(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102665055 A
(43)申请公布日 2012.09.12

(21)申请号 201210085034.6

(22)申请日 2012.03.28

(71)申请人 姜宁
地址 210000 江苏省南京市白下区御水湾花园 33 栋 304

(72)发明人 姜宁

(74)专利代理机构 南京天翼专利代理有限责任公司 32112
代理人 汤志武

(51)Int.Cl.
H04N 5/765(2006.01)
H04N 21/234(2011.01)
H04N 21/2347(2011.01)
G06F 3/02(2006.01)
G06F 3/033(2006.01)
G06F 3/14(2006.01)

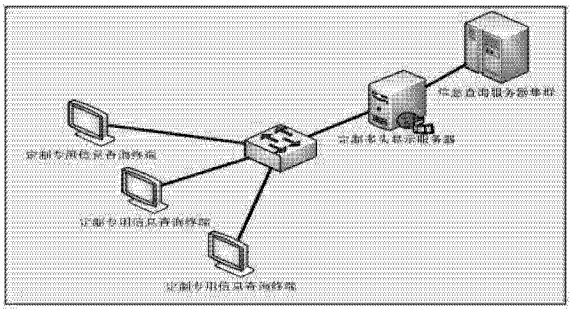
权利要求书 1 页 说明书 3 页 附图 2 页

(54)发明名称

一种 IO 远程映射设备及方法

(57)摘要

一种 IO 数据远程映射方法，提供 IO 数据远程端口映射，将操作对象的视频接口输出的视频数据加密后传输到操作者这边的端设备显示，将操作者端设备的显示设备信息加密后传输到操作对象的视频接口；IO 数据远程映射的过程是由 IO 远程设备将操作对象的各种 IO 设备如 VGA/DVI、USB、串行口等 IO 数据进行压缩、加密、封装传输过程进行 IO 映射并通过 IP 网络传输，在操作对象对端进行数据解封装、解密、解压缩后再将数据实时映射到操作端的相应设备里，实现 IO 远程映射过程。



CN 102665055 A

1. 一种 IO 数据远程映射方法，其特征在于：提供 IO 数据远程端口映射，将操作对象的视频接口输出的视频数据加密后传输到操作者这边的端设备显示，将操作者端设备的显示设备信息加密后传输到操作对象的视频接口。

2. 根据权利要求 1 所述的 IO 数据远程映射方法，其特征在于：IO 数据远程映射的过程是由 IO 远程设备将操作对象的各种 IO 设备如 VGA/DVI、USB、串行口等 IO 数据进行压缩、加密、封装传输过程进行 IO 映射并通过 IP 网络传输，在操作对象对端进行数据解封装、解密、解压缩后再将数据实时映射到操作端的相应设备里，实现 IO 远程映射过程。

3. 根据权利要求 1 所述的 IO 数据远程映射方法，其特征在于：对 USB 的信息在操作者端设备上只实现往操作对象传输数据的端口映射，将 USB 的写数据线置空，即完成了 USB 只读端口映射；提供 IO 数据远程端口映射时，将操作者端设备的只读 USB 的数据流映射到远程的操作对象的 USB 接口。

4. 根据权利要求 1 所述的 IO 数据远程映射方法，其特征在于：提供 IO 数据远程端口映射时，提供打印设备将操作者端设备的屏幕的显示图像打印到纸张上。

一种 IO 远程映射设备及方法

[0001] 技术领域

本发明涉及一种信息技术领域的 IO 远程映射设备及方法，特别是对远程的各种 IO 端口进行镜像的设备及方法。

[0002] 背景技术

目前一些专有系统的使用和维护还离不开各种终端。但是目前的各种终端映射方法如 kvm over IP 只支持键盘、鼠标和显示器。很多时候我们并不是只需要支持键盘和鼠标，也不只是为了实现对远程主机的维护。在一类特殊的应用场合，我们需要对远程主机、服务器之类的操作对象进行更多的操作，比如远程接入指纹识别仪、触摸屏、打印机、摄像头甚至是其他 USB 设备。一类更加特殊的应用中需要接入只读 USB 设备，即让 USB 设备不能写入任何数据，比如有些保密终端限制只能浏览不能将信息拷贝出来。因此常规的 kvm over IP (带外管理由网络设备管理系统，服务器管理系统，电源管理系统，集中管理平台四部分组成；带有远程管理功能的 KVM 切换器，KVM 是键盘、显示器、鼠标 (Keyboard、Video、Mouse) 的缩写) 已经不能满足这里的要求了。通过独立管理通道对机房网络设备，服务器设备以及电源系统进行整合管理。

[0003] 发明内容

本发明目的是提出 IO 远程映射设备及方法，通过远程端口映射的方式，将操作者的端口操作映射到远程的端口，使得远程的操作对象能够象在操作对象前一样操作远程的计算，并能够对计算机进行各种输入输出操作，包括但不仅仅只是局限于键盘、显示器和鼠标的操作。

[0004] 本发明的技术方案是：一种 IO 数据远程映射方法，其特征在于：提供 IO 数据远程端口映射，将操作对象的视频接口输出的视频数据加密后传输到操作者这边的端设备显示，将操作者端设备的显示设备信息加密后传输到操作对象的视频接口；具体言之：IO 数据远程映射的过程是由 IO 远程设备将操作对象的各种 IO 设备如 VGA/DVI、USB、串行口等 IO 数据进行压缩、加密、封装传输过程进行 IO 映射并通过 IP 网络传输，在操作对象对端进行数据解封装、解密、解压缩后再将数据实时映射到操作端的相应设备里，实现 IO 远程映射过程。

[0005] USB 的信息在操作者端设备上只实现往操作对象传输数据的端口映射，将 USB 的写数据线置空，即完成了 USB 只读端口映射。提供 IO 数据远程端口映射时，将操作者端设备的只读 USB 的数据流映射到远程的操作对象的 USB 接口。

[0006] 提供 IO 数据远程端口映射时，提供打印设备将操作者端设备的屏幕的显示图像打印到纸张上。

[0007] 本发明在需要远程在操作对象前输入一些有用数据的时候非常有用，比如使用本发明申请中设备在远程安装机器的时候，拷贝一个系统镜像和驱动的时候非常有用，即使操作对象没有连接网络或者需要跨越封闭隔离的内网也可以完成，同时不影响操作对象的网络隔离状态，操作者和操作对象间的互联网络仅相当于安全屏蔽了的延长线，因此具有很高的安全性和保密性。由于使用本发明申请中相关技术的保密终端操作过程有点像在云

里操作计算资源，我们也把它称为云终端。

[0008] 本发明申请与常规 kvm over IP 的区别是，本发明申请实现了丰富的外接设备与操作对象的连接，而不仅仅只是键盘、鼠标和显示器的连接；提供了数据单向传输的机制，提高了远程操作的安全性。

[0009] 本发明申请带来的直接好处是能够跨越隔离的网络来实现对隔离网络内主机或服务器的操作，能够将隔离网络丰富的外接设备与操作对象进行连接。同时提供只读的USB接口，提供一种硬件措施让高等级保护系统的数据导入和远程操作更加安全。

[0010] 本发明的有益效果是：本发明应用中提供了端到端的信息查询服务。用户无需考虑配置终端 PC 和相应的网络，降低了用户的使用门槛。易用：通过专用查询终端提供相对于 PC 终端更易用、更简洁的用户界面，提升用户体验。安全性好：查询终端本地无主机、无操作系统、无可写的 USB 接口，RHD KVM 接收端和发送端之间只通过专用的协议进行交互，不允许其他任何协议数据通过。这种体系结构能够有效阻止利用查询终端或查询终端的接入网线作为入口入侵后端系统。通过查询终端能够严格控制接入查询服务的终端数量，并且对使用查询服务的用户做严格和一致性的身份验证和操作审计。在用于互联网、办公专网、业务专网三个网络不得相互连通场合时，用户只能为访问每个网络分别配置一台 PC 机，此时用户桌面就需要放置 3 台 PC 机和对应显示器、键鼠，占据了很大的桌面空间。针对上述情况，引入 RHD KVM 技术后的解决方案极为方便。

[0011] 附图说明

图 1 为本发明应用的基于专用终端的系统架构；

图 2 采用 RHD KVM 后用户桌面 PC 配置情况的框图；

图 3 是多路 RHD KVM 接收端内部逻辑图；

图 4 是本发明的流程图。

[0012] 具体实施方式

如图 1 基于专用终端的系统架构所示，本申请的 IO 远程映射设备的工作过程如下：

步骤 1：本发明申请的系统方案中，系统在。

[0013] 步骤 2：本发明申请的系统方案中，系统在。

[0014] 如图 1 所示，信息查询服务器集群、定制多头显示服务器、专用信息查询终端（终端数目不限）共同组成一个封闭的信息查询系统，用户不用再去考虑购买和配置 PC 服务器和对应的网络即可享用信息查询服务。上述方案中两个关键的设备分别是：定制专用信息查询终端和定制多头显示服务器，下面分别介绍。

[0015] 定制专用信息查询终端

定制专用信息查询终端（下文简称查询终端）由：主流触摸显示屏、指纹识别仪或再加标清摄像头、RHD KVM 接收端、电源模块组成。触摸显示屏提供查询界面（对信息查询触摸界面的设计要求另行讨论）。指纹识别仪等用于用户身份认证。RHD KVM 用于接收远端主机上传来的用户界面视频数据，传输指纹识别仪和标清摄像头等设备的 USB 数据。根据用户需要查询终端对外提供一个只读的 USB 接口，用于读取用户的身份认证 U 盘。

[0016] 定制多头显示服务器

定制多头显示服务器用于支持多个查询终端。该服务器内置多台 PC 服务器（每台服务器配置 1 至 4 块显卡）、与服务器数量对应的 RHD KVM 发射端、以太网交换机。定制多头显

示服务器能够根据查询终端台数进行扩充。考虑到所有查询终端同时使用的概率很小，因此最好能够在查询终端接入时自动选择空闲的 PC 服务器和显示卡使用，从而避免查询终端和 PC 服务器、显卡资源静态绑定。

[0017] 因为互联网、办公专网、业务专网三个网络不得相互连通，因此用户只能为访问每个网络分别配置一台 PC 机，此时用户桌面就需要放置 3 台 PC 机和对应显示器、键鼠，占据了很大的桌面空间。针对上述情况，引入 RHD KVM 技术后的解决方案如图 2 所示 :给出采用 RHD KVM 后用户桌面 PC 配置情况。

[0018] 使用 RHD KVM 后，用户桌面只需要配置一套显示器和鼠标、键盘。在用户桌面的 RHD KVM 同时接入三根网线，接收三路视频信号，用户通过键盘热键切换不同的 PC 或 Server。此时的 RHD KVM 实质上是一个多路 RHD KVM。多路 RHD KVM 接收端的内部逻辑如下图所示 :通过 IO 数据远程端口映射，将操作对象的视频接口输出的视频数据加密后传输到操作者这边的端设备显示，将操作者端设备的显示设备信息加密后传输到操作对象的视频接口 ;将操作对象的 VGA/DVI IO 数据进行压缩、加密、封装传输过程进行 IO 映射并通过 IP 网络传输，在操作对象对端进行数据解封装、解密、解压缩后再将数据实时映射到操作端的相应设备里，实现 IO 远程映射过程。

[0019] USB 的信息在操作者端设备上只实现往操作对象传输数据的端口映射，将 USB 的写数据线置空，即完成了 USB 只读端口映射。

[0020] 图 3 多路 RHD KVM 接收端内部逻辑图中，当严格要求互联网、办公专网、业务专网之间不能接通，因此在多路 RHD KVM 中分别设置三个物理独立的单路 RHD KVM。每个单路 RHD KVM 仅仅通过专用的信号线与视频处理 &KVM 模块连接。视频处理 &KVM 模块负责按照用户的热键指令切换不同的视频源输出。视频处理 &KVM 模块还可实现将任意 2 个单路 RHD KVM 的视频信号组合起来输出到一个宽屏显示器上。举例来说，用户看到的效果就是屏幕左边显示的是互联网的界面，屏幕右边显示的是办公专网的界面。此时鼠标和键盘则根据用户选择只在一个界面上使用。本实施例简单 :用户桌面只有一套显示器和键鼠，既省空间又整洁。节省 :结合一台 PC 支持多个用户，本方案整体部署成本显著降低。安全 :桌面没有主机，通过控制 USB 端口，可以控制信息的泄露。

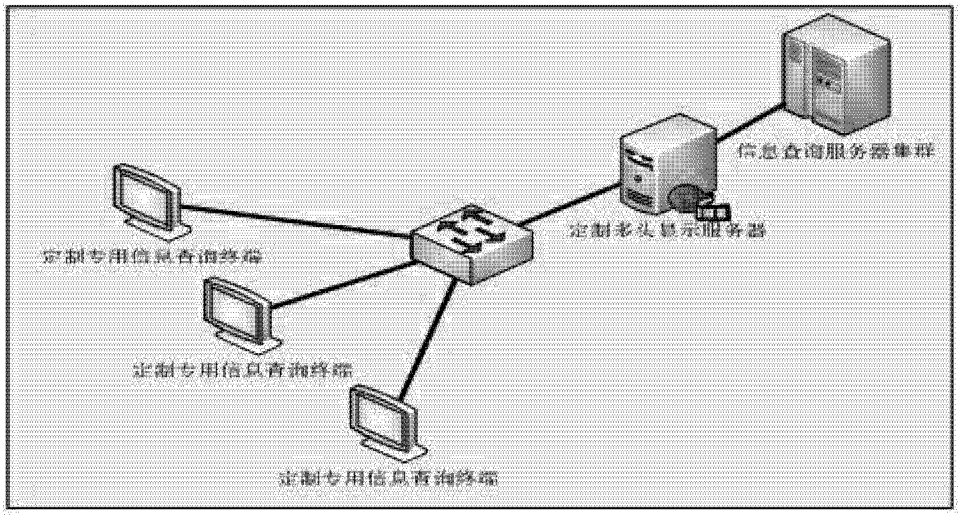

信息查询服务器集群
定制老头显示服务器
定制专用信息查询终端
定制专用信息查询终端
定制专用信息查询终端

图 1

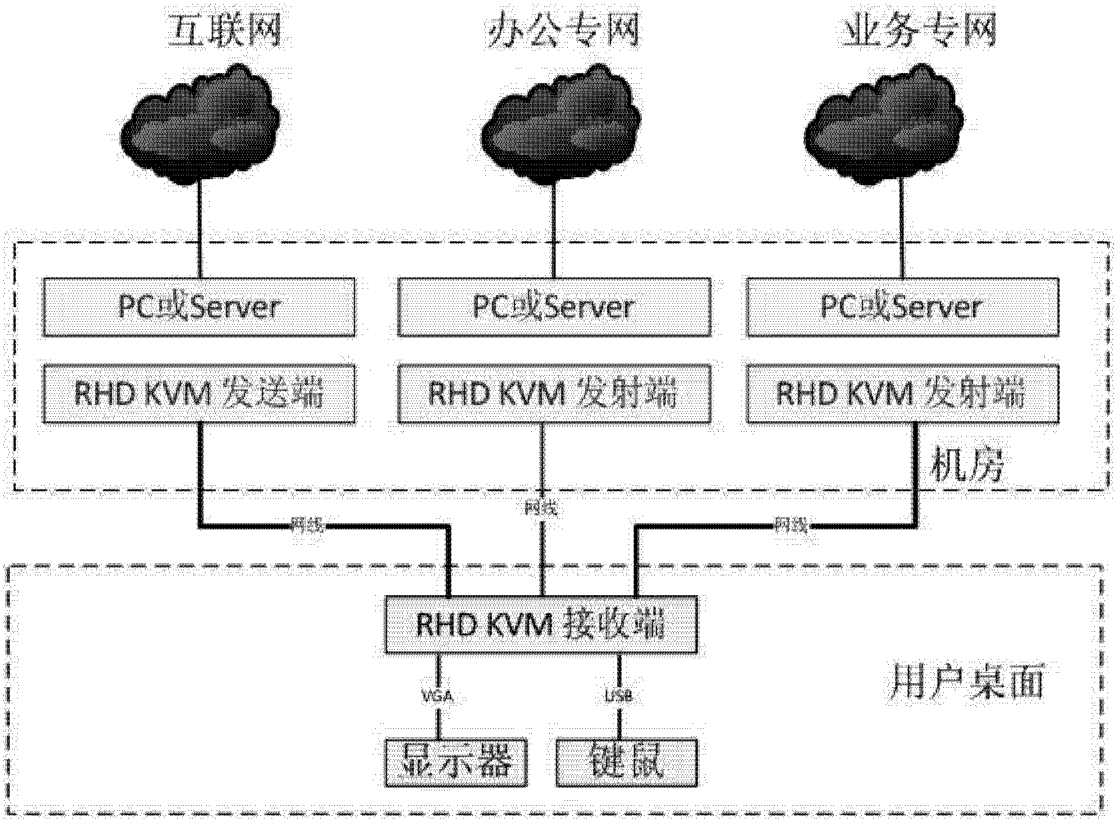

互联网
办公专网
业务专网
PC或Server
PC或Server
PC或Server
RHD KVM 发送端
RHD KVM 发射端
RHD KVM 发射端
机房
网线
网线
网线
RHD KVM 接收端
VGA
USB
显示器
键鼠
用户桌面

图 2

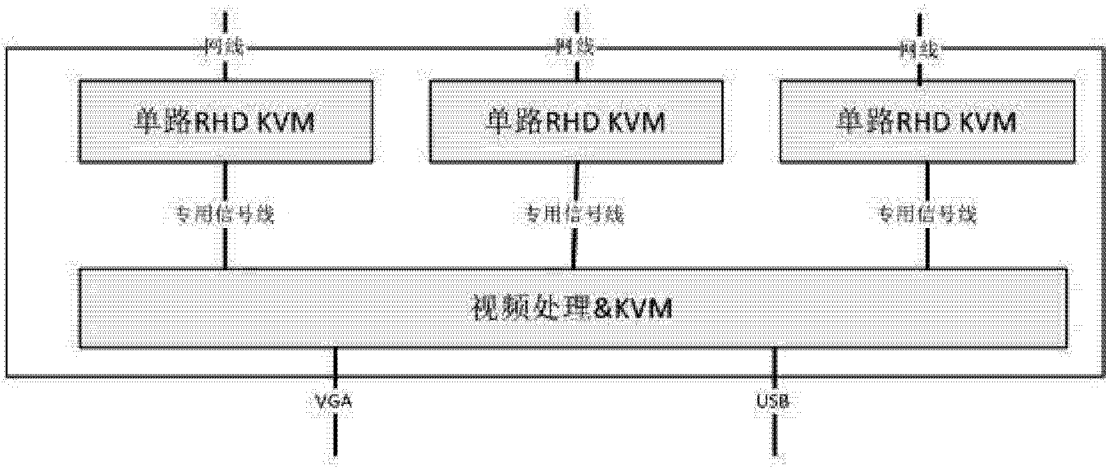

网线
网线
网线
单路RHD KVM
单路RHD KVM
单路RHD KVM
专用信号线
专用信号线
专用信号线
视频处理&KVM
VGA
USB

图 3

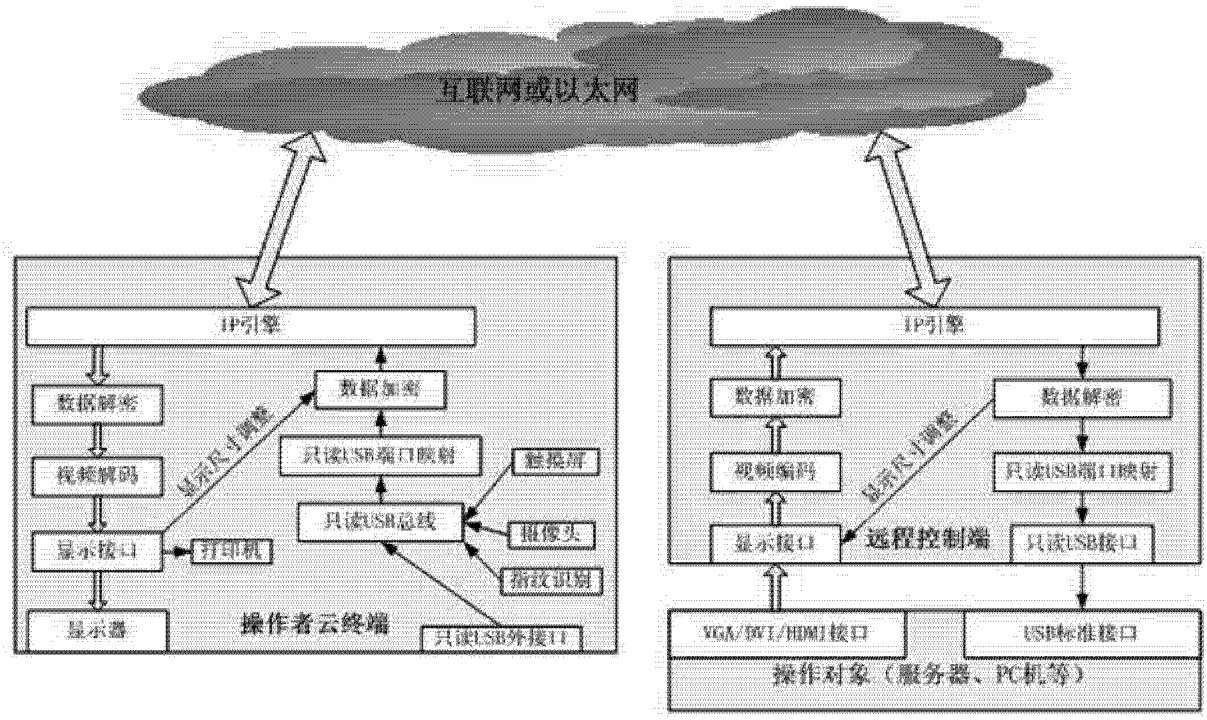

互联网或以太网
IP引擎
数据解密
视频解码
显示接口
显示器
数据加密
只读USB端口映射
只读USB总线
只读USB外接口
显示尺寸调整
打印机
触摸屏
摄像头
指纹识别
操作者云终端
IP引擎
数据加密
视频编码
显示接口
数据解密
只读USB端口映射
只读USB接口
显示尺寸调整
远程控制端
VGA/DVI/HDMI接口
USB标准接口
操作对象（服务器、PC机等）

图 4