

(12) 发明专利申请

(10) 申请公布号 CN 102483786 A

(43) 申请公布日 2012. 05. 30

(21) 申请号 201080040250. 8

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

(22) 申请日 2010. 08. 16

代理人 刘红 刘鹏

(30) 优先权数据

09170094. 8 2009. 09. 11 EP

(51) Int. Cl.

G06F 21/00 (2006. 01)

(85) PCT申请进入国家阶段日

2012. 03. 09

(86) PCT申请的申请数据

PCT/IB2010/053685 2010. 08. 16

(87) PCT申请的公布数据

W02011/030248 EN 2011. 03. 17

(71) 申请人 皇家飞利浦电子股份有限公司

地址 荷兰艾恩德霍芬

(72) 发明人 H. A. W. 范格斯特尔

M. 范纽文霍文

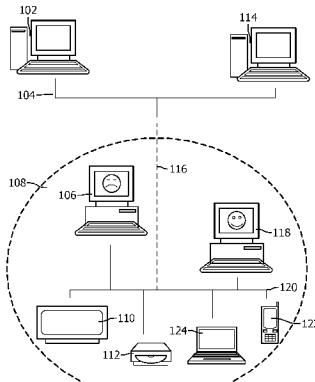
权利要求书 2 页 说明书 11 页 附图 4 页

(54) 发明名称

用于恢复域管理的方法和系统

(57) 摘要

本发明涉及用于为其中内容访问权限在一个或多个设备(106, 110, 112, 118, 122, 124)之间共享的域(108)恢复域管理的方法和系统，其中由第一域管理设备(106)执行并由这个第一域管理设备(106)停止域管理。第一域管理设备(106)在域注册服务器(114)上注册域(108)的一个或多个特征。在由第一域管理设备(106)停止域管理之后，第二域管理设备(118)向域注册服务器(114)发送请求，以获得管理域(108)的权限。域注册服务器(114)提供管理域(108)的权限以及域(108)的一个或多个注册的特征之中的至少一个特征。本发明进一步涉及在用于恢复域管理的系统中使用的域注册服务器(114)和域管理设备(106, 118)。



1. 一种为域(108)恢复域管理的方法(200),其中在所述域中在一个或多个设备(106, 110, 112, 118, 122, 124)之间共享内容访问权限,其中所述域管理由第一域管理设备(106, 304, 404)执行,所述方法包括以下步骤:

在第一域管理设备(106, 304, 404)停止所述域(108)的管理之前,由第一域管理设备(106, 304, 404)在域注册服务器(114, 312, 406)上注册(208, 332, 416)所述域(108)的一个或多个特征,

从第二域管理设备(118, 320, 408)发送(210, 334, 422)对于获得管理所述域的权限的请求给所述域注册服务器(114, 312, 406),

提供(212)管理所述域的权限以及所述域(108)的注册的一个或多个特征之中的至少一个特征给第二域管理设备(118, 320, 408)。

2. 根据权利要求1所述的恢复域管理的方法(200),其中如果所述域注册服务器(114, 312, 406)信任第二域管理设备(118, 320, 408),仅提供管理所述域的权限。

3. 根据权利要求1所述的恢复域管理的方法(200),其中管理所述域的权限是无限期权限或临时权限。

4. 根据权利要求3所述的恢复域管理的方法(200),其中如果所述域注册服务器(114, 312, 406)合理地信任第二域管理设备(118, 320, 408),仅提供管理所述域的临时权限,并且其中如果所述域注册服务器非常信任第二域管理设备(118, 320, 408),则所述域注册服务器(114, 312, 406)提供管理所述域的无限期权限。

5. 根据权利要求3所述的恢复域管理的方法(200),所述方法进一步包括以下步骤:

由第二域管理设备(118, 320, 408)请求(214, 426)管理所述域的临时权限的延长,

由所述域注册服务器(114, 312, 406)提供(216, 428)管理所述域的临时权限的延长给第二域管理设备(118, 320, 408)。

6. 根据权利要求5所述的恢复域管理的方法(200),其中如果所述域注册服务器(114, 312, 406)合理地信任第二域管理设备,仅提供管理所述域的临时权限的延长,其中如果所述域注册服务器(114, 312, 406)没有充分信任第二域管理设备,则所述域注册服务器(114, 312, 406)拒绝管理所述域的临时权限的延长,并且其中如果所述域注册服务器(114, 312, 406)非常信任第二域管理设备(118, 320, 408),则所述域注册服务器(114, 312, 406)通过提供管理所述域的无限期权限给第二域管理设备(118, 320, 408)来提供管理所述域的临时权限的延长。

7. 根据权利要求2、4或6所述的恢复域管理的方法(200),其中所述域注册服务器(114, 312, 406)在域历史数据文件中存储(314)一组活动,所述活动相对于所述域(108)在所述域注册服务器(114, 312, 406)上执行,并且其中所述域历史数据文件(314)由所述域注册服务器(114, 312, 406)分析,以便确定所述域注册服务器(114, 312, 406)对于第二域管理设备(118, 320, 408)所具有的信任量。

8. 根据权利要求7所述的恢复域管理的方法(200),所述方法进一步包括以下步骤:

通过在所述域注册服务器(114, 312, 406)中分析所述域历史数据文件(314),检测(218)与所述域(108)有关的欺诈,和

由所述域注册服务器(114, 312, 406)去激活第一域管理设备(106, 304, 404)进行的域管理和 / 或至第二域管理设备(118, 320, 408)的域管理。

9. 根据权利要求 1 所述的恢复域管理的方法(200),其中所述域(108)的一个或多个特征包括至少以下之一 :所述域(108)的名称,所述域(108)的策略,至所述域的绑定的列表,所述域(108)的设备和所述域(108)之间的绑定的一个或多个拷贝,所述内容和所述域(108)之间的绑定的一个或多个拷贝,属于所述内容的许可证的一个或多个拷贝,属于所述内容的安全密钥的一个或多个拷贝,或所述域的口令。

10. 根据权利要求 1 所述的恢复域管理的方法(200),其中所述域注册服务器(114, 312, 406)进一步被安排来创建新的域,所述方法进一步包括以下步骤 :

由第一域管理设备(106,304,404)在所述域注册服务器(114,312,406)上请求(202, 412)所述域(108)的创建,

在所述域注册服务器(114,312,406)上创建(204)管理所述域的权限,

提供(206,214)管理所述域的权限给第一域管理设备(106,304,404)。

11. 根据权利要求 1 所述的恢复域管理的方法(200),所述方法进一步包括以下步骤 :

由第一域管理设备(106,304,404)或第二域管理设备请求所述域注册服务器(114, 312, 406)撤消所述域(108)的注册的一个或多个特征中的至少一个特征的注册。

12. 根据权利要求 1 所述的恢复域管理的方法(200),其中所述域(108)是 Marlin 域,且第一域管理设备(106,304,404)和第二域管理设备(118,320,408)是 Marlin 设备。

13. 一种用于为域(108)恢复域管理的系统(302,402),其中在所述域中在一个或多个设备(106,110,112,118,122,124)之间共享内容访问权限,其中所述域管理由第一域管理设备(106,304,404)执行,所述系统包括 :

域注册服务器(114,312,406),被安排来注册所述域(108)的一个或多个特征,在第一域管理设备(106,304,404)停止所述域(108)的管理之前,从第一域管理设备(106,304, 404)接收所述一个或多个特征,和

第二域管理设备(118,320,408),被安排来发送对于获得管理所述域的权限的请求和接收管理所述域(108)的权限以及所述域(108)的一个或多个特征,

其中,响应于接收对于获得管理所述域的权限的请求,所述域注册服务器(114,312, 406)进一步被安排来给第二域管理设备(118,320,408)提供管理所述域的权限以及所述域的注册的一个或多个特征中的至少一个。

14. 一种域注册服务器(114,312,406),用于在权利要求 13 的系统(302,402)中使用。

15. 一种域管理设备(106,118,304,320,404,408),用于在权利要求 13 的系统(302, 402)中使用。

## 用于恢复域管理的方法和系统

### 技术领域

[0001] 本发明涉及用于为其中内容访问权限在一个或多个设备之间共享的域恢复域管理的方法和系统，其中域管理由第一域管理设备来执行。本发明进一步涉及在用于恢复域管理的系统中使用的域注册服务器和域管理设备。

### 背景技术

[0002] “Marlin (马林)”是由 Marlin Developer Community (马林开发者社区) 创建的开放标准、内容共享技术平台。Marlin 提供数字版权管理 (Digital Rights Management) 平台，其中提供可以在设备和计算机程序中使用的访问控制技术。通过许可和加密，内容提供者、出版者和 / 或版权持有者可以根据 Marlin 标准来保护所分发的内容。该标准的主要文件是由 Marlin Engineering Group (马林工程组) 创建并由 Marlin Community (马林社区) 分发的“Marlin-Core System Specification (马林 - 核心系统规范)”。

[0003] 如果支持 Marlin 标准的设备的内容提供者处具有帐户，则该设备能够利用 Marlin 技术从内容提供者下载内容。如果下载内容的许可证 (license) 允许播放该内容，以及如果该设备具有解密密钥，则该 Marlin 设备可以向该设备的用户播放该内容。

[0004] Marlin 标准引入 Marlin 域的概念。Marlin 域是共享一组受保护内容的一组 Marlin 设备。Marlin 域中的所有设备对于该域中的内容具有相同的访问权限。获得的 Marlin 内容与许可证和解密密钥一起被绑定到该域而不是被绑定到个别设备。

[0005] 在 Marlin 域中，这些设备中的一个设备是域管理器。该域管理器通过绑定新的设备到该域或释放在该域和绑定到该域的设备之间的绑定来控制该域。内容提供者信任该域管理器并要求该域管理器例如通过限制被绑定到该域的设备的数量来防止滥用 (misuse)。Marlin 域的设备连接到共享网络，或这些设备定期共享该网络。例如，用户可能具有家庭网络，其大多数数字设备被永久地连接到该家庭网络。这些设备中的一个设备是域管理器，优选地，永久连接的设备。该用户也可能具有便携式数字设备，当这些设备位于家中的时候，这些设备连接到该网络。这些便携式设备在它们连接到家庭网络的时候获得内容、许可证和解密密钥。如果这些便携式设备没有连接到家庭网络，因为它们在早期获得许可证和解密密钥，所以它们能够播放内容。

[0006] 如果活动域管理软件驻留于其上的设备发生故障，该域将被损坏并可能丢失。诸如将设备、内容、许可者和解密密钥绑定到域之类的中央域管理功能被停止 (discontinue)。很多信息被丢失，诸如在内容和域之间的绑定和 / 或在设备和域之间的绑定。现今，用于克服域管理器的损失的唯一解决方案是创建新的域，其中新的域必须成为原域的拷贝。这是繁琐的任务，因为绑定必须手动恢复，并且必须再次联系内容提供者，以获得许可来绑定该内容到新的域。然而，如果没有接收到针对该内容的新的付费，内容提供者不愿意提供许可来绑定该内容到新的域。内容提供者几乎不可能查明：旧域是否真的丢失，并决定新的域是可以被信任还是欺诈的。

## 发明内容

[0007] 本发明的目的是可靠地恢复发生故障的域。

[0008] 本发明的第一方面提供如权利要求 1 中定义的恢复域管理的方法。本发明的第二方面提供如权利要求 13 中定义的用于恢复域管理的系统。有利的实施例定义在从属权利要求中。

[0009] 根据本发明的第一方面，提供用于为其中内容访问权限在一个或多个设备之间共享的域恢复域管理的方法，其中域管理由第一域管理设备来执行。该方法包括以下步骤：在第一域管理设备停止域的管理之前，由第一域管理设备在域注册服务器上注册域的一个或多个特征。该方法进一步包括从第二域管理设备向域注册服务器发送对于获得管理域的权限的请求的步骤。在该方法的进一步步骤中，域注册服务器给第二域管理设备提供管理域的权限以及所注册的一个或多个特征中的至少一个。

[0010] 该方法防止域的丢失以及与该域有关的重要数据的丢失。最初在管理该域的第一域管理设备在域注册服务器上注册一个或多个特征。由第一域管理设备提供的信息存储在域注册服务器上。稍后，可以由第一域管理设备停止设备管理，这是因为它发生故障、被损坏或例如被用户丢弃。由于域管理的停止，所以与该域有关并被存储在第一域管理设备上的重要信息丢失。然而，域注册服务器存储必须被用于恢复域的一个或多个重要的域特征。能够管理该域的另一设备作为第二域管理设备进行安装。为了得到运行在第二域管理设备上的域，它必须向域注册服务器发送对于获得管理该域的权限的请求。随后，域注册服务器可以向第二域管理设备提供管理该域的权限。与管理该域的权限一起，域注册服务器提供该域的注册的一个或多个特征中的至少一个。第二域管理设备使用至少一个接收的该域的特征来建立最初由第一域管理设备管理的域。按照上面给出的步骤，防止运行域所需的重要数据的丢失。

[0011] 域注册服务器最好由内容提供者所信任的信任方来运行。由第一域管理设备注册的信息最好安全地进行存储并加以保护以防止欺诈攻击。

[0012] 第一域管理设备和第二域管理设备将经由数据网络与域注册服务器通信。注册一个或多个特征、发送请求、提供管理域的权限和 / 或拒绝管理域的权限将通过数据网络在数据消息中从这些域管理设备传送到域注册服务器，或者反之亦然。

[0013] 没有必要的是：因为域管理软件不能在第一域管理设备上再起作用，所以第一域管理设备停止该设备的管理。在另一实施例中，第二域管理设备想从第一域管理设备接管域的管理。为了由第一域管理设备停止域管理，第二域管理设备请求第一域管理设备放弃其任务，或域注册服务器向第一域管理设备发送请求来停止域的管理。

[0014] 在一个实施例中，仅在域注册服务器信任第二域管理设备时，域注册服务器才提供管理域的权限。在进一步实施例中，如果域注册服务器不信任第二域管理设备，则由该域注册服务器明确拒绝管理域的权限。信任域管理设备意味着：域注册服务器信任第二域管理设备到足够的程度。因此，不信任设备意味着：没有足够的信任。

[0015] 除了是用于存储域的一个或多个特征的服务器之外，域注册服务器还是防止滥用和欺诈的中央服务器。域注册服务器有可能检测到来自域管理设备的对于获得管理域的权限的请求的不信任。如果设备不被信任，则这是可能欺诈或可能滥用的指示。在这样的情况下，最好不提供管理域的权限，这是因为内容提供者只愿意在域注册服务器抵御滥用和

欺诈时提供内容给通过使用这个域注册服务器可以恢复的域。例如,如果第二域管理设备获得管理域的权限并且被认为发生故障的第一域管理设备联系域注册服务器,对于域注册服务器来说毋庸置疑的将是:第一域管理设备或第二域管理设备可能不再被信任。在这种情况下,两个域管理设备似乎在管理该域,而这不被内容提供者允许。在另一示例中,当域注册服务器在短时间内接收到多个恢复域的请求时,明显的是发送这些请求的域管理设备可能不被信任。

[0016] 在一个实施例中,管理域的权限是无限期或临时(temporal)权限。提供管理域的无限期权限或临时权限的可能性导致给不同类型的域管理设备提供管理域的不同权限。域注册服务器能够区分不同类型的第二域管理设备。域注册服务器例如可以给已依据最新的数字版权管理标准安装域管理软件的第二域管理设备提供管理域的无限期权限,或可以给安装较旧软件的设备提供临时权限。在另一实施例中,内容提供者可以要求:正在运行恢复设备的域管理服务器可以只拥有管理域的临时权限。内容提供者可能喜欢在域管理设备停止之后恢复域管理的概念,但他们可能仅通过引入附加条件来支持这个概念:仅在管理域的临时权限的基础上可以恢复域。

[0017] 在进一步实施例中,如果域注册服务器合理地信任第二域管理设备,则域注册服务器提供管理域的临时权限。如果域注册服务器非常信任第二域管理设备,则域注册服务器提供管理域的无限期权限。在另一实施例中,如果域注册服务器并不充分信任第二域管理设备,则明确拒绝管理域的权限。

[0018] 如前所述,授予管理域的无限期或临时权限的决定基于域注册服务器信任域管理设备的程度的事实引入额外的时间点,在这个时间点上域注册服务器能够打击欺诈和滥用。这是早先的决定可以根据新的见解进行纠正的时间点。例如,在一个实施例中,第一域注册服务器可能已修复,并且可能已在第一域注册服务器上卸载域管理软件。在移除域管理软件的过程期间,第一域管理设备给域注册提供软件移除的通知。第一域管理设备上软件移除的知识导致域注册服务器更加信任第二域管理设备。

[0019] 在另一实施例中,该方法进一步包括由第二域管理设备请求延长管理域的临时权限的步骤,并且进一步包括由域注册服务器向第二域管理设备提供管理域的临时权限的延长的步骤。

[0020] 只有管理域的临时权限的第二域管理设备必须请求延长,否则它在管理域的临时权限终止的时刻之后将无法继续域管理。此外,接收延长管理域的临时权限的请求通知域注册服务器:第二域管理设备仍在操作并愿意管理域。域注册服务器的知识因而由于接收到该请求而被更新。

[0021] 在进一步实施例中,如果域注册服务器合理地信任第二域管理设备,仅提供管理域的临时权限的延长。如果域注册服务器非常信任第二域管理设备,它将通过提供无限期权限来延长管理域的临时权限。如果域注册服务器并不充分信任第二域管理设备,则它将拒绝管理域的临时权限的延长。

[0022] 具有管理域的临时权限的域管理设备必须请求延长这个权限的事实引入可以由域注册服务器使用来打击滥用和欺诈的另一安全步骤。授予管理设备的无限期权限的决定不能被取消,即使这似乎是不正确的决定。通过拒绝管理域的临时权限的延长,域注册服务器有能力来消除不正确决定的影响或结束由欺诈域管理设备进行的域的管理。

[0023] 在一个实施例中,域注册服务器在域历史数据文件中存储对于域注册服务器执行的与域有关的一组活动。域注册服务器执行域历史数据文件的分析,以便确定域注册服务器信任第二域管理设备的程度。

[0024] 分析域历史数据文件的域注册服务器也能够决定第二域管理设备是否可以被信任。域历史数据文件提供可靠信息,其中授予可能临时的权限的决定可以基于该可靠信息。基于可以注册在域历史数据文件中的分配正的或负的信任值给具体情况的一组规则,域注册服务器可以为第二域管理设备计算信任值。所计算的信任值可以与预定义值进行比较。如果所计算的值低于第一预定义值,则没有足够的信任。如果所计算的值高于第二预定义值,则具有很多信任。否则,具有合理程度的信任。

[0025] 因为域和内容提供者之间的关系基于信任,所以参与域的维护的附加服务器必须被内容提供者信任。通过使用和分析域历史数据文件,内容提供者可以相信:域注册服务器正在使用可靠的处理来确定域管理设备的信任,并因而可以更信任域注册服务器和域。内容提供者和域之间更多的信任可以导致例如从内容提供者接收在该域中绑定更多设备的许可或针对该内容的较低价格。

[0026] 存储在域历史数据文件中的信息可以包括与以下活动中的一个或多个有关的信息:注册一个或多个特征,接收获得管理域的权限的请求,以前分析的结果,提供和/或拒绝管理域的权限。例如,这些活动的信息项是:活动发生的时刻,与之进行通信的域管理设备,哪个确切信息被注册,指向其中存储一个或多个特征的指针等。应当注意:域历史数据文件中的信息不限于上面提到的示例。基本上,存储在域历史数据文件中的信息是打击滥用和欺诈所需的信息。

[0027] 数据历史文件的分析可以包括所有类型的统计分析,例如,接收到的对于获得管理域的权限的请求的数量,获得管理权限的请求到达的频率,获得管理域的权限的拒绝的数量等。在另一分析中,域注册服务器可以建立被认为发生故障的域管理设备的列表,其包括自从这些设备被认为发生故障的时候以来的信息。这个信息可以与相同的或其它的域管理设备试图联系域注册服务器的时刻的时间戳相结合。分析的实施例并不限于上面所提到的具体示例。基于使用人工智能的分析是另一示例。或者,在另一示例中,域注册服务器的运营商参与分析。

[0028] 在另一实施例中,该方法进一步包括通过分析域历史数据文件来检测与域有关的欺诈的步骤。这个分析由域注册服务器来执行。该方法进一步包括由域注册服务器去激活(inactivate)由第一域管理设备和/或第二域管理设备进行的域管理。若干解决方案可以用于去激活域管理。在一个实施例中,在检测到由各自的第一和/或第二域管理设备实施的欺诈之后,从域注册服务器向第一和/或第二域管理设备发送域去激活代理。域去激活代理是在各自的第一和/或第二域管理设备上自动执行的一段程序代码。域去激活代理的程序代码的自动执行导致由各自的第一和/或第二域管理设备进行的域管理的去激活。

[0029] 欺诈的检测和域去激活代理的发送改善恢复域管理的方法的可靠性。从域注册服务器向域管理设备发送域去激活代理是欺诈的并导致欺诈的终止。

[0030] 如在上文的实施例中所述的,域历史数据文件的分析可以包括将从域管理设备接收到数据的时间戳与代表自从域管理设备被认为发生故障的时候以来的时刻的时间戳进行匹配。这在第一域管理设备联系域注册服务器时可能导致由第一域管理设备实施的欺诈

的检测,尽管域注册被认为长时间发生故障。如果在向第二域管理设备提供管理域的权限之后在短时间内接收到对于获得管理域的权限的许多请求,这也可能导致由第二域管理设备实施的可能欺诈的检测。

[0031] 域去激活代理在接收到域去激活代理的域管理设备上执行。域去激活代理包含由接收域去激活代理的处理器执行的指令。这些指令可以删除例如管理域的权限或可以调节在接收域管理设备中设置的变量的值。

[0032] 在进一步实施例中,域的一个或多个特征包括下列项中的至少一个:域的名称,域的策略,绑定到域的设备的列表,域的设备和域之间的绑定的一个或多个拷贝,内容和域之间的绑定的一个或多个拷贝,属于内容的许可证的一个或多个拷贝,属于内容的安全密钥的一个或多个拷贝,或域的口令。应当注意:该列表并不限制可以在域注册服务器上注册的特征的类型。基本上,域管理设备具有的所有的域相关信息可以在域注册服务器上进行注册。在一个实施例中,在第二域注册服务器上恢复域所需的所有信息被注册在域注册服务器上。

[0033] 在另一实施例中,域是 Marlin 域,并且第一和第二域管理设备是 Marlin 设备。

[0034] 在恢复域管理的方法的进一步实施例中,域注册服务器进一步被安排来创建新的域。该方法进一步包括以下步骤:由第一域管理设备在域注册服务器上请求域的创建,在域注册服务器中创建管理域的权限,并向第一域管理设备提供管理域的权限。

[0035] 这个实施例增加域的使用的安全性。域注册服务器创建域,并且域管理服务器只获得管理域的权限。事实上,域注册服务器是域的所有者/创建者,并且仅分发管理域的权限给另一设备。相比于撤销域的所有权/创建权而言,撤销管理域的权限是更容易的。

[0036] 在一个实施例中,该方法进一步包括由第一或第二域管理设备请求域注册服务器撤消注册的域的一个或多个特征中的至少一个特征的注册。第一或第二域管理设备可以释放放在域管理设备和域之间的绑定。例如,当一个设备想从第一域移到第二域时,在第一域和该设备之间的绑定必须通过请求域注册服务器撤消以前注册的一些特征的注册来释放。域注册服务器将因而尽可能是最新的,这在停止初始的域管理设备的域管理之后协助域的恢复。

[0037] 根据本发明的第二方面的系统包括被安排来注册域的一个或多个特征的域注册服务器。在第一域管理设备停止域的管理之前,从第一域管理设备接收一个或多个特征。该系统进一步包括被安排来发送对于获得管理域的权限的请求的第二域管理设备。第二域管理设备进一步被安排来接收管理域的权限以及域的一个或多个特征。响应于接收到对于获得管理域的权限的请求,域注册服务器进一步被安排来向第二域管理设备提供管理域的权限以及域的注册的一个或多个特征中的至少一个。根据本发明的第二方面的系统提供与根据本发明的第一方面的方法相同的益处。

[0038] 本发明的这些和其它方面从下文描述的实施例中是显而易见的,并将参考这些实施例来阐述。

## 附图说明

[0039] 在附图中:

图 1 示意性地显示具有设备、内容提供者和域注册服务器的域,

图 2 示意性地显示恢复域管理的方法,

图 3 示意性地显示用于恢复域管理的系统的第一实施例,

图 4 示意性地显示用于恢复域管理的系统的第二实施例。

[0040] 应当注意:在不同的附图中利用相同的参考数字表示的项具有相同的结构特征和相同的功能或者是相同的信号。如果这样的项的功能和 / 或结构进行解释了,在具体实施方式中没有必要重复其解释。

## 具体实施方式

[0041] 第一实施例显示在图 1 中。多个设备 106、110、112、118、122、124 连接到局域网 120。这些设备 106、110、112、118、122、124 是用户家用的电子数字设备。局域网 120 可以是有线网络、无线网络或二者的组合。这些设备 106、110、112、118、122、124 是域 108 的成员,或者换言之,它们被绑定到该域。域 108 可以是 Marlin 域,并且这些设备 106、110、112、118、122、124 可以是 Marlin 设备。

[0042] 设备 106 是在个人计算机上实现的第一域管理设备。设备 118 是也在个人计算机上实现的第二域管理设备。域管理设备 106、118 能够运行管理域 108 的软件。在 Marlin 域的情况下,域管理软件根据 Marlin 规范来实现。

[0043] 设备 110 是能够播放电影和音频的电视。设备 112 是能够播放电影、音频和运行游戏的游戏机。设备 124 是能够播放电影、音频、运行游戏和运行程序的便携式计算机。设备 122 是能够执行小型应用程序和播放音频的移动电话。如果移动电话 122 和 / 或便携式计算机 124 不在局域网 120 的附近,则它们变成从这个网络断开。虽然被断开,但是移动电话 122 和便携式计算机 124 仍然被绑定到域 108。

[0044] 局域网 120 具有与广域网 104 的连接 116。广域网 104 将局域网连接到内容提供者的内容服务器 102 和连接到域注册服务器 114。域注册服务器 114 由至少被内容提供者信任并且一般被内容的购买者广泛信任的信任方来维护。内容服务器 102 可以提供利用 Marlin 数字版权管理技术来保护以防滥用的数字内容。

[0045] 域 108 最初由第一域管理设备 106 来管理。第二域管理设备 118 并没有作为域管理器在使用,并且最初只是域 108 的普通成员。在一个实施例中,第一域管理设备 106 创建域 108 并向内容服务器 102 请求在域 108 中使用从内容提供者购买的内容的许可。在另一实施例中,第一域管理设备 106 向域注册服务器 114 发送创建域 108 的请求,并且域注册服务器 114 向第一域管理设备 106 提供管理域 108 的许可。内容提供者信任域注册服务器 114 作为域的创建者,并且自动地提供在域 108 的所有设备 106、110、112、118、122、124 上播放 / 使用 / 执行从内容服务器 102 获得的内容的许可。

[0046] 例如,通过提供域绑定许可证给这些设备 110、112、118、122、124 或通过给所有这些设备 110、112、118、122、124 提供共享域口令,第一域管理设备 106 将这些设备 110、112、118、122、124 绑定到该域。当用户使用这些设备 106、110、112、118、122、124 之一时,他可以开始与内容服务器 102 联系,以获得内容,例如,视频、电影、音乐文件、游戏、移动电话应用程序或软件。该内容由内容服务器 102 加密并被传送到获得设备。获得设备或第一域管理设备 106 获得播放 / 使用 / 执行该内容所需的许可证和解密密钥。许可证和解密密钥被绑定到该域 108,而不是被绑定到个别设备 106、110、112、118、122、124。在一个实施例中,第

一域管理设备存储并管理与域 108 的内容相关的该组许可证和解密密钥，并向该域的设备 106、110、112、118、122、124 提供许可证和解密密钥。在另一实施例中，每个个别设备 106、110、112、118、122、124 存储许可证和密钥的子集并与该域 108 的所有这些设备共享这些许可证和密钥。

[0047] 如果这些设备 106、110、112、118、122、124 之一想播放 / 使用 / 执行该内容，则它可能已存储了内容、许可证和解密密钥，而如果它被绑定到与许可证和解密密钥所绑定至的同一域并且满足许可策略，则它可以播放 / 使用 / 执行该内容。在另一实施例中，这些设备 106、110、112、118、122、124 必须从另一设备 110、112、118、122、124 或从第一域管理设备 106 下载内容和 / 或许可证和 / 或解密密钥。

[0048] 刚好在域的创建之后或在稍后的时刻，第一域管理设备 106 发送消息给域注册服务器 114，其中第一域管理设备 106 利用该消息在域注册服务器 114 上注册域 108 的一个或多个特征。一个或多个特征可以包括以下之一：域 108 的名称，域 108 的策略，绑定到域的设备 110、112、118、122、124 的列表，设备 110、112、118、122、124 和域 108 之间的绑定的拷贝，存储在第一域管理设备 106 上的许可证和解密密钥的拷贝，域口令等。取决于用于创建域 108 的特定的数字版权管理技术，这些和其它特征对于恢复域管理是重要的。第一域管理设备 106 在域注册服务器 114 中注册恢复域管理所需的至少一个或多个特征。在一个实施例中，域注册服务器 114 是域的创建者，并且第一域管理设备 106 必须只注册域注册服务器 114 尚未意识到的那些重要特征。

[0049] 如果域 108 在操作，第一域管理设备 106 可以绑定新的设备到这个域。新的内容连同许可证和解密密钥一起也可以被绑定到该域 108。在一个实施例中，第一域管理设备 106 定期在域注册服务器 114 上注册域 108 的一个或多个特征，以致存储在域注册服务器 114 上的信息代表该域 108 的实际状态。

[0050] 不久，第一域管理设备 106 出现故障，并导致由第一域管理设备进行的域管理的停止。这意味着：域 108 被损坏和 / 或发生故障。例如，没有新的设备可以被绑定到域 108，没有当前的域管理设备 110、112、118、122、124 可以离开该域，仅存储在第一域管理设备 106 上的内容、许可证和解密密钥被丢失，以及由第一域管理设备 106 保持的域 108 的成员设备 110、112、118、122、124 的列表被丢失。例如，如果用户想在便携式计算机 124 上观看电影，而该电影的许可证和解密密钥存储在第一域管理设备 106 上，这是麻烦的情况并且可能导致严重的问题。

[0051] 用户可以决定：已在其家中使用的个人计算机 118 必须变成域管理器。个人计算机 118 能够运行域管理软件，并且用户在个人计算机 118 中激活这个软件。必须变成第二域管理设备 118 的个人计算机 118 因而联系域注册服务器 114 并请求管理域 108 的权限。

[0052] 响应于接收对于获得管理域 108 的权限的请求，域注册服务器 114 决定它或信任或不信任第二域管理设备 118。有关是否信任第二域管理设备 118 的决定可以基于例如用于授予管理域 108 的权限的规则或基于由第二域管理设备提供的信息。例如，它可以是在第一域管理设备 106 的一个或多个特征的注册之后在一周内不允许向第二域管理设备 118 提供管理域 108 的权限的规则。这在如此短的时间内多次使用域注册服务器 114 的服务来获得对于域 108 在操作的另一域管理设备时似乎是欺诈。这可以是一次只信任一个另一域管理设备的进一步规则。

[0053] 如果第二域管理设备 118 被域注册服务器 114 信任，则管理域 108 的权限被提供给第二域管理设备 118。与管理域 108 的权限一起，第二域管理设备 118 接收由第一域管理设备 106 在域注册服务器 114 上先前注册的域 108 的注册的一个或多个特征。所接收到的一个或多个特征由第二域管理设备 118 用来恢复域 108 的管理。一个或多个特征被装载到域管理软件中。

[0054] 如果第二域管理设备 118 不被域注册服务器 114 信任，则域注册服务器 114 拒绝第二域管理设备 118 管理域 108 的权限。在一个实施例中，拒绝的通知可以从域注册服务器 114 发送到第二域管理设备 118，或在另一实施例中，域注册服务器 114 不回答对于获得管理该设备的权限的请求。

[0055] 在另一实施例中，所提供的管理域 108 的权限是临时权限。管理域 108 的临时权限包括对于有限的时间管理这个域 108 的权限或在指定日期之前管理的权限。正好在第二域管理设备 118 被允许管理该域的时段结束之前，第二域管理设备 118 必须请求在域注册服务器 114 上管理域 108 的临时权限的延长。响应于接收到延长管理域 108 的临时权限的请求，域注册服务器 114 必须再次决定它信任第二域管理设备 118 到什么程度。如果没有信任的话，则拒绝延长。如果具有超过特定水平的信任，则域注册服务器 114 提供管理域 108 的权限的延长。如果完全信任第二域管理设备 118，则域注册服务器 114 可以提供管理域的无限期权限。

[0056] 第二实施例显示在图 2 中。图 2 示意性地显示恢复域的域管理的方法 200。该方法 200 用于具有在多个设备之间共享内容的域的环境中。该域由第一域管理设备来管理。在步骤 208，第一域管理设备在域注册服务器上注册域的一个或多个特征。在以后的时间，第一域管理设备例如由于故障而停止域的管理。在步骤 210，第二域管理设备向域注册服务器发送对于获得管理域的权限的请求。响应于接收到对于获得管理域的权限的请求，在步骤 212，域注册服务器向第二域管理设备提供管理域的权限。与提供管理域的权限一起，提供域的一个或多个注册的特征提供给第二域管理设备。

[0057] 在步骤 212 的可选实施例中，仅在域注册服务器信任第二域管理设备时，域注册服务器才提供管理域的权限给第二域管理设备。如果域注册服务器并不信任第二域管理设备，则域注册服务器拒绝管理域的权限。

[0058] 在方法 200 的另一实施例中，域注册服务器创建域。在步骤 208 之前，执行附加的方法步骤。在步骤 202，第一域管理设备在域注册服务器上请求域的创建。响应于接收到创建请求，域注册服务器在步骤 204 创建域和管理域的权限。在步骤 206，管理域的权限被提供给第一域管理设备。

[0059] 在另一实施例中，提供给第二域管理设备的管理域的权限是临时权限。在步骤 214，第二域管理设备在域注册服务器上请求管理域的临时权限的延长。在步骤 216，域注册服务器提供管理域的临时权限的延长。

[0060] 在步骤 216 的可选实施例中，进一步确定：域注册服务器是否仍信任第二域管理设备。如果没有足够的信任，则域注册服务器拒绝管理域的临时权限的延长。如果具有合理的信任量，则域注册服务器给第二域管理设备提供管理域的临时权限的延长。如果域注册服务器完全信任第二域管理设备，则提供管理域的无限期权限给第二域管理设备。

[0061] 在另一实施例中，域注册服务器在域历史数据文件中存储与域相关的域注册服务

器所执行的所有活动。域历史数据文件被分析,以便确定域注册服务器对于第二域管理设备具有的信任量。恢复域管理的方法 200 进一步包括通过分析域历史数据文件来检测与该域有关的欺诈。

[0062] 域历史数据文件的分析可以包括将从域管理设备接收数据的时间戳与代表自域管理设备被认为已出现故障的时候起的时刻的时间戳进行匹配。如果第一域管理设备联系域注册服务器,而第一域管理设备被认为已长时间出现故障,则这可能导致由第一域管理设备从事的欺诈的检测。如果在向第二域管理设备提供管理域的权限之后在短时间内接收到许多对于获得管理域的权限的请求,这也可能导致由第二域管理设备从事的可能欺诈的检测。在短时间内接收到许多对于获得管理域的权限的请求表明:大概,这些请求的所有提出者可能不被信任。应当注意:检测欺诈可以基于以规则为基础的系统,其检测其中域管理设备之一可能是欺诈的具体情况。

[0063] 如果由第一域管理设备和 / 或第二域管理设备进行的欺诈被检测到,则域注册服务器在步骤 220 向各自的第一域管理设备和 / 或第二域管理设备发送域去激活代理 (inactivation agent)。第一域管理设备和 / 或第二域管理设备具有处理器,并且域去激活代理是在各自的第一域管理设备和 / 或第二域管理设备的处理器上执行的一段程序代码。该段程序代码的执行的结果是由各自的第一域管理设备和 / 或第二域管理设备进行的域管理的去激活。该段程序代码可以包括在域管理设备上删除管理域的权限的指令。该段程序代码也可以包括改变变量的值的指令,其中变量例如是表明域管理设备可以管理该域到何时的管理域的临时权限的变量。通过将在其之前域管理设备可以管理域的日期设置在过去的时刻,管理域的临时权限已期满。应当注意:这些段程序代码段的指令的示例不限于在实施例中给出的示例。每一个具体的数字版权管理技术要求它自己特定的技术来去激活域的管理。

[0064] 第三实施显示在图 3 中。图 3 示意性地显示用于恢复域管理的第一系统 302。第一系统 302 包括第一域管理设备 304、域注册服务器 312 和第二域管理设备 320。第一域管理设备和第二域管理设备包括:用于在域注册服务器 312 上注册由各自的域管理设备管理的域的一个或多个特征的注册装置 306、322;用于向域注册服务器 312 发送请求以获得管理域的权限的请求发送器 308、324,并且两个域管理设备包括用于接收管理域的权限以及接收域的一个或多个特征的管理权限接收器 310、326。域注册服务器 312 包括用于存储域历史数据文件 314 以及域的一个或多个特征的数据存储设备 316、用于从一个或多个域管理设备接收一个或多个特征的注册的一个或多个特征接收器 318 以及用于从一个或多个域管理设备接收对于获得管理域的权限的请求的请求接收器 330。域注册服务器也包括管理权限发送器 328,用于提供或拒绝管理域的权限以及提供一个或多个注册的域的特征给一个或多个域管理设备。

[0065] 在典型的使用情况中,第一域管理设备 304 正在管理该域。该域包括共享一组内容的多个设备(未示出)。第一域管理设备 304 已绑定多个设备到该域,并至少存储绑定到该域的许可证和解密密钥的子集。在特定的时刻,第一域管理设备 304 从其注册装置 306 发送注册消息 332 到域注册服务器 312 的一个或多个特征接收器 318。注册消息预定用于注册由第一域管理设备 304 管理的域的一个或多个特征。域注册服务器 312 在数据存储设备 316 中存储所接收的一个或多个特征,并利用与一个或多个特征的接收相关的信息来更

新域历史数据文件 314, 例如, 时间戳被注册, 并且指向数据存储设备 316 中的一个或多个特征的指针被注册在域历史数据文件 314 中。包含在注册消息中的一个或多个特征是例如被绑定到域的设备以及存储在第一域管理设备 304 上的许可证和解密密钥的拷贝的列表。

[0066] 在稍后的时刻, 第二域管理设备 320 在第一域管理设备 304 发生故障之后联系域注册服务器 312。第二域管理设备 320 的请求发送器 324 给域注册服务器 312 的请求接收器 330 发送请求消息。随后, 域注册服务器 312 决定是否信任第二域管理设备。这可以通过分析域历史数据文件 314 来完成。结论可能是: 第二域管理设备被信任, 这是因为第一域管理设备似乎已长时间在操作并很可能发生故障。如果域注册服务器 312 信任第二域管理设备 320, 则管理权限发送器 328 向第二域管理设备 320 的管理权限接收器 326 发送提供消息。这个提供消息给第二域管理设备 320 提供管理域的权限, 并提供存储在数据存储设备 316 中的注册的域的一个或多个特征。随后, 域注册服务器 312 利用与接收请求消息和发送提供消息有关的信息来更新域历史数据文件。

[0067] 稍后, 第一域管理设备 304 的请求发送器向域注册服务器 312 的请求接收器 318 发送请求消息, 以获得管理与对其而言管理域的权限最近已被提供给第二域管理设备 320 的那个域相同的域的权限。例如, 用户可能已修复第一域管理设备 304, 并且在修复之后, 域管理软件联系域注册服务器 312。通过分析域历史数据文件 314, 域注册服务器 312 发现: 第一域管理设备 304 被认为发生故障并且可能不是用于管理该域的域管理设备。随后, 管理权限发送器 328 向第一域管理设备 304 的管理权限接收器 310 发送包含管理域的权限的拒绝的消息。

[0068] 第四实施例显示在图 4 中。图 4 示意性地显示用于恢复域管理的第二系统 402。第二系统 402 包括第一域管理设备 404、域注册服务器 406 和第二域管理设备 408。消息 412、414、416、420、422、424、426 的多次传输利用各自的箭头来显示。该消息源于其中箭头开始的设备, 并被发送到箭头指向的设备。带有字母 t 的箭头 418 表示时间线。如果消息 412、414、416、420、422、424、426 的传输被绘制在时间线上的较低位置, 则在稍后的时刻发送它。

[0069] 在这个实施例中, 域注册服务器 406 也预定用于创建新的域。为了创建新的域, 第一域管理设备 404 向域注册服务器 406 发送包括创建新的域的请求的创建请求消息 412。如果域注册服务器 406 愿意创建新的域并提供管理新的域的权限给第一域管理设备 404, 则域注册服务器 406 发送提供消息 414 给第一域管理设备 404。提供消息 414 包括管理域的权限。域注册服务器 406 利用与域的创建以及对于第一域管理设备 404 的管理域的权限的提供有关的信息来创建域历史数据文件。

[0070] 在稍后的时间, 当第一域管理设备 404 已绑定例如新的设备到域和 / 或已接收到例如内容的许可证与解密密钥时, 第一域管理设备 404 向域注册服务器 406 发送第一注册消息 416。第一注册消息 416 包括例如新的设备已进入该域的信息和 / 或包括例如许可证与解密密钥的拷贝。域注册服务器 406 在安全的存储设备中存储接收到的信息并利用与域信息的注册有关的信息来更新域历史数据文件。

[0071] 在一段时间之后, 第二域管理设备发送请求消息 422 给域注册服务器 406。请求消息 422 包括对于获得管理域的权限的请求。域注册服务器 406 确定它是否信任第二域管理设备, 以及在图 4 所绘制的情况下, 第二域管理设备被信任到某种程度, 并且域注册服务器 406 愿意将管理域的临时权限给予第二域管理设备 408。域注册服务器 406 向第二域管

理设备 408 发送提供消息 424。提供消息 424 包括管理域的临时权限以及在第二域管理设备 408 上为了恢复域管理所需的域的一个或多个特征。此外，域注册服务器 406 利用与接收请求和发送管理域的权限的提供有关的信息来更新域历史数据文件。

[0072] 由于由第二域管理设备 408 接收到的管理域的权限只是临时的，所以这个设备必须更新管理域的权限的提供。在稍后的时间，至少在管理域的临时权限的终止之前，第二域管理设备 408 因此向域注册服务器 406 发送延长请求消息 426。在图 4 所示的示例中，域注册服务器 406 仍然信任第二域管理设备到某种程度并愿意延长管理域的临时权限。域注册服务器 406 将利用包括管理域的临时权限的延长的延长提供消息 428 来应答接收到延长请求消息 426。

[0073] 然而，第一域管理设备 404 并没有发生故障并且仍在管理该域。第一域管理设备 404 已绑定例如新的设备到该域并向域注册服务器 406 发送第二注册消息 420。第二注册消息 420 包括有关新的设备至域的绑定的信息。通过从第一域管理设备 404 接收另一注册消息，域注册服务器 406 检测到：至少一个域管理设备是欺诈性的。不可能两个不同的域管理设备在管理该域。在图 4 所示的示例中，域注册服务器 406 决定：第一域管理设备 404 被信任，这是因为它是请求创建域的初始设备并且因为对于管理第二域管理设备 408 的域的请求可能是对该域的欺诈攻击。

[0074] 由第二域管理设备检测到欺诈的结果可能导致不提供管理域的临时权限的延长或导致发送域去激活消息 430 给第二域管理设备 408。域去激活消息 430 由第二域管理设备 408 的处理器 410 来接收。域去激活消息包括域去激活代理。域去激活代理是自动地由第二域管理设备 408 的处理器 410 执行的一段程序代码。运行域去激活代理具有由第二域管理设备 408 停止域管理的结果。

[0075] 应当注意：上面提到的实施例说明而非限制本发明，并且本领域技术人员能够设计许多替换的实施例而不脱离所附的权利要求书的范围。

[0076] 在权利要求书中，放置在括号之间的任何参考符号不应被理解为限制权利要求。动词“包括”及其动词变形的使用不排除除了权利要求中所陈述的那些元素或步骤之外的元素或步骤的存在。在元素前面的冠词“一”或“一个”并不排除多个这样的元素的存在。本发明可以利用包括若干不同元素的硬件并且利用适当编程的计算机来实现。在枚举若干装置的设备权利要求中，这些装置中的若干装置可以利用同一项硬件来实施。某些措施在互不相同的从属权利要求中被阐述的简单事实并不表明不能有利使用这些措施的组合。

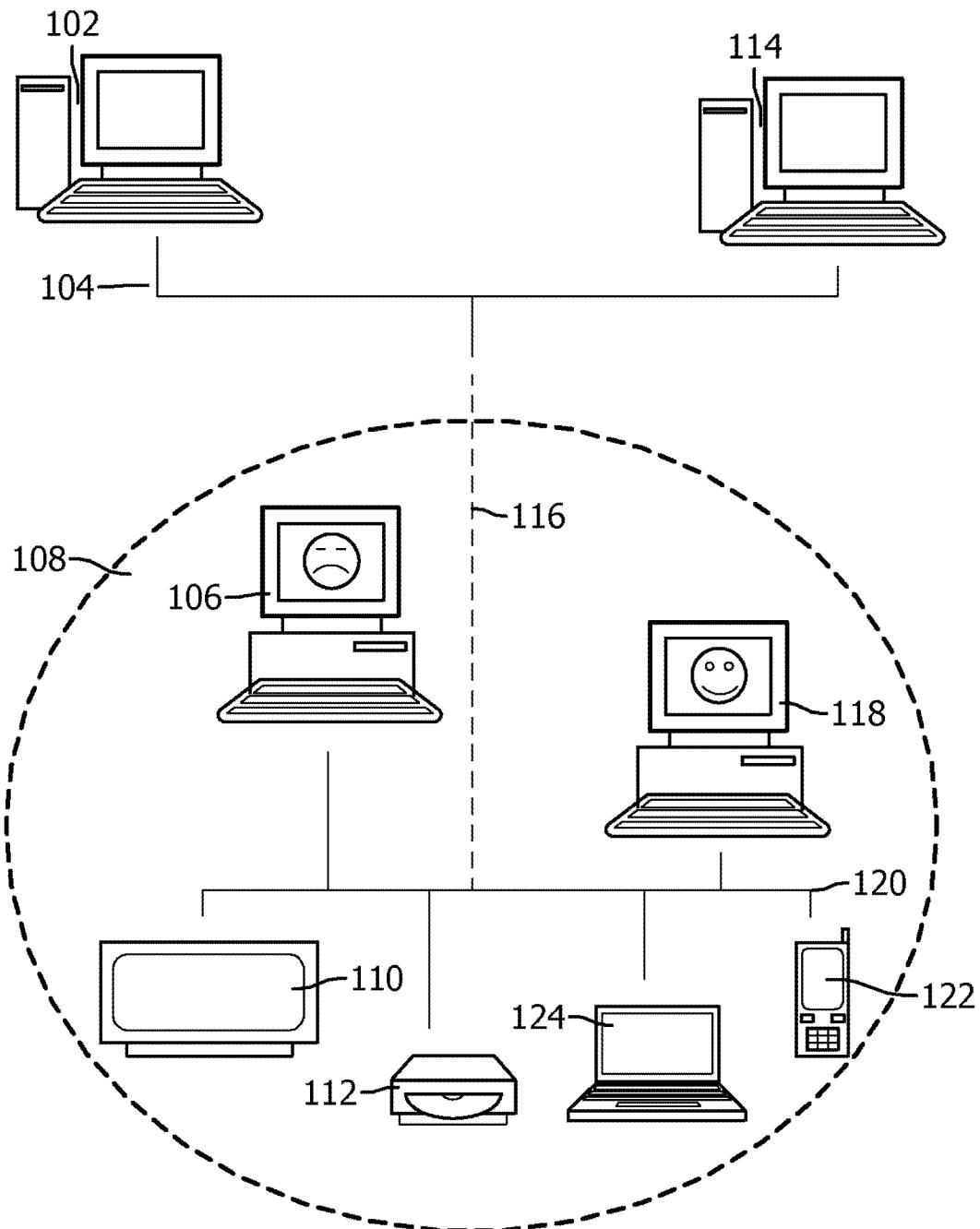


图 1

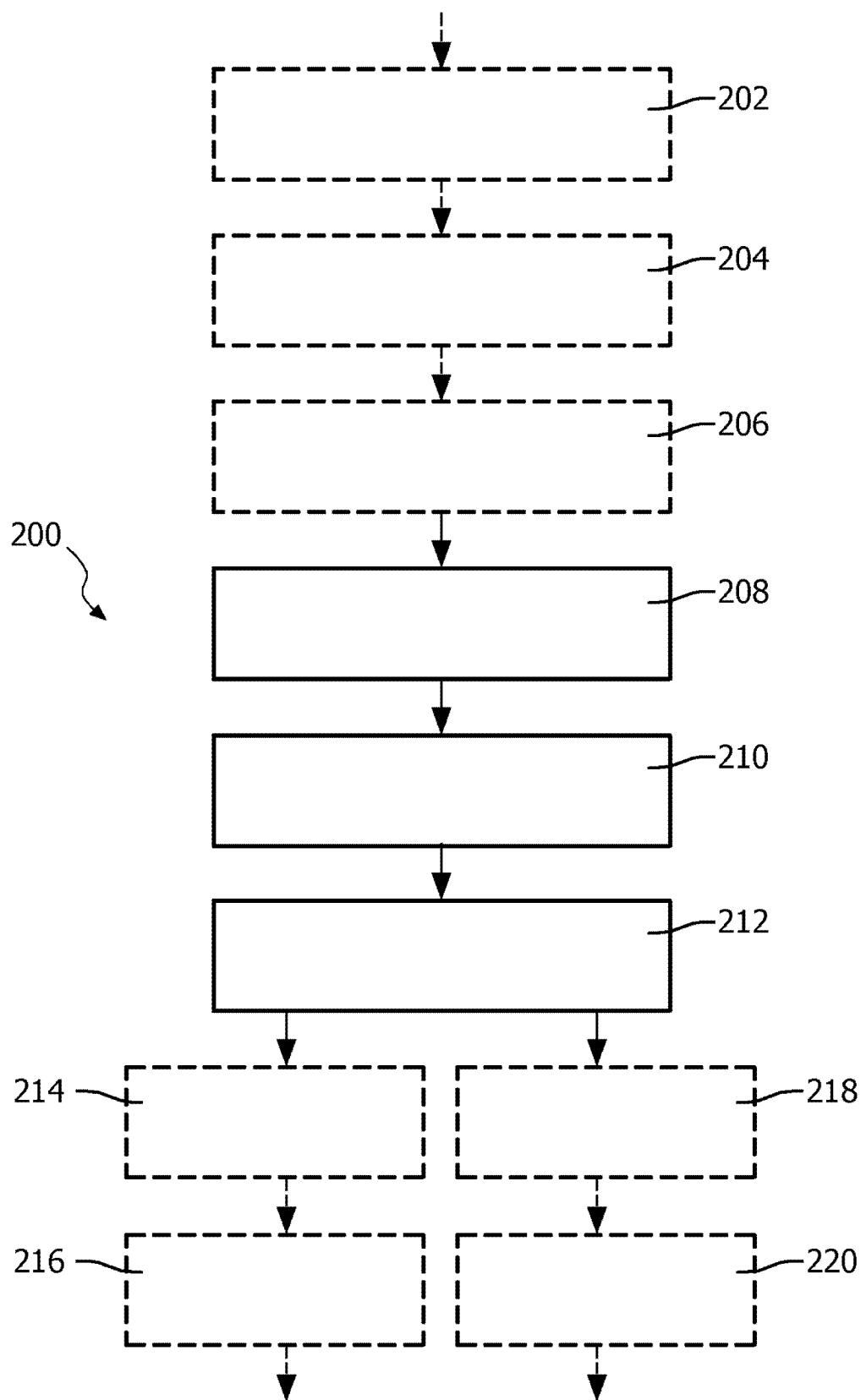


图 2

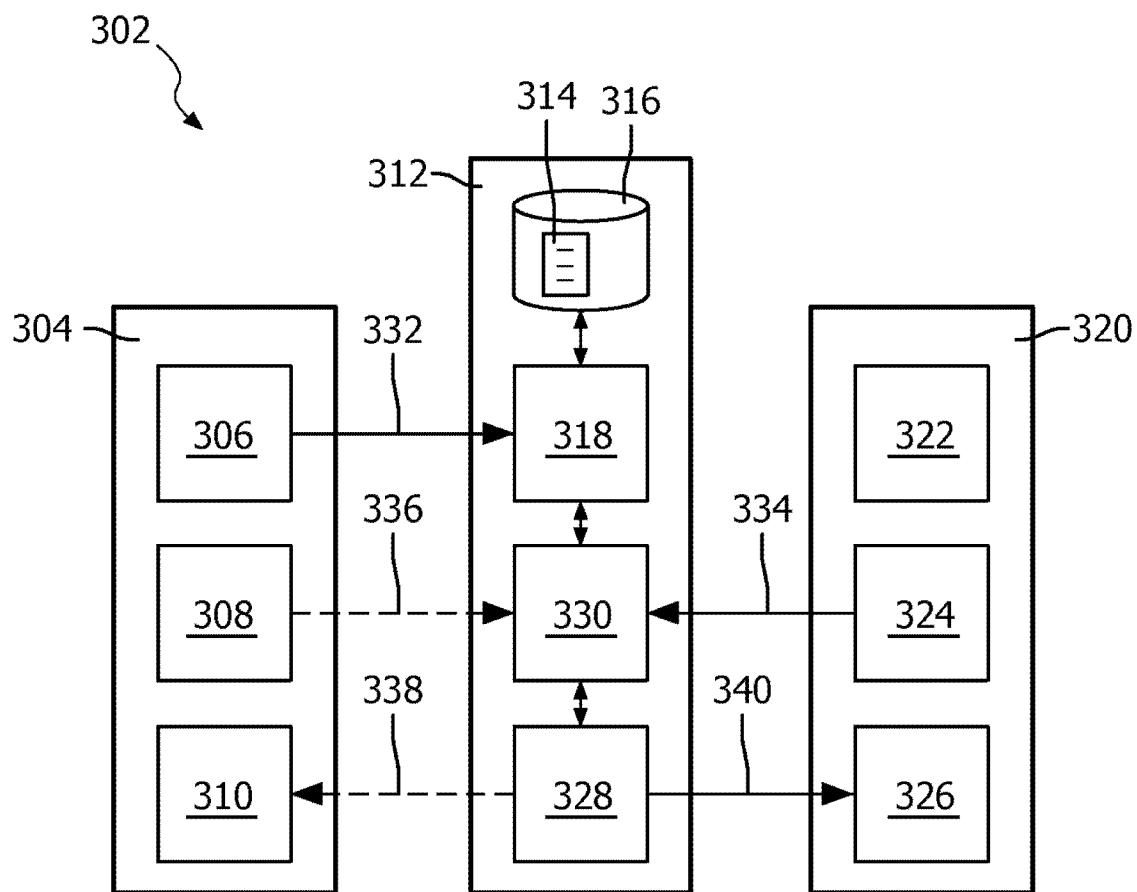


图 3

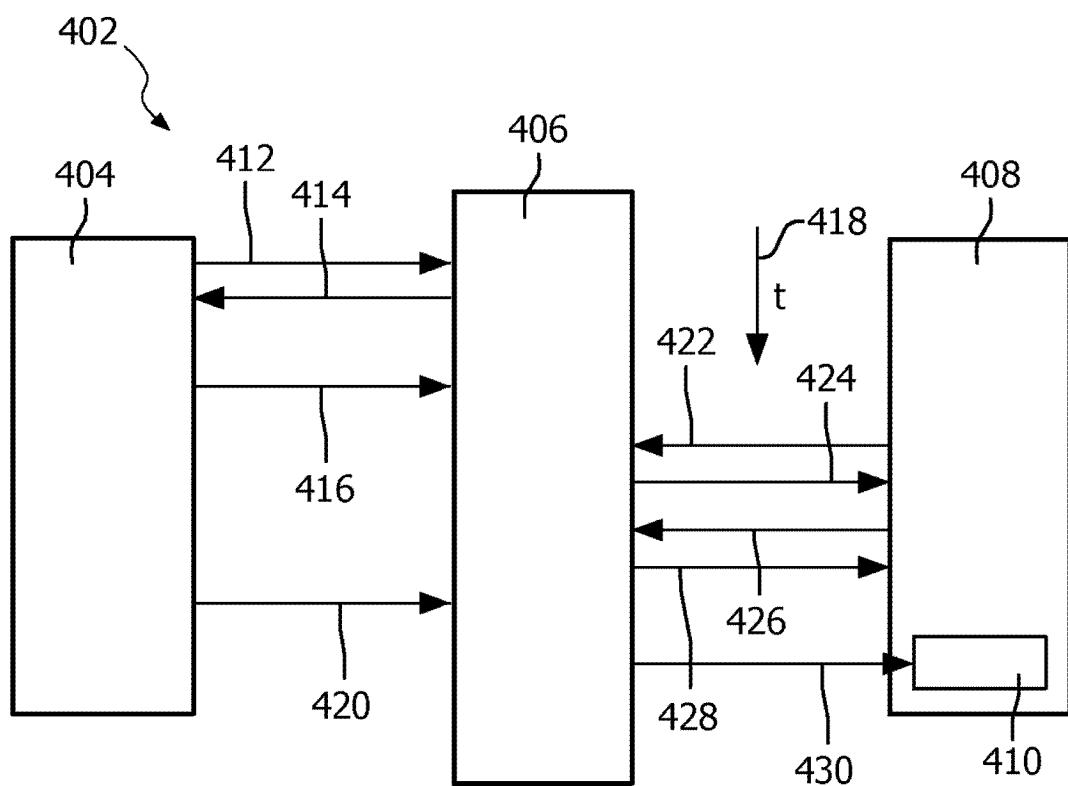


图 4