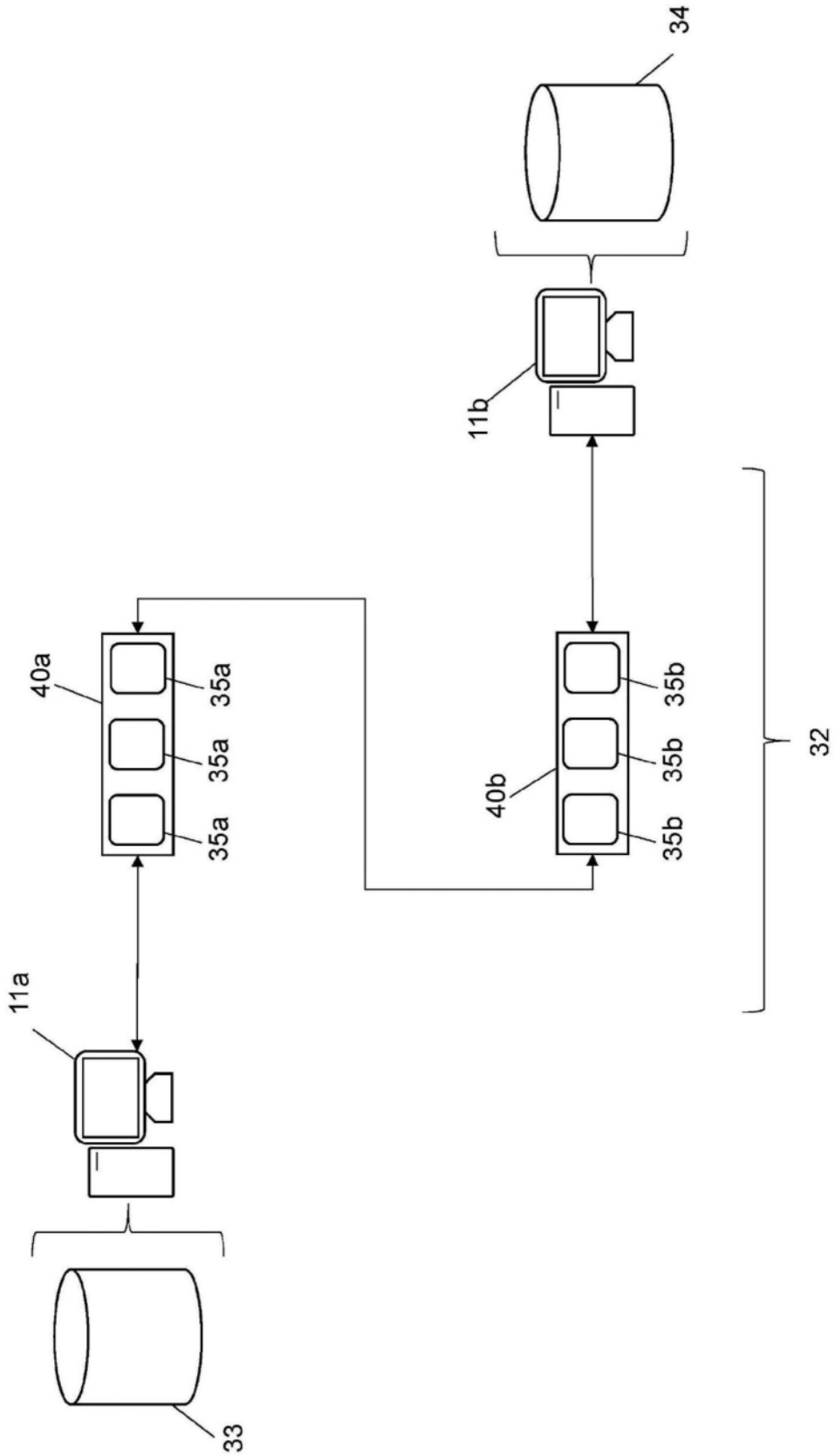


图4

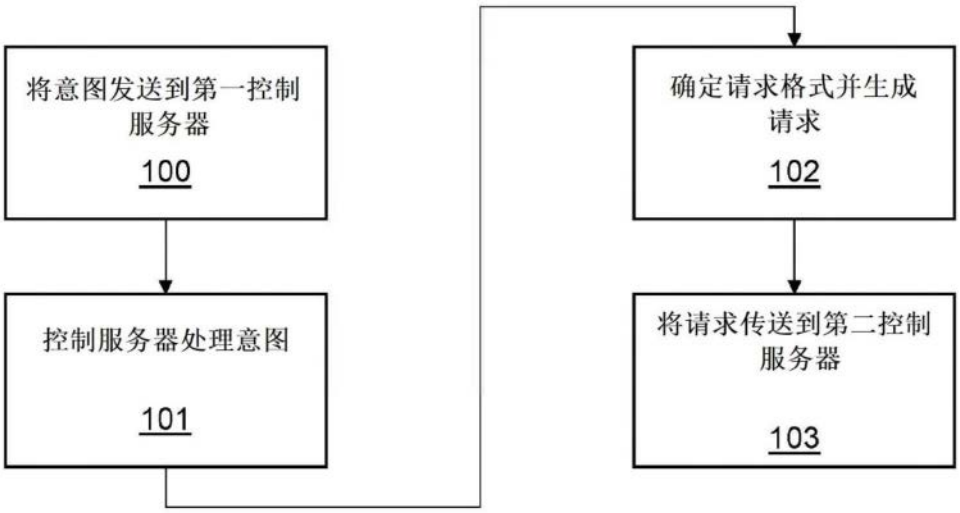

将意图发送到第一控制服务器
100
控制服务器处理意图
101
确定请求格式并生成请求
102
将请求传送到第二控制服务器
103

图5

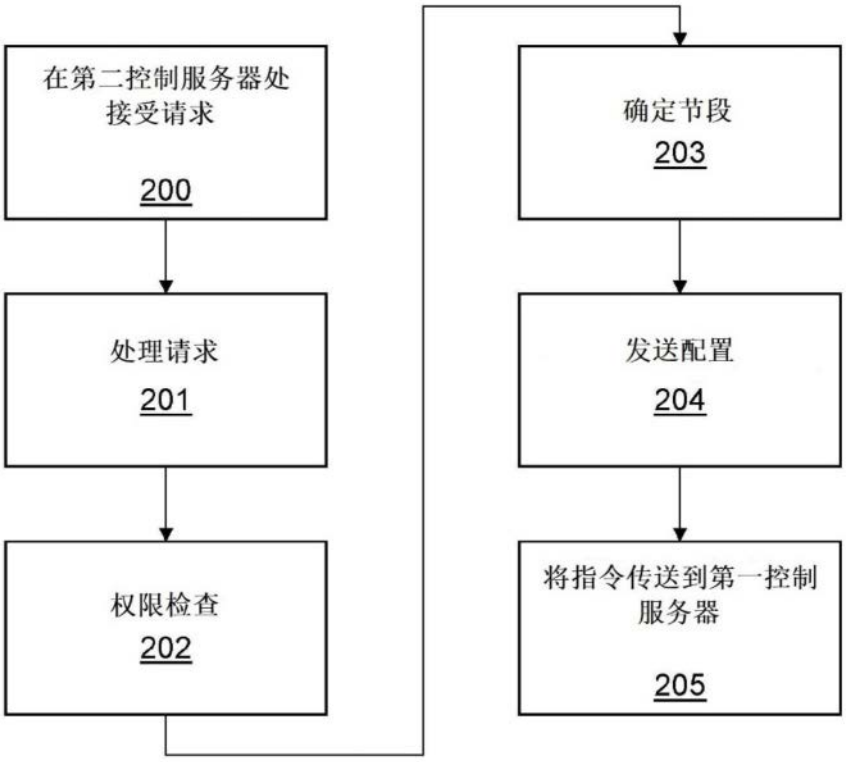

在第二控制服务器处接受请求
200
处理请求
201
权限检查
202
确定节段
203
发送配置
204
将指令传送到第一控制服务器
205

图6

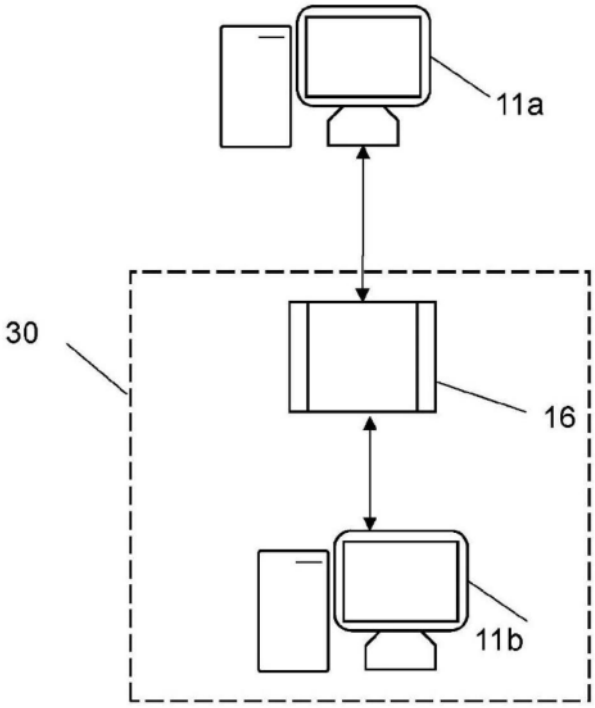


图7

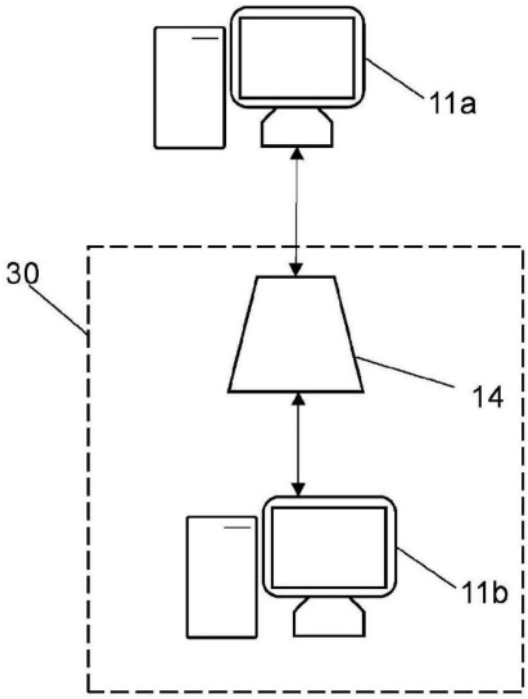


图8

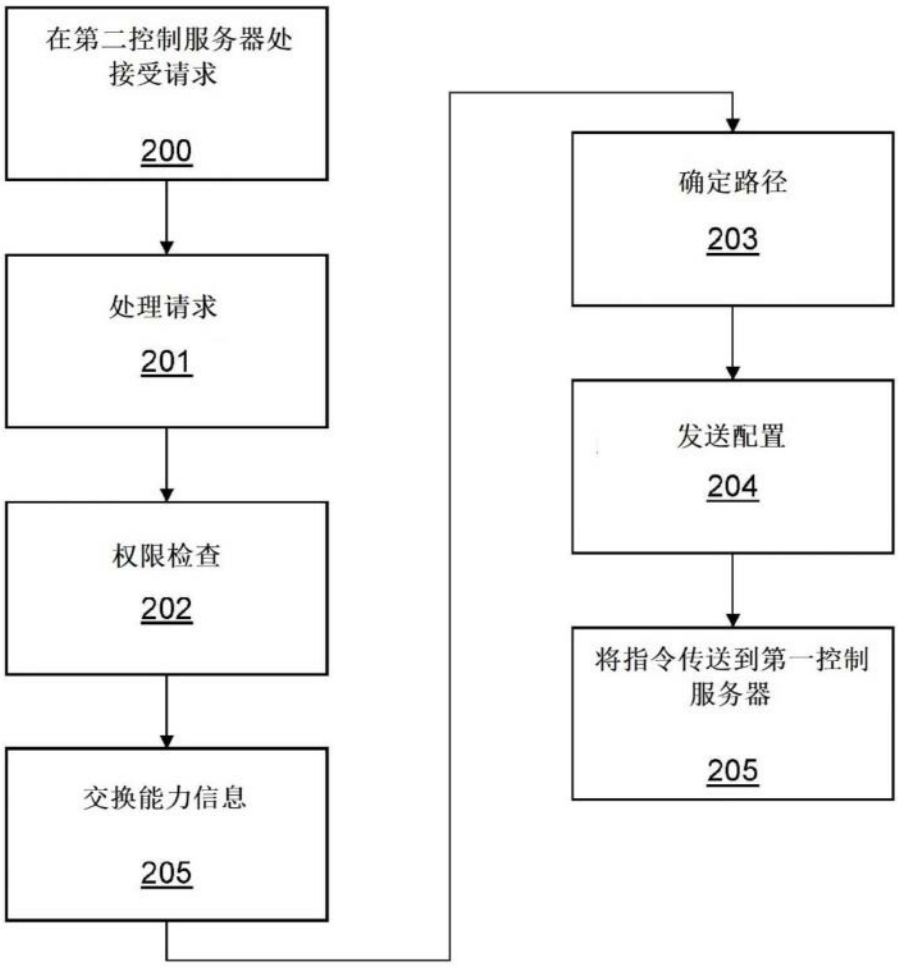

在第二控制服务器处接受请求
200
处理请求
201
权限检查
202
交换能力信息
205
确定路径
203
发送配置
204
将指令传送到第一控制服务器
205

图9

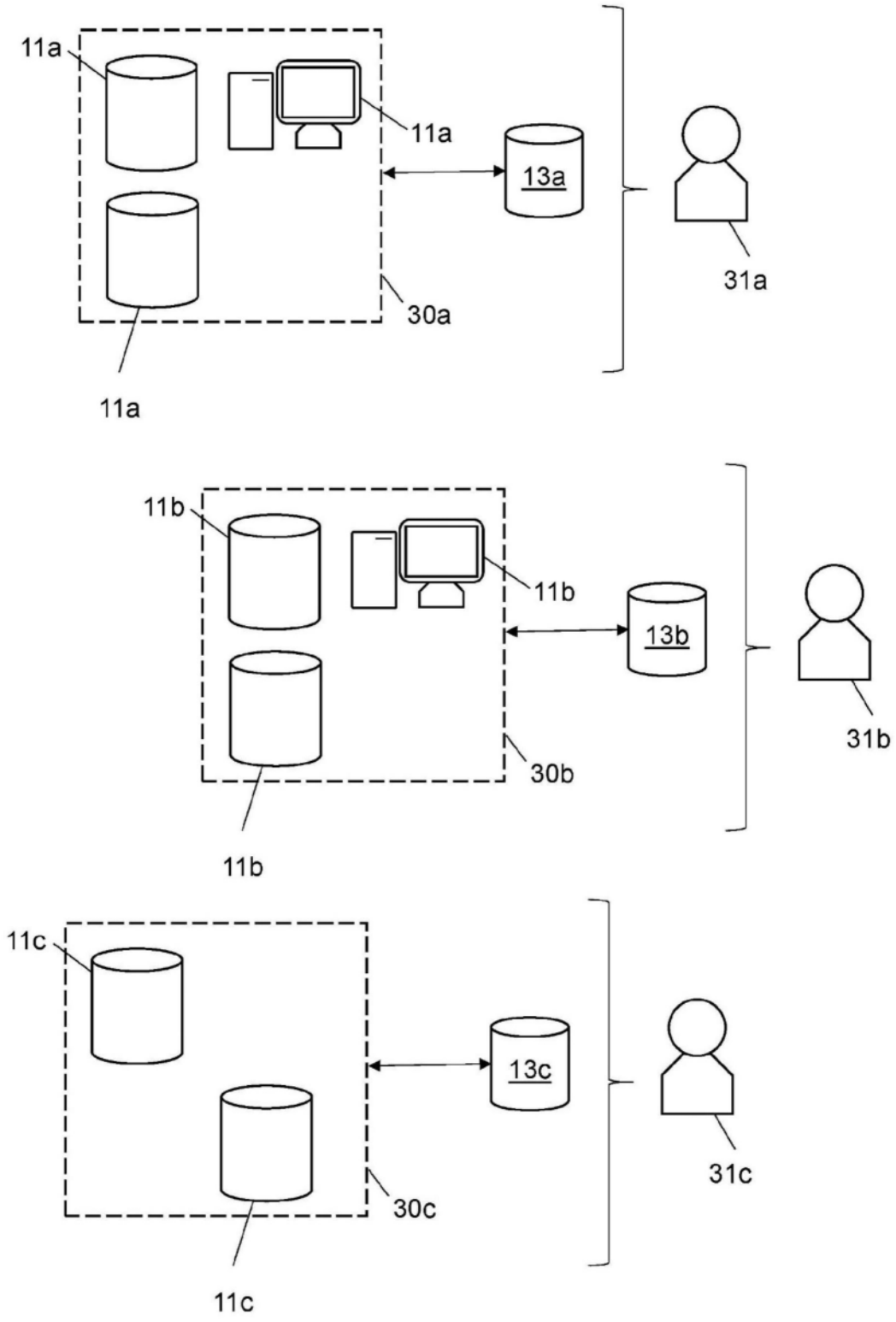

11a
11a
13a
30a
31a
11a
11b
11b
13b
30b
31b
11b
11c
13c
30c
31c
11c

图10A

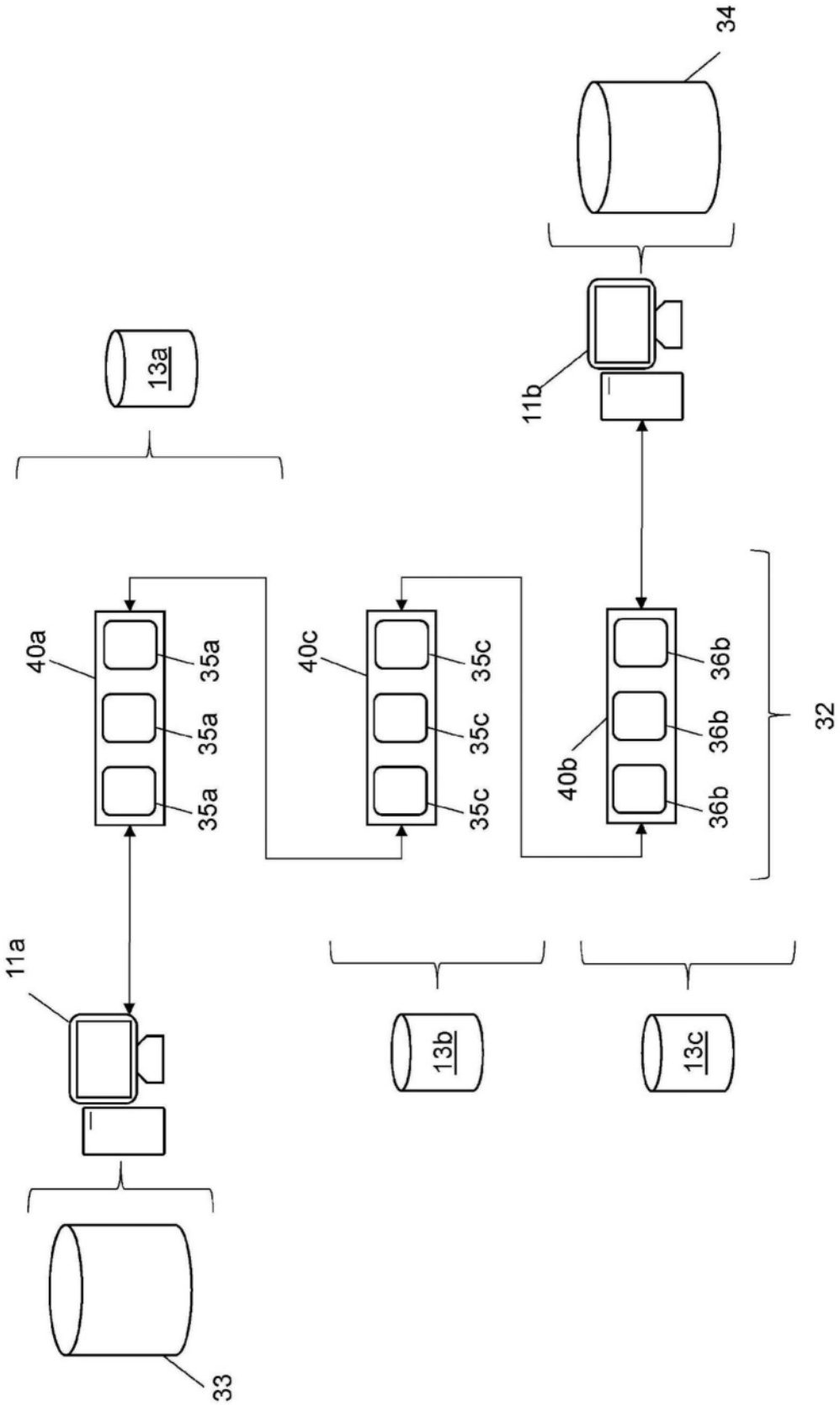

34
11b
13a
40a
35a
35a
35a
40c
35c
35c
35c
40b
36b
36b
36b
32
11a
13b
13c
33

图10B

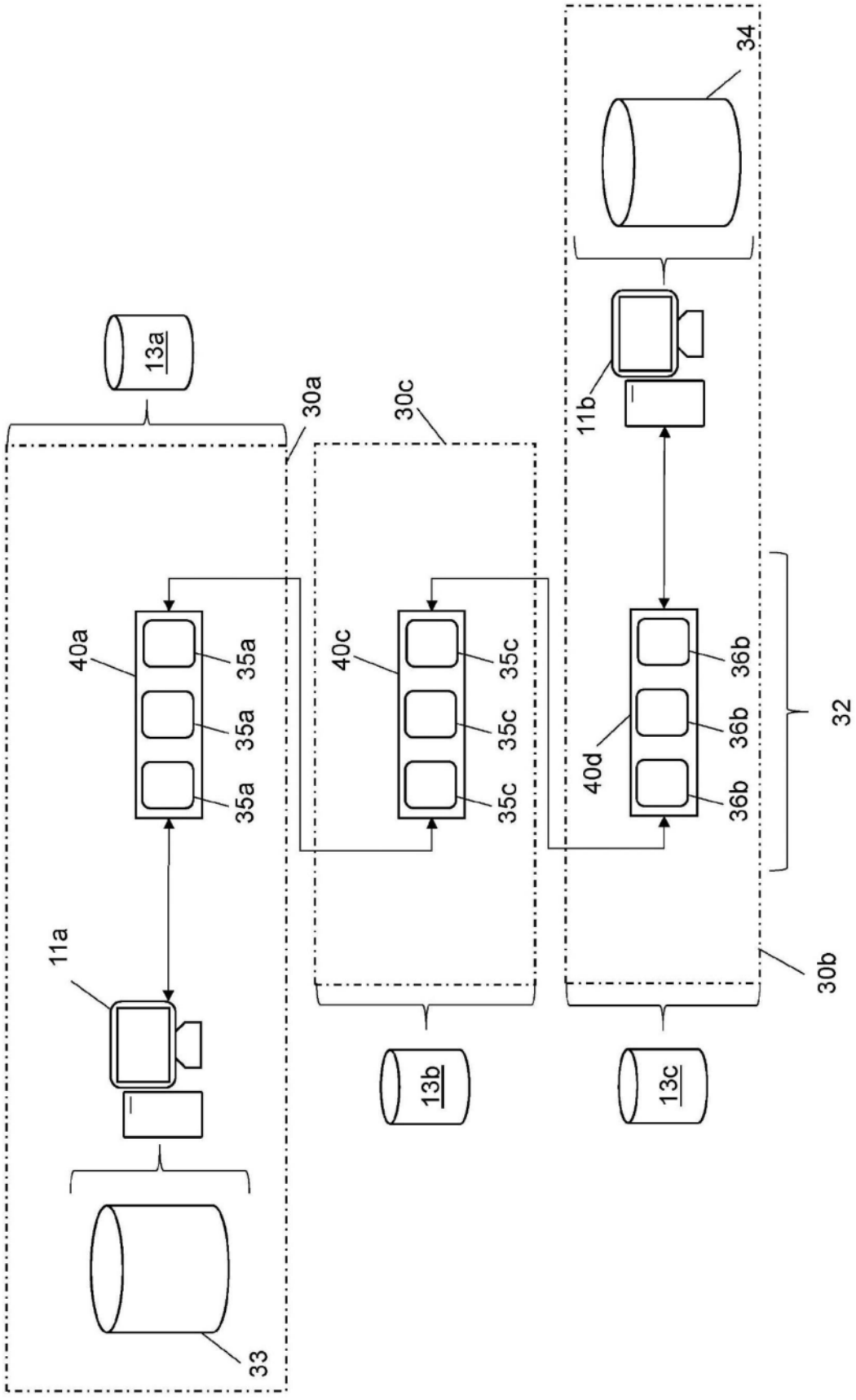

13a
30a
30c
34
11b
40a
35a
35a
35a
40c
35c
35c
35c
40d
36b
36b
36b
32
11a
30b
13b
13c
33

图11