(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 111107100 A
(43)申请公布日 2020.05.05

(21)申请号 201911398045.8

(22)申请日 2019.12.30

(71)申请人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6楼

(72)发明人 杨昀桦

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 王茹

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

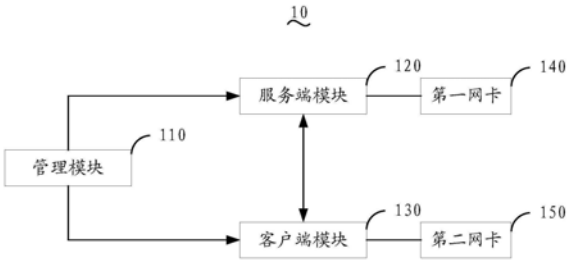
权利要求书1页 说明书6页 附图2页

(54)发明名称

用于传输工业协议流量报文的设备

(57)摘要

本申请提供一种用于传输工业协议流量报文的设备，安装有被配置为同一网段的两个IP地址的两个网卡，装载有管理模块、服务端模块、客户端模块，服务端模块和第一网卡绑定，客户端模块与第二网卡绑定；管理模块分别启动客户端模块和服务端模块；客户端模块用于与服务端模块建立连接，基于指定工业协议生成第一报文，并发送给服务端模块，以及解析服务端模块发送的第二报文；服务端模块解析来自客户端模块的第一报文，并执行第一报文后，基于指定工业协议生成第二报文，发给客户端模块。可以实现无需复制工业现场即可产生工业协议流量应用到非工业环境的应用场景中，并且，只需一台设备实现产生工业协议流量的服务器-客户机架构，环境搭建简便。



CN 111107100 A

1.一种设备，用于传输工业协议流量报文，其特征在于，所述设备安装有两个网卡，两个网卡被配置为同一网段的两个IP地址，所述设备装载有管理模块、服务端模块、客户端模块，所述服务端模块和第一网卡绑定，所述客户端模块与第二网卡绑定；

所述管理模块用于当接收到工业协议流量生成指令时，分别启动所述客户端模块和所述服务端模块；

所述客户端模块用于与所述服务端模块建立连接，基于所述指定工业协议生成第一报文，并发送给所述服务端模块，以及解析所述服务端模块发送的第二报文；

所述服务端模块用于与所述客户端模块建立连接，解析来自所述客户端模块的第一报文，并执行所述第一报文后，基于所述指定工业协议生成第二报文，发给所述客户端模块。

2.根据权利要求1所述的设备，其特征在于，所述设备还包括与所述第二网卡绑定的控制模块，

所述管理模块还用于当接收到工业控制指令时，启动所述客户端模块；

所述客户端模块还用于基于所述指定工业协议生成第三报文，发送给所述控制模块，以使所述控制模块控制所连接的外部设备。

3.根据权利要求2所述的设备，其特征在于，所述服务端模块、所述客户端模块和所述控制模块利用脚本语言实现。

4.根据权利要求3所述的设备，其特征在于，所述设备存储有至少一个工业协议的服务端脚本及客户端脚本。

5.根据权利要求1所述的设备，其特征在于，所述设备还装载有可扩展工具集模块，用于实现所述客户端模块或所述服务端模块的扩展功能。

6.根据权利要求1所述的设备，其特征在于，所述设备还存储有数据库，用于服务端模块在接收到并解析第一报文后，根据解析得到的功能码从所述数据库读取或者写入所述功能码所对应的信息，基于所述对应的信息生成所述第二报文发送给所述客户端模块。

7.根据权利要求1所述的设备，其特征在于，所述管理模块包括WEB组件，所述WEB组件用于提供人机交互的界面。

8.根据权利要求7所述的设备，其特征在于，所述工业协议流量生成指令由用户通过所述WEB组件输入。

9.根据权利要求7所述的设备，其特征在于，所述设备还装载有监控模块，所述监控模块用于监控所述第一网卡与所述第二网卡传输的报文内容，并将监控结果发送给所述管理模块，所述WEB组件还用于可视化展示所述监控结果。

10.根据权利要求7所述的设备，其特征在于，所述WEB组件还用于接收用户输入的更新所述客户端模块或服务端模块功能的配置数据。

用于传输工业协议流量报文的设备

技术领域

[0001] 本申请涉及工业协议应用技术领域，尤其涉及一种用于传输工业协议流量报文的设备。

背景技术

[0002] 工业协议是一种应用在工业自动化的通信协议，包括了许多消息及服务，应用范围与制造自动化有关。目前，工业协议的应用场景不仅仅局限于工业环境中，还可以适用于高校实验室环境、安全设备厂商等应用场景中，例如，将产生的工业协议流量应用到实验设备，对工控安全设备进行防护测试等。由于工业环境具有特殊性，想要完全复制工业现场从而将产生的工业协议流量应用到其他应用场景相对比较困难且不实际。在相关技术中，产生工业协议流量的主要方法为通过在两台计算机上分别手动开启客户端与服务端的模拟器软件，把需要工业协议流量通过的对象串接到客户端与服务端之间，分别在客户端或服务端上进行相关的操作，从而产生对应的工业协议流量通过对象。

[0003] 然而，每一次进行工业协议的发收包操作都需要两台计算机，需要分别手动运行客户端和服务端，环境搭建也较为繁琐，且后期需要更新升级客户端和服务端时，需分别在两台计算机上进行更新。

发明内容

[0004] 为克服相关技术中存在的问题，本申请提供了一种工业协议流量生成装置。

[0005] 本申请实施例提供一种设备，用于传输工业协议流量报文，所述设备安装有两个网卡，两个网卡被配置为同一网段的两个IP地址，所述设备装载有管理模块、服务端模块、客户端模块，所述服务端模块和第一网卡绑定，所述客户端模块与第二网卡绑定；

[0006] 所述管理模块用于当接收到工业协议流量生成指令时，分别启动所述客户端模块和所述服务端模块；

[0007] 所述客户端模块用于与所述服务端模块建立连接，基于所述指定工业协议生成第一报文，并发送给所述服务端模块，以及解析所述服务端模块发送的第二报文；

[0008] 所述服务端模块用于与所述客户端模块建立连接，解析来自所述客户端模块的第一报文，并执行所述第一报文后，基于所述指定工业协议生成第二报文，发给所述客户端模块。

[0009] 在一示例性实施例中，所述设备还包括与所述第二网卡绑定的控制模块，所述管理模块还用于当接收到工业控制指令时，启动所述客户端模块；

[0010] 所述客户端模块还用于基于所述指定工业协议生成第三报文，发送给所述控制模块，以使所述控制模块控制所连接的外部设备。

[0011] 在一示例性实施例中，所述服务端模块、所述客户端模块和所述控制模块利用脚本语言实现。

[0012] 在一示例性实施例中，所述设备存储有至少一个工业协议的服务端脚本及客户端

脚本。

[0013] 在一示例性实施例中，所述设备还装载有可扩展工具集模块，用于实现所述客户端模块或所述服务端模块的扩展功能。

[0014] 在一示例性实施例中，所述设备还存储有数据库，用于服务端模块在接收到并解析第一报文后，根据解析得到的功能码从所述数据库读取或者写入所述功能码所对应的信息，基于所述对应的信息生成所述第二报文发送给所述客户端模块。

[0015] 在一示例性实施例中，所述管理模块包括WEB组件，所述WEB组件用于提供人机交互的界面。

[0016] 在一示例性实施例中，所述工业协议流量生成指令由用户通过所述WEB组件输入。

[0017] 在一示例性实施例中，所述设备还装载有监控模块，所述监控模块用于监控所述第一网卡与所述第二网卡传输的报文内容，并将监控结果发送给所述管理模块，所述WEB组件还用于可视化展示所述监控结果。

[0018] 在一示例性实施例中，所述WEB组件还用于接收用户输入的更新所述客户端模块或服务端模块功能的配置数据。

[0019] 本申请的实施例提供的技术方案可以包括以下有益效果：

[0020] 本技术方案中的用于传输工业协议流量报文的设备，将可以生成工业协议流量所需的客户端和服务端通过绑定两个网卡的形式集成于同一设备，需要使用工业协议流量的设备可以分别与设备中的客户端的网卡及服务端的网卡接入，设备的管理模块在接收到工业协议流量生成指令时，启动客户端模块和服务端模块，客户端模块与服务端模块建立连接，并可以基于指定的工业协议向服务端模块发送第一报文，服务端模块接收并解析第一报文，以及执行第一报文的相关操作，并向客户端模块返回第二报文，客户端模块与服务端模块之间基于指定工业协议的通信交互过程产生指定工业协议的流量，这些工业协议流量可以应用于与客户端的网卡及服务端的网卡连接的需要使用该工业协议流量的设备。这样，可以实现无需复制工业现场即可产生工业协议流量应用到非工业环境的应用场景中，并且，相比于相关技术，本技术方案只需一台设备实现产生工业协议流量的服务器-客户机架构，环境搭建简便，后期需要更新升级客户端和服务端时，只需更新一台设备即可，提高便捷性。

[0021] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

[0022] 此处的附图被并入说明书中并构成本申请的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

[0023] 图1为本申请一示例性实施例示出的一种用于传输工业协议流量报文的设备的结构示意图。

[0024] 图2为本申请一示例性实施例示出的另一种用于传输工业协议流量报文的设备的结构示意图。

具体实施方式

[0025] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0026] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0027] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0028] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0029] 下面结合附图，对本申请的用于传输工业协议流量报文的设备进行详细说明。在不冲突的情况下，下述的实施例及实施方式中的特征可以相互组合。

[0030] 本申请提供了一种用于传输工业协议流量报文的设备，图1为本申请一示例性实施例示出的一种用于传输工业协议流量报文的设备的结构示意图。如图1所示，该用于传输工业协议流量报文的设备10装载有管理模块110、服务端模块120和客户端模块130，所述管理模块110分别与所述服务端模块120、所述客户端模块130通信连接，该设备安装有两个网卡(140、150)，两个网卡被配置为同一网段的两个IP地址，所述服务端模块和第一网卡140绑定，所述客户端模块与第二网卡150绑定，例如，与服务端模块绑定的第一网卡的IP地址被配置为192.168.1.1/24，与客户端模块绑定的第二网卡的IP地址被配置为192.168.1.2/24。该设备通过服务端模块与客户端模块之间的通信交互可以生成工业协议流量给分别与两个网卡连接的外部设备应用。

[0031] 以下对通过服务端模块与客户端模块之间的通信交互生成工业协议流量的实现进行说明：

[0032] 所述管理模块110用于当接收到工业协议流量生成指令时，分别启动所述客户端模块和所述服务端模块；

[0033] 所述客户端模块130用于与所述服务端模块建立连接，基于所述指定工业协议生成第一报文，并发送给所述服务端模块，以及解析所述服务端模块发送的第二报文；

[0034] 所述服务端模块120用于与所述客户端模块建立连接，解析来自所述客户端模块的第一报文，并执行所述第一报文后，基于所述指定工业协议生成第二报文，发给所述客户端模块。

[0035] 本实施例的上述用于传输工业协议流量报文的设备，将可以生成工业协议流量所

需的客户端和服务端通过绑定两个网卡的形式集成于同一设备，需要使用工业协议流量的设备可以分别与设备中的客户端的网卡及服务端的网卡接入，设备的管理模块在接收到工业协议流量生成指令时，启动客户端模块和服务端模块，客户端模块与服务端模块建立连接，并可以基于指定的工业协议向服务端模块发送第一报文，服务端模块接收并解析第一报文，以及执行第一报文的相关操作，并向客户端模块返回第二报文，客户端模块与服务端模块之间基于指定工业协议的通信交互过程产生指定工业协议的流量，这些工业协议流量可以应用于与客户端的网卡及服务端的网卡连接的需要使用该工业协议流量的设备。这样，可以实现无需复制工业现场即可产生工业协议流量应用到非工业环境的应用场景中，并且，相比于相关技术，本技术方案只需一台设备实现产生工业协议流量的服务器-客户机架构，环境搭建简便，后期需要更新升级客户端和服务端时，只需更新一台装置即可，提高便捷性。

[0036] 在本申请一示例性实施例中，两个网卡可以是有线网卡。在本申请另一示例性实施例中，两个网卡可以是无线网卡。

[0037] 在本申请一示例性实施例中，所述设备还包括与所述第二网卡绑定的控制模块，所述管理模块还用于当接收到工业控制指令时，启动所述客户端模块；所述客户端模块还用于基于所述指定工业协议生成第三报文，发送给所述控制模块，以使所述控制模块控制所连接的外部设备。

[0038] 本实施例中，该设备除了具有产生工业协议流量的功能之外，还可以作为工业控制系统中的客户端，当设备的管理模块接收到工业控制指令时，只启动客户端模块，客户端模块可以基于指定工业协议生成第三报文，将第三报文发送给控制模块，控制模块还与第二网卡绑定，控制模块可以将控制指令通过第二网卡发送到连接的外部设备，以控制外部设备，实现工业控制。例如，实现PLC(Programmable Logic Controller，可编程逻辑控制器)等设备的控制。

[0039] 在本申请一示例性实施例中，所述服务端模块、所述客户端模块和所述控制模块利用脚本语言实现。例如，python脚本语言等。

[0040] 在本申请一示例性实施例中，管理模块通过调用Linux内核system函数启动指定工业协议的服务端脚本和客户端脚本。

[0041] 在本申请一示例性实施例中，所述设备存储有至少一个工业协议的服务端脚本及客户端脚本。这样，可以根据工业协议流量生成指令中携带的指定的工业协议信息，或者根据工业控制指令中携带的指定的工业协议信息，调用相对应的服务端脚本及客户端脚本，或者客户端脚本，实现指令所对应的操作。也就是说，该设备可以支持多种工业协议流量的生成，此外，也可以支持基于多种工业协议的工业控制。

[0042] 在本申请一示例性实施例中，所述设备还存储有数据库，用于服务端模块在接收到并解析第一报文后，根据解析得到的功能码从所述数据库读取或者写入所述功能码所对应的信息，基于所述对应的信息生成所述第二报文发送给所述客户端模块。功能码可以标明一个工业协议的报文的用途，例如，读取或者写入。服务端模块接收并解析客户端模块基于工业协议所发送的第一报文后，可以根据解析到的功能码确定从数据库读取或者写入功能码对应的信息。这样，该设备具有数据库可以更好地模拟出外部设备(例如，工控设备)的内部存储点位。例如，当服务端模块解析出从客户端模块发送的第一报文为读起始地址为

0,地址个数为1的值的功能码报文时,则服务端模块通过查询数据库对应于该工业协议的表里的地址为0所对应的值,并将该对应的值生成第二报文返回给客户端,从而完成一次交互。在本申请一示例性实施例中,该数据库为MySQL数据库。

[0043] 在本申请一示例性实施例中,所述服务端脚本、所述客户端脚本通过Python+Socket实现。例如,对于Modbus工业协议,根据报文协议规范,报文中主要字段为功能码、起始地址、地址个数以及值,则可将这些字段作为变量输入,然后使用Struct.pack函数对报文内容进行打包,并通过Socket.send函数将该报文发送至服务端模块;服务端模块通过Socket.recv函数接收来自客户端模块的数据包,并使用Struct.unpack对包进行拆解得到实际的报文内容,对主要字段的内容进行解析。例如,解析到的功能码为读类型功能码,则从MySQL数据库中读取对应信息,并将读取到的信息按照协议规范转换成对应字段信息,并按照客户端模块发包的流程对整个报文进行打包,并发送至客户端模块,客户端模块收到服务端模块返回的报文后,同理进行解析,最终获取到请求的信息,完成整个报文交互过程。若解析为写功能码类型,发收包原理相同,仅对于数据库操作有所不同,若为写功能码,则从请求报文中解析出写服务器的起始地址、地址个数以及值,将对应值写入指定位置的数据库中。在本申请一示例性实施例中,对数据库的操作使用的是Python标准数据库接口Python DB-API,引用MySQL数据库,实现对数据库的增删、查改操作。

[0044] 在本申请一示例性实施例中,所述控制模块为工业协议工具脚本库,工业协议工具脚本库可以存储有至少一个工业协议工具脚本,通过第二网卡与外部设备连接,可以在工业环境内快速进行工业控制操作。例如,S7 PLC控制、S7 PLC资产信息扫描、Profinet DCP设备IP配置等。

[0045] 在本申请一示例性实施例中,所述设备还装载有可扩展工具集模块,用于实现所述客户端模块或所述服务端模块的扩展功能。例如,用户可以根据需求将自定义的扩展功能的脚本加载到可扩展工具集模块,以对客户端模块和服务端模块进行扩展和更新。

[0046] 在本申请一示例性实施例中,所述管理模块包括WEB组件,所述WEB组件用于提供人机交互的界面。

[0047] 在本申请一示例性实施例中,所述工业协议流量生成指令由用户通过所述WEB组件输入。这样,用户可以通过WEB组件选择使用该设备的工业协议流量生成功能。应该理解的是,所述工业控制指令也可以是用户通过WEB组件输入的。

[0048] 在本申请一示例性实施例中,所述WEB组件还用于接收用户输入的更新所述客户端模块或服务端模块功能的配置数据。例如,用户添加扩展功能的脚本也可以通过WEB组件导入加载可扩展工具集模块。例如,可以采用流式套接字(SOCK-STREAM)、数据报套接字(SOCK-DGRAM)或者原始套接字(SOCK-RAW)进行通信,并通过WEB组件导入可扩展工具集模块。

[0049] 在本申请一示例性实施例中,所述设备还装载有监控模块,所述监控模块用于监控所述第一网卡与所述第二网卡传输的报文内容,并将监控结果发送给所述管理模块,所述WEB组件还用于可视化展示所述监控结果。便于用户通过WEB组件的界面对报文内容进行查看。例如,可以通过TCP Dump参数将第一网卡与第二网卡传输的报文内容写入文档中,对文档内的内容采用正则匹配分离出五元组以及应用层报文信息,并使用Java将处理后的应用层报文信息展示到WEB组件的界面。

[0050] 在本申请一示例性实施例中，所述监控模块还用于监控所述第一网卡与所述第二网卡的发包结果。这样，可以从发包结果得到客户端模块与服务端模块的连接状态，连接状态也可以通过WEB最贱进行可视化展示，以便用户可以对连接状态进行实时监控。

[0051] 在本申请一示例性实施例中，所述设备还装载有配置模块，所述配置模块可以用于配置网卡的IP地址、WEB组件的界面等。

[0052] 图2为本申请一示例性实施例示出的另一种用于传输工业协议流量报文的设备的结构示意图。如图2所示，该设备20装载有Linux系统，在Linux系统中，装载有系统管理模块210、工业协议发收包模块220及工业协议可扩展工具集模块230，系统管理模块210分别与工业协议发收包模块220、工业协议可扩展工具集模块230通信连接，工业协议发收包模块220与工业协议可扩展工具集模块230通信连接。该设备安装有两个网卡，两个网卡被配置为同一网段的两个IP地址。其中：

[0053] 系统管理模块210包括监控子模块211、系统配置子模块212以及功能配置子模块213；

[0054] 工业协议发收包模块220包括服务端子模块221及客户端子模块222，服务端子模块与第一网卡绑定，客户端子模块与第二网卡绑定；

[0055] 工业协议可扩展工具集模块230包括工业协议客户服务端脚本库231、工业协议工具脚本库232、扩展脚本库233。

[0056] 本实施例的各模块与前述实施例的相关模块的功能相同，在此不再进行赘述。

[0057] 上述对本申请特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0058] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

[0059] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

[0060] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本申请记载的范围。

[0061] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

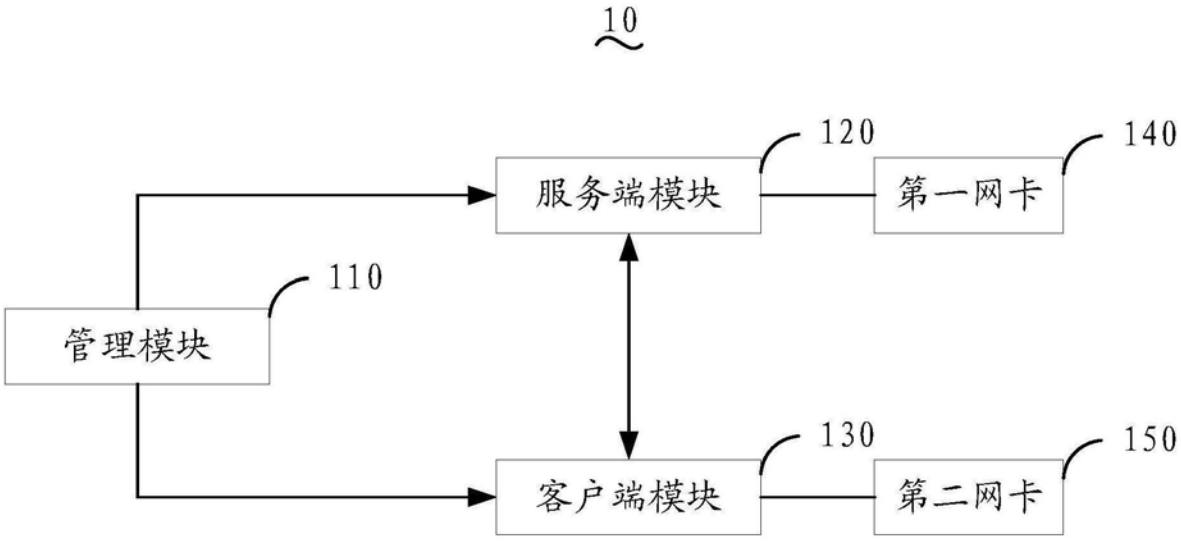


图1

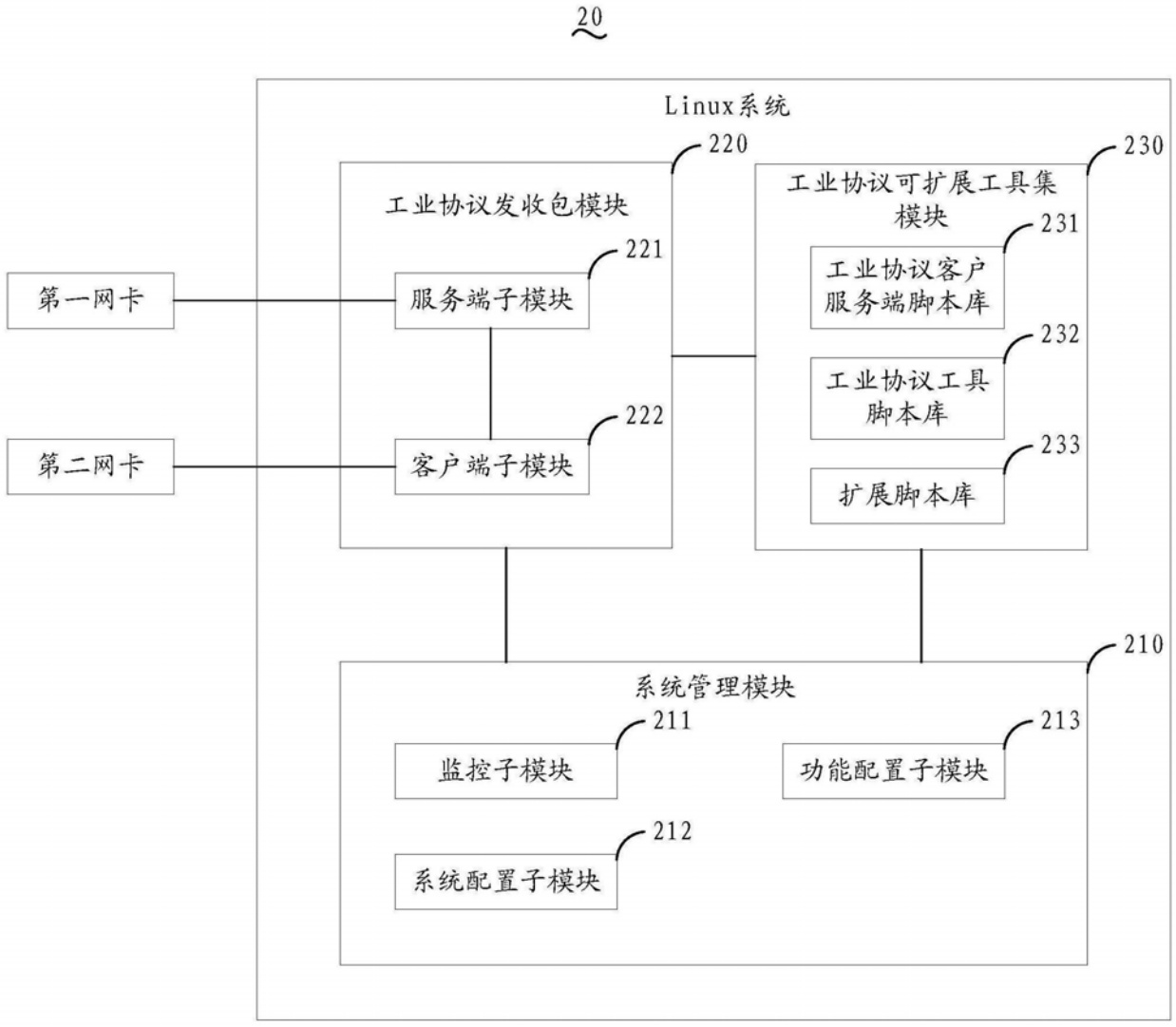

20
Linux系统
220
工业协议发收包模块
221
服务端子模块
222
客户端子模块
第一网卡
第二网卡
230
工业协议可扩展工具集模块
231
工业协议客户服务端脚本库
232
工业协议工具脚本库
233
扩展脚本库
210
系统管理模块
211
监控子模块
212
系统配置子模块
213
功能配置子模块

图2