(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101232397 B
(45)授权公告日 2010.10.27

(21)申请号 200810007277.1

(22)申请日 2008.02.22

(73)专利权人 成都市华为赛门铁克科技有限公司
地址 611731 四川省成都市高新区西部园区清水河片区

(72)发明人 刘仁伟 陈华

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04L 12/24(2006.01)
G06F 9/445(2006.01)

(56)对比文件
CN 1257591 A,2000.06.21, 说明书第3页第15行-第4页第21行, 第18页第27行-第21页第29行、权利要求1-11,17-26,32,52,63、摘要.
CN 1940878 A,2007.04.04, 全文.
CN 1908910 A,2007.02.07, 说明书第1页第9-13行, 第3页第11行-第4页最后1行, 第8页第12行-第10页第1行、图4,7.
US 2007/0101119 A1,2007.05.03, 全文.
CN 1690963 A,2005.11.02, 全文.
KR 10-2004-0047209 A,2004.06.05, 全文.

审查员 张臻贤

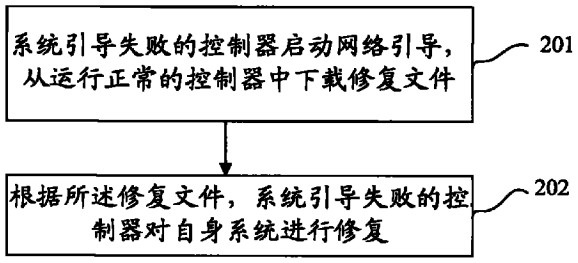
权利要求书 2 页 说明书 6 页 附图 5 页

(54)发明名称

多控制器系统修复的方法和装置

(57)摘要

本发明实施例公开了一种多控制器系统修复的方法和装置,涉及多控制器结构的控制系统,为实现自动修复控制器的系统,保证控制系统始终在多个控制器下运行而发明。所述方法包括:系统引导失败的控制器启动网络引导,从运行正常的控制器中下载修复文件;根据所述修复文件,系统引导失败的控制器对自身系统进行修复。所述装置包括:至少两个控制器;网络引导单元,连接所述至少两个控制器,用于系统引导失败的控制器启动网络引导;在每个控制器中,包括,检测单元、本地引导单元、修复文件下载单元和修复单元。本发明实施例可在任一控制器系统引导失败后,自动通过网络引导从另一个控制器中下载系统文件进行系统修复。



CN 101232397 B

1. 一种多控制器系统修复的方法，其特征在于，包括步骤：

系统上电后，每个控制器启动本地系统引导程序；

如果本地引导成功，则加载应用程序运行；

如果本地引导失败，则系统引导失败的控制器启动网络引导，从运行正常的控制器中下载修复文件，并根据所述修复文件，系统引导失败的控制器对自身系统进行修复。

2. 根据权利要求 1 所述的多控制器系统修复的方法，其特征在于，所述系统引导失败的控制器对自身系统进行修复，如果修复成功，则重启系统；如果修复不成功，则从所述运行正常的控制器中下载应用程序并加载运行。

3. 根据权利要求 1 所述的多控制器系统修复的方法，其特征在于，在所述系统引导失败的控制器启动网络引导之前，还包括下列步骤：

编译内核文件和初始化内存文件系统文件；

按照预引导执行环境分别配置简单文件传送协议服务器和动态主机配置协议服务器；

设置网络引导启动选项。

4. 根据权利要求 3 所述的多控制器系统修复的方法，其特征在于，所述按照预引导执行环境配置简单文件传送协议服务器包括下列步骤：

设置简单文件传送协议的目录；

将所述的内核文件和初始化内存文件系统文件配置在所述简单文件传送协议的目录下；

将预引导执行环境启动引导文件配置在所述简单文件传送协议的目录下；

指定引导操作系统文件为所述的内核文件和初始化内存文件系统文件；

开启简单文件传送协议服务。

5. 根据权利要求 3 所述的多控制器系统修复的方法，其特征在于，所述按照预引导执行环境配置动态主机配置协议服务器包括下列步骤：

指定动态主机配置协议所用的网卡及网段；

指定简单文件传送协议的服务器 IP 地址；

指定预引导执行环境启动引导文件的位置；

开启动态主机配置协议服务。

6. 一种多控制器系统修复的装置，其特征在于，包括：

至少两个控制器；

网络引导单元，连接所述至少两个控制器，用于系统引导失败的控制器启动网络引导；

在每个控制器中，包括

检测单元，用于检测控制器的本地引导单元引导系统是否成功，如果不成功，则启动修复文件下载单元，如果成功，则启动本地引导单元；

本地引导单元，用于控制器启动本地系统引导，加载应用程序运行；

修复文件下载单元，用于系统引导失败的控制器从运行正常的控制器中下载修复文件；

修复单元，用于根据所述修复文件下载单元下载的修复文件，对控制器自身系统进行

修复。

7. 根据权利要求 6 所述的多控制器系统修复的装置，其特征在于，所述修复单元具体包括：

判断模块，用于判断控制器对自身系统进行修复是否成功；如果修复成功，则启动重启模块；如果修复不成功，则启动应用程序下载模块；

重启模块，用于重新启动系统；

应用程序下载模块，用于从运行正常的控制器中下载应用程序，加载应用程序运行。

多控制器系统修复的方法和装置

技术领域

[0001] 本发明涉及多控制器结构的控制系统，尤其涉及一种多控制器系统修复的方法和装置。

[0002] 背景技术

[0003] 在控制系统中，为提高系统的可靠性，往往采用双控制器或多控制器的结构。多控制器之间采用网络连接进行相互通信，系统运行时，一个控制器中缓存的内容被完整的镜像至另外一个控制器中，为彼此提供冗余的性能。

[0004] 图 1 所示为 2 个控制器配置示意图，每个控制器维护有两个高速缓存，在系统正常运行时，控制器 1 的高速缓存中 1 的数据镜像至控制器 2 的高速缓存 1 中，控制器 2 的高速缓存 2 中的数据镜像至控制器 1 的高速缓存 2 中，这种多控制器配置方式可以提高控制系统的可靠性能，能够利用冗余的控制器缓存中的数据重新配置缓存，保持控制器的冗余性。

[0005] 在实现本发明的过程中，发明人经过研究发现 :现有技术中的双控制器或多控制器之间的网络连接只是做相关的数据同步和冗余设计，当一个控制器的系统文件发生故障后，该控制器无法自动恢复，必须通过人工干预，重新安装操作系统 (Operation System，OS) 才能恢复，从而影响了控制系统的可靠性。

[0006] 发明内容

[0007] 一方面，本发明实施例提供了一种多控制器系统修复的方法，该方法能够自动修复控制器的系统，保证控制系统始终在多个控制器下运行。

[0008] 为解决上述目的，本发明实施例是通过以下技术方案实现的 :

[0009] 一种多控制器系统修复的方法，包括以下步骤 :

[0010] 系统上电后，每个控制器启动本地系统引导程序 ;

[0011] 如果本地引导成功，则加载应用程序运行 ;

[0012] 如果本地引导失败，则系统引导失败的控制器启动网络引导，从运行正常的控制器中下载修复文件，并根据所述修复文件，系统引导失败的控制器对自身系统进行修复。。

[0013] 本发明实施例提供的多控制器系统修复的方法，通过在多控制器之间的网络连接上增加网络引导功能，在一个控制器本地引导系统失败后，将启动网络引导，从另外一个控制器中下载系统文件到系统引导失败的控制器，在所述系统引导失败的控制器中进行系统修复。因此，在任一个控制器在系统软件损坏的情况下，可以通过网络引导启动起来，然后自动从另外一个控制器下载系统文件进行修复，实现自动系统修复，保证控制系统始终在多个控制器下运行，提高了控制系统的可靠性。

[0014] 另一方面，本发明实施例提供了一种多控制器系统修复的装置。利用所述装置，能够实现自动修复控制器的系统，保证控制系统始终在多个控制器下运行。

[0015] 为解决上述目的，本发明实施例是通过以下技术方案实现的 :

[0016] 一种多控制器系统修复的装置，包括 :

[0017] 至少两个控制器 ;

[0018] 网络引导单元，连接所述至少两个控制器，用于系统引导失败的控制器启动网络

引导；

[0019] 在每个控制器中，包括，

[0020] 检测单元，用于检测控制器的本地引导单元引导系统是否成功，如果不成功，则启动修复文件下载单元，如果成功，则启动本地引导单元；

[0021] 本地引导单元，用于控制器启动本地系统引导，加载应用程序运行；

[0022] 修复文件下载单元，用于系统引导失败的控制器从运行正常的控制器中下载修复文件；

[0023] 修复单元，用于根据所述修复文件下载单元下载的修复文件，对控制器自身系统进行修复。

[0024] 本发明实施例提供的多控制器系统修复的装置，通过在多控制器之间的网络连接上增加网络引导功能，当一个控制器本地引导系统失败，通过网络引导单元启动网络引导，由修复文件下载单元从另外一个控制器中下载系统修复程序到系统引导失败的控制器，由修复单元在系统引导失败的控制器中进行系统修复。因此，在任一个控制器在系统软件损坏的情况下，可以通过网络引导启动起来，然后自动从另外一个控制器下载系统文件进行修复，实现自动系统修复，保证控制系统始终在多个控制器下运行，提高了控制系统的可靠性。

[0025] **附图说明**

[0026] 图 1 为现有技术中多控制器提供系统冗余的原理图；

[0027] 图 2 为本发明实施例一多控制器系统修复的方法的流程图；

[0028] 图 3 为本发明实施例使用的预引导执行环境技术的工作原理图；

[0029] 图 4 为本发明实施例双控制器控制框结构图；

[0030] 图 5 为本发明实施例为进行网络引导在控制器中进行设置的流程图；

[0031] 图 6 为本发明实施例按照预引导执行环境技术，配置 TFTP 服务器的流程图；

[0032] 图 7 为本发明实施例按照预引导执行环境技术，配置 DHCP 服务器的流程图；

[0033] 图 8 为本发明实施例二多控制器系统修复的装置的结构图；

[0034] 图 9 为本发明实施例三多控制器系统修复的装置的结构图。

具体实施方式

[0035] 为了实现能够自动修复控制器的系统，保证控制系统始终在多个控制器下运行，从而提高控制系统的可靠性，本发明实施例提供了一种多控制器系统修复的方法和装置，下面结合实施例进行详细说明。

[0036] 实施例一，一种多控制器系统修复的方法，流程如图 2 所示，包括：

[0037] 步骤 201，系统引导失败的控制器启动网络引导，从运行正常的控制器中下载修复文件。

[0038] 所述网络引导就是使用预引导执行环境 (Preboot Execution Environment，PXE) 技术使客户端通过网络从服务器端下载系统引导程序进行系统引导启动。

[0039] 其中，所述 PXE 技术的工作原理，如图 3 所示：

[0040] 301，客户端以广播的形式发送一个请求帧，客户端启动后，其网卡上的自启动芯片以广播的形式发送一个请求帧，如 FIND 帧，所述 FIND 帧带有所述网卡的 ID 号；

[0041] 302，客户端获得远程启动服务器的 IP 地址，远程启动服务器收到客户端广播的 FIND 帧后，根据帧中所带的网卡 ID 号，向客户端发送一个 FOUND 帧，FOUND 帧中包含了远程启动服务器的网卡 ID 号；

[0042] 303，客户端请求远程启动服务器传送启动所需文件，客户端在收到远程启动服务器端发回的 FOUND 帧后，则会回应一个帧，以请求传送启动所需文件；

[0043] 304，客户端从远程启动服务器获取启动所需文件，当远程启动服务器收到传送启动所需文件帧的要求后，会根据其远程启动数据库中的客户端记录查找对应的启动块，将客户端所需的启动文件传送给客户端；

[0044] 305，客户端执行启动文件，客户端在接收到完整的启动文件后，就开始执行文件中的启动程序，将执行点转向启动块的入口，启动客户端。

[0045] 当然不同的操作系统有不同的引导方式。

[0046] 本实施例中，为能够启动网络引导，在硬件上，在每一控制器上需要配置支持 PXE 的网卡，例如 intel 的 ESB2 集成网卡；在软件上，需要设置网络引导启动选项，例如，在系统引导程序 CMOS 中设置硬盘做第一启动选项，ESB2 集成网卡做第二启动选项。

[0047] 所述硬盘不限于采用 RAIDI 磁盘阵列，还可采用如 SCSI 硬盘、RAID0/3/5 阵列、单 IDE 硬盘、磁带机、磁带库、光盘、CF 卡、flash 等存储介质。

[0048] 以双控制器为例，如图 4 所示，在控制系统的两个控制器之间配置支持 PXE 的网卡，控制系统上电后，从每个控制器中启动系统引导程序，如果引导操作系统成功，则在控制器中加载应用程序运行，如果引导操作系统不成功，则系统引导失败的控制器将启动网络引导，从运行正常的控制器中下载修复文件。对于网络引导而言，双控制器中的每一个控制器都可以做服务器，也可以做客户端。

[0049] 所述的操作系统不限于 Linux 系列操作系统，也可以为 Windows 系统操作系统，或 Unix 系统操作系统等其它操作系统。

[0050] 为进行网络引导，还需要在双控制器中的每个控制器中进行如下设置，如图 5 所示：

[0051] 501，编译内核文件和初始化内存文件系统文件；

[0052] 502，按照 PXE 技术，配置简单文件传送协议 (Trivial File TransferProtocol，TFTP) 服务器；

[0053] 503，按照 PXE 技术，配置动态主机配置协议 (Dynamic Host ConfigurationProtocol，DHCP) 服务器；

[0054] 504，设置网络引导启动选项。

[0055] 以 Linux 系列操作系统为例，每步设置具体操作为：

[0056] 步骤 501，编译内核文件 bzImage 和初始化内存文件系统文件 initramfs。

[0057] 本步骤为准备步骤，在本实施例中，引导系统为基于 unattended 项目的 Linux 系统，使用作为客户端控制器加载的系统中自带的命令，可从作为服务器的控制器中下载系统引导程序。

[0058] 步骤 502，按照 PXE 技术，配置 TFTP 服务器，具体步骤如图 6 所示：

[0059] 601，把 TFTP 的目录设置为 /tftpboot/；

[0060] 602，将所述内核文件 bzImage 和初始化内存文件系统文件 initramfs 配置在 TFTP

的 /tftpboot/ 目录下；

[0061] 603，将 PXE 启动引导文件 pxelinux.0 配置在 /tftpboot/ 目录下；

[0062] 604，配置 /tftpboot/pxelinux.cfg/default 文件，指定客户端引导的操作系统文件为 bzImage 和 initramfs；

[0063] 605，开启 TFTP 服务。

[0064] 步骤 503，按照 PXE 技术，配置 DHCP 服务器，具体步骤如图 7 所示：

[0065] 701，配置 /etc/sysconfig/dhcpd，指定 DHCP 所用的网卡；

[0066] 702，配置 /etc/dhcpd.conf，指定 DHCP 的网段；

[0067] DHCP 配置是至关重要的，这关系到 PXE 技术是否正常引导，例如，指定 DHCP 的网段，起始地址：192.168.0.2；结束地址：192.168.0.80；子网掩码：255.255.255.0。

[0068] 703，指定 TFTP 的服务器 IP 地址及 PXE 启动引导文件的位置；

[0069] 例如，指定 TFTP 的服务器 IP 地址：192.168.0.1；子网掩码：255.255.255.0；网关：192.168.0.1。

[0070] 本实施例中，指定的 PXE 启动引导文件的位置为配置在 /tftpboot/ 目录下。

[0071] 704，开启 DHCP 服务。

[0072] 经过上述设置后，当一个控制器的系统文件损坏后，该系统引导失败的控制器作为客户端通过 PXE 技术从运行正常的控制器中获取需要的系统修复包，此时运行正常的控制器将作为网络引导的服务器端。

[0073] 系统引导失败的控制器获取运行正常的控制器的 IP 地址后，将获取启动引导文件 pxeliunx.0、配置文件 default、内核文件 bzImage、初始化内存文件系统文件 initramFs，使用 FTP 从运行正常的控制器上将系统修复包下载到本地控制器中。

[0074] 步骤 202，根据所述修复文件，系统引导失败的控制器对自身系统进行修复。

[0075] 如果修复成功，则重启系统；如果修复不成功，则从所述运行正常的控制器中下载应用程序并加载运行。

[0076] 本发明实施例通过在多控制器之间的网络连接上增加网络引导功能，使得其中任一个控制器在系统软件损坏的情况下，可以通过网络引导启动起来，然后自动从另外一个控制器下载系统文件进行修复，即使修复不成功，也能从另外一个控制器下载应用程序继续运行，保障系统始终可以在多控制器下运行，大大提高了系统的可靠性。

[0077] 实施例二，如图 8 所示，一种多控制器系统修复的装置，包括：

[0078] 至少两个控制器 (801,802)；

[0079] 网络引导单元 803，连接所述至少两个控制器，用于系统引导失败的控制器启动网络引导；

[0080] 在每个控制器中，包括，

[0081] 检测单元 804，用于检测控制器的本地引导单元引导系统是否成功，如果不成功，则启动修复文件下载单元 806，如果成功，则启动本地引导单元 805；

[0082] 本地引导单元 805，用于控制器启动本地系统引导，加载应用程序运行；

[0083] 修复文件下载单元 806，用于系统引导失败的控制器从运行正常的控制器中下载修复文件；

[0084] 修复单元 807，用于根据所述修复文件下载单元 806 下载的修复文件，对控制器自

身系统进行修复。

[0085] 为了在多控制器之间的网络连接上实现网络引导功能，需要对每个控制器进行一定的设置，具体包括：

[0086] 设置网络引导启动选项，如在 CMOS 中设置硬盘做第一启动选项，支持 PXE 技术的网卡做第二启动选项。

[0087] 编译内核文件和初始化内存文件系统文件；

[0088] 配置 TFTP 服务器，包括：配置 TFTP 的目录；将所述的内核文件和初始化内存文件系统文件配置在所述 TFTP 的目录下；将 PXE 启动引导文件配置到所述 TFTP 的目录下；指定引导操作系统文件为所述的内核文件和初始化内存文件系统文件；开启 TFTP 服务。

[0089] 配置 DHCP 服务器，包括：指定 DHCP 所用的网卡；指定 DHCP 的网段；指定 TFTP 的服务器 IP 地址及 PXE 启动引导文件的位置；开启 DHCP 服务。

[0090] 在修复文件下载单元 806 中，系统引导失败的控制器作为客户端，获取运行正常的控制器（作为服务器端）的 IP 地址后，将获取启动引导文件、配置文件、内核文件、初始化内存文件系统文件，然后使用 FTP 从作为服务器端的控制器上将系统修复包下载到系统引导失败的控制器中。

[0091] 本发明实施例多控制器系统修复的装置，可用于执行实施例一多控制器系统修复的方法。双控制器或多控制器之间通过网络引导单元连接，用于系统引导失败的控制器启用网络引导，从运行正常的控制器中下载修复程序，进行自身系统的修复，保证控制系统始终在多个控制器下运行，提高了控制系统的可靠性，并且可以节约成本，不需要额外使用存储介质来进行系统的备份和恢复。

[0092] 本发明实施例可以用于各种控制系统，实现对存储系统、操作系统等被控设备的系统恢复。

[0093] 实施例三，如图 9 所示，一种多控制器系统修复的装置，包括：

[0094] 至少两个控制器 (901，902)；

[0095] 网络引导单元 903，连接所述至少两个控制器，用于系统引导失败的控制器启动网络引导；

[0096] 在每个控制器中，包括，

[0097] 检测单元 904，用于检测控制器的本地引导单元引导系统是否成功，如果不成功，则启动修复文件下载单元 906，如果成功，则启动本地引导单元 905；

[0098] 本地引导单元 905，用于控制器启动本地系统引导，加载应用程序运行；

[0099] 修复文件下载单元 906，用于系统引导失败的控制器从运行正常的控制器中下载修复文件；

[0100] 修复单元 907，用于根据所述修复文件下载单元 906 下载的修复文件，控制器对自身系统进行修复。

[0101] 所述修复单元进一步包括：

[0102] 判断模块 9071，用于判断控制器对自身系统进行修复是否成功；如果修复成功，则启动重启模块 9072；如果修复不成功，则启动应用程序下载模块 9073；

[0103] 重启模块 9072，用于重新启动系统；

[0104] 应用程序下载模块 9073，用于从运行正常的控制器中下载应用程序，加载应用程

序运行。

[0105] 在本发明实施例中，当一个控制器系统引导失败，通过网络引导单元启动网络引导，由修复文件下载单元从运行正常的控制器中下载系统修复程序到系统引导失败的控制器，由修复单元在系统引导失败的控制器中进行系统修复。在修复单元中，由判断模块判断控制器对自身系统进行修复是否成功，如果修复成功，则启动重启模块，控制系统进入正常模式；如果修复不成功，则启动应用程序下载模块，从运行正常的控制器中下载应用程序，加载应用程序运行。因此，本实施例的装置可始终保证控制系统在多个控制器下运行，大大提高了系统的可靠性。

[0106] 当然，本发明的实施例还可有多种，在不背离本发明的实施例精神及其实质的情况下，本领域技术人员当可根据本发明的实施例做出各种相应的改变和变形，将本发明实施例应用于不同的控制系统中，但这些相应的改变和变形都应属于本发明的实施例所附的权利要求的保护范围。

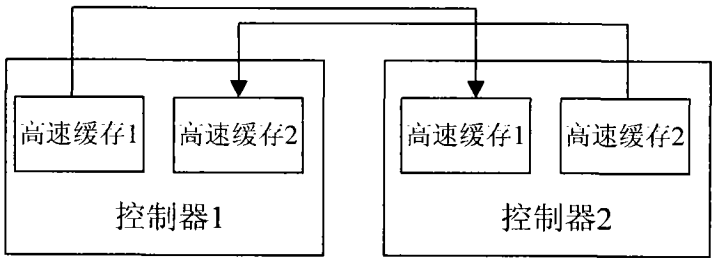

高速缓存1
高速缓存2
控制器1
高速缓存1
高速缓存2
控制器2

图 1

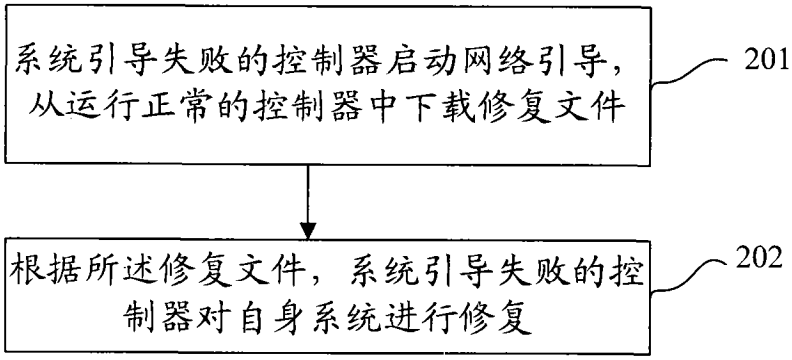

系统引导失败的控制器启动网络引导，从运行正常的控制器中下载修复文件
201
根据所述修复文件，系统引导失败的控制器对自身系统进行修复
202

图 2

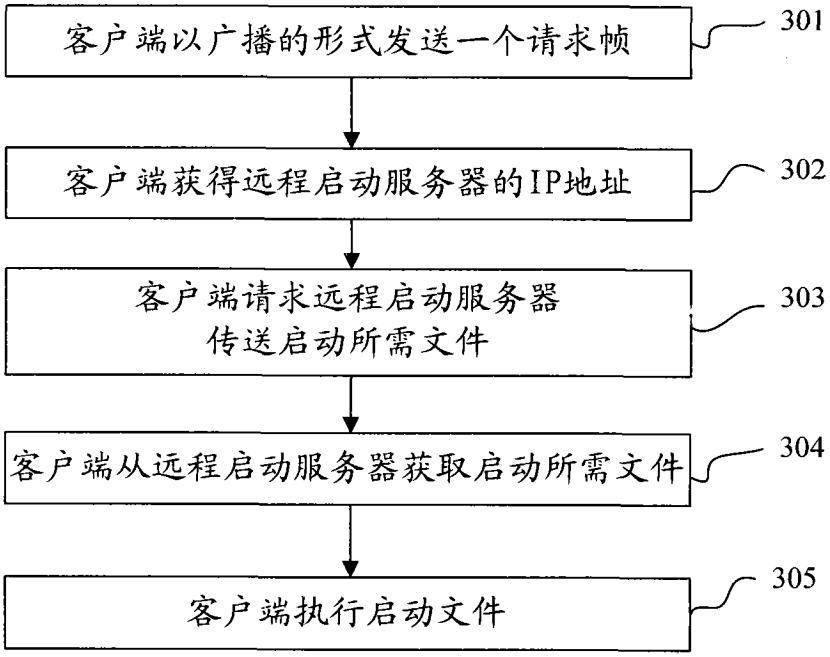

客户端以广播的形式发送一个请求帧
301
客户端获得远程启动服务器的IP地址
302
客户端请求远程启动服务器
传送启动所需文件
303
客户端从远程启动服务器获取启动所需文件
304
客户端执行启动文件
305

图 3

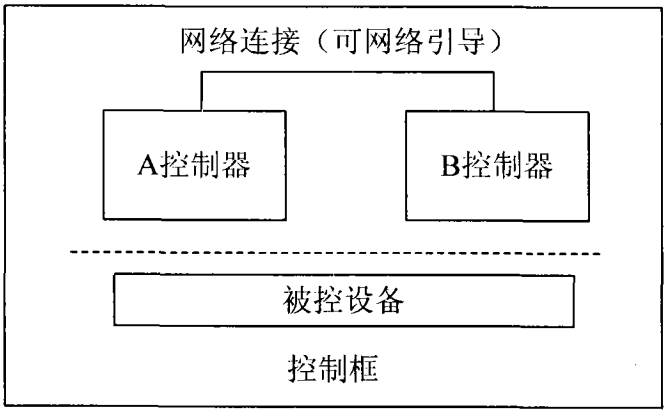

网络连接（可网络引导）
A控制器
B控制器
被控设备
控制框

图 4

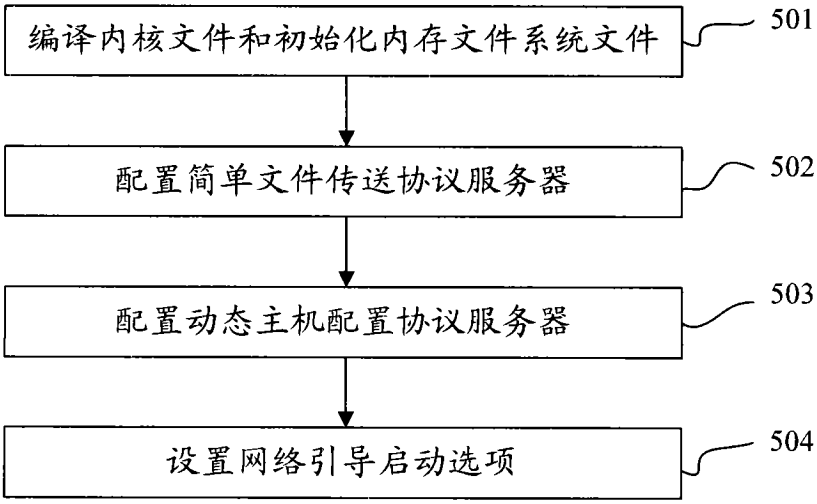

编译内核文件和初始化内存文件系统文件
501
配置简单文件传送协议服务器
502
配置动态主机配置协议服务器
503
设置网络引导启动选项
504

图 5

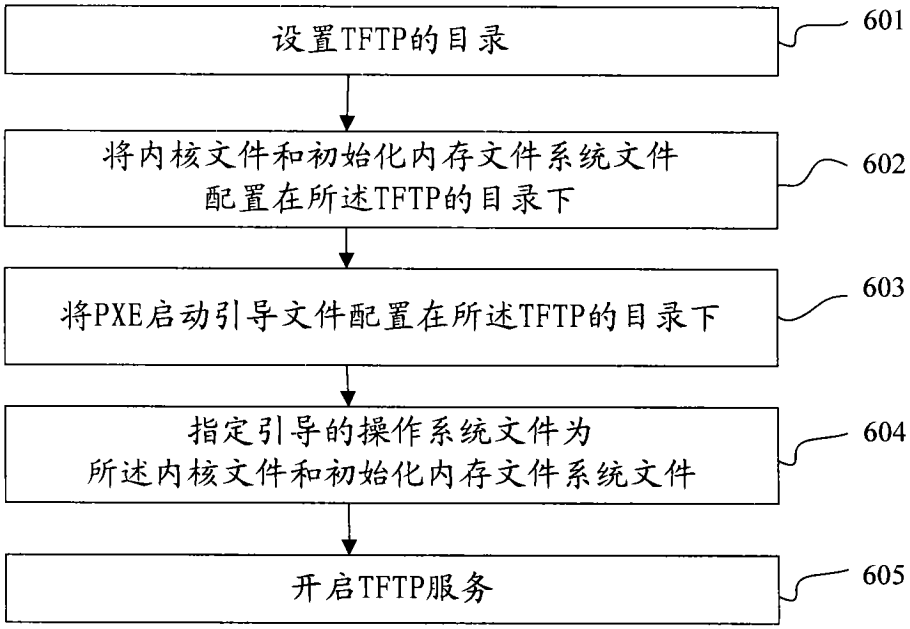

设置TFTP的目录
601
将内核文件和初始化内存文件系统文件
配置在所述TFTP的目录下
602
将PXE启动引导文件配置在所述TFTP的目录下
603
指定引导的操作系统文件为
所述内核文件和初始化内存文件系统文件
604
开启TFTP服务
605

图 6

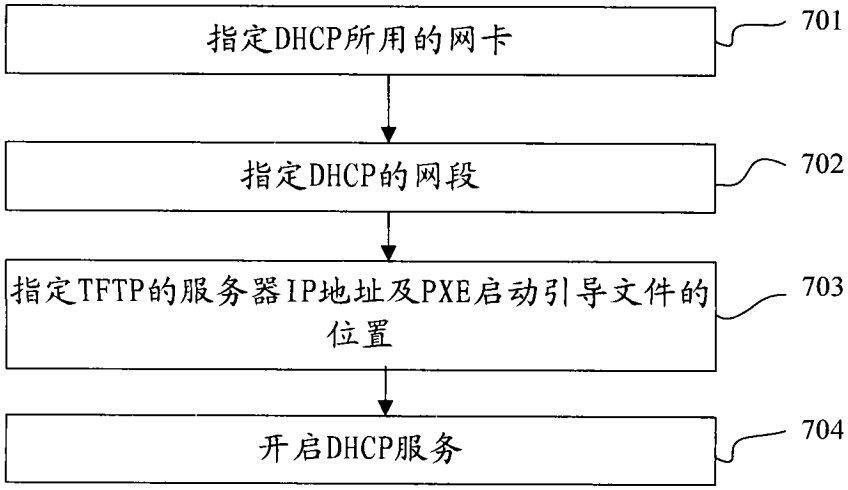

指定DHCP所用的网卡
701
指定DHCP的网段
702
指定TFTP的服务器IP地址及PXE启动引导文件的位置
703
开启DHCP服务
704

图 7

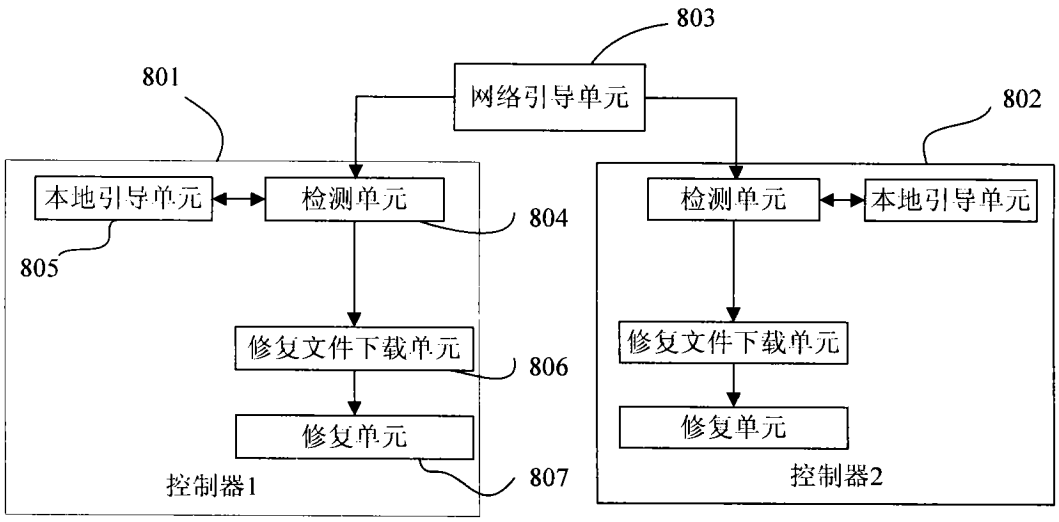

803
801
网络引导单元
802
本地引导单元
检测单元
804
805
检测单元
本地引导单元
修复文件下载单元
806
修复单元
807
控制器1
修复文件下载单元
修复单元
控制器2

图 8

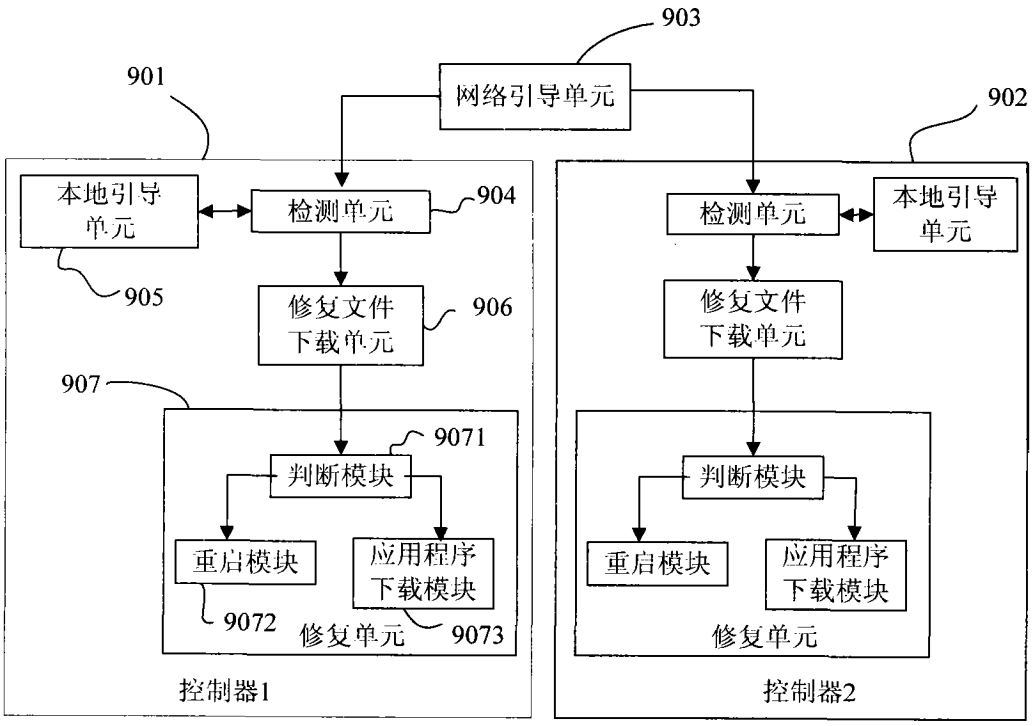

903
网络引导单元
901
902
本地引导单元
检测单元
904
905
修复文件下载单元
906
907
9071
判断模块
重启模块
应用程序下载模块
9072
修复单元
9073
控制器1
检测单元
本地引导单元
修复文件下载单元
判断模块
重启模块
应用程序下载模块
修复单元
控制器2

图 9