(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 109150661 A
(43)申请公布日 2019.01.04

(21)申请号 201811005577.6

(22)申请日 2018.08.30

(71)申请人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 宋小恒

(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 林祥

(51)Int.Cl.
H04L 12/26(2006.01)
H04W 8/00(2009.01)

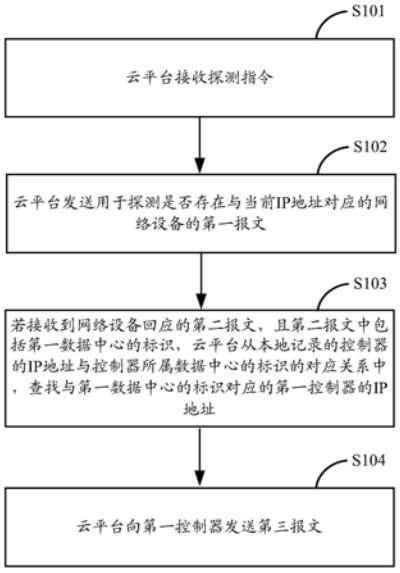
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种设备发现方法及装置

(57)摘要

本发明实施例提供一种设备发现方法及装置，本发明中，云平台基于IP地址探测网络设备，并在探测过程中获取网络设备所属数据中心的标识以及网络设备的设备信息，将网络设备的设备信息通知给网络设备所属数据中心的控制器，使控制器本地添加与其属于同一数据中心的网络设备的设备信息。实现网络设备的自动发现，提升控制器发现网络设备的效率。



CN 109150661 A

1.一种设备发现方法,应用于云平台,其特征在于,所述方法包括:

接收探测指令,所述探测指令中包括待探测的地址段;

对所述地址段中每一个IP地址执行如下操作:

发送用于探测当前IP地址是否存在对应的网络设备的第一报文,所述第一报文的目的IP地址为所述当前IP地址;

若接收到所述网络设备回应的第二报文,且所述第二报文中包括第一数据中心的标识,从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中,查找与所述第一数据中心的标识对应的第一控制器的IP地址,其中,所述第一数据中心为所述网络设备所属的数据中心;

向所述第一控制器发送第三报文,所述第三报文中包括所述第二报文中包括的所述网络设备的设备信息。

2.如权利要求1所述的方法,其特征在于,所述第一报文中包括用于标识所述云平台身份的认证信息,以使所述网络设备基于所述认证信息确认所述云平台身份合法时,向所述云平台回应所述第二报文。

3.如权利要求2所述的方法,其特征在于,所述认证信息为所述云平台的数字证书,所述第二报文中包括所述网络设备利用所述数字证书的公钥加密的第一信息,所述第一信息包括所述第一数据中心的标识和所述网络设备的设备信息;

所述若接收到所述网络设备回应的第二报文之后,还包括:

利用所述数字证书的私钥对所述第一信息进行解密。

4.如权利要求1所述的方法,其特征在于,所述若接收到所述网络设备回应的第二报文之后,还包括:

向所述网络设备发送第四报文,所述第四报文中包括所述第一控制器的IP地址,以使所述网络设备基于所述第一控制器的IP地址,允许所述第一控制器对其进行配置管理。

5.如权利要求4所述的方法,其特征在于,所述第一报文中包括所述云平台支持的加密算法,所述第二报文中包括所述网络设备从所述云平台支持的加密算法中选择的第一加密算法和密钥;所述向所述网络设备发送第四报文,还包括:

利用所述第一加密算法和所述密钥,对所述第一控制器的IP地址进行加密;

将加密后的所述第一控制器的IP地址,通过所述第四报文发送至所述网络设备。

6.如权利要求1所述的方法,其特征在于,所述方法还包括:

若接收到所述网络设备回应的第二报文,且所述第二报文中不包括数据中心的标识,确定所述网络设备为不属于任一数据中心的汇聚设备;

本地添加所述第二报文中包括的所述网络设备的设备信息。

7.一种设备发现装置,应用于云平台,其特征在于,所述装置包括:

接收单元,用于接收探测指令,所述探测指令中包括待探测的地址段;

发送单元,用于发送用于探测当前IP地址是否存在对应的网络设备的第一报文,所述第一报文的目的IP地址为所述当前IP地址;

查找单元,用于若接收到所述网络设备回应的第二报文,且所述第二报文中包括第一数据中心的标识,从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中,查找与所述第一数据中心的标识对应的第一控制器的IP地址,其中,所述第一数据中心

为所述网络设备所属的数据中心；

所述发送单元，还用于向所述第一控制器发送第三报文，所述第三报文中包括所述第二报文中包括的所述网络设备的设备信息。

8.如权利要求7所述的装置，其特征在于，所述第一报文中包括用于标识所述云平台身份的认证信息，以使所述网络设备基于所述认证信息确认所述云平台身份合法时，向所述云平台回应所述第二报文。

9.如权利要求8所述的装置，其特征在于，所述认证信息为所述云平台的数字证书，所述第二报文中包括所述网络设备利用所述数字证书的公钥加密的第一信息，所述第一信息包括所述第一数据中心的标识和所述网络设备的设备信息；

所述装置还包括：

解密单元，用于利用所述数字证书的私钥对所述第一信息进行解密。

10.如权利要求7所述的装置，其特征在于：

所述发送单元，还用于向所述网络设备发送第四报文，所述第四报文中包括所述第一控制器的IP地址，以使所述网络设备基于所述第一控制器的IP地址，允许所述第一控制器对其进行配置管理。

11.如权利要求10所述的装置，其特征在于，所述第一报文中包括所述云平台支持的加密算法，所述第二报文中包括所述网络设备从所述云平台支持的加密算法中选择的第一加密算法和密钥；

所述发送单元，具体用于利用所述第一加密算法和所述密钥，对所述第一控制器的IP地址进行加密；将加密后的所述第一控制器的IP地址，通过所述第四报文发送至所述网络设备。

12.如权利要求7所述的装置，其特征在于，所述装置还包括：

确定单元，用于若接收到所述网络设备回应的第二报文，且所述第二报文中不包括数据中心的标识，确定所述网络设备为不属于任一数据中心的汇聚设备；

添加单元，用于本地添加所述第二报文中包括的所述网络设备的设备信息。

一种设备发现方法及装置

技术领域

[0001] 本发明涉及网络通信技术领域,尤其涉及一种设备发现方法及装置。

背景技术

[0002] SDN(Software Defined Networks,软件定义网络)是一种新型的网络创新架构,通过控制平面和数据平面分离,实现网络流量的灵活控制。

[0003] 在基于SDN构建的数据中心中,网络管理员需要将网络设备的设备信息手动录入控制器。控制器基于录入的设备信息,发现待接入数据中心的网络设备,进而对网络设备进行配置管理。

[0004] 在跨数据中心的网络中,网络管理员需要针对每一个数据中心执行上述录入操作,需要录入的设备信息量极大。即使采用文件方式将设备信息批量导入控制器,但文件中的设备信息仍需网络管理员手动维护,导致控制器发现网络设备的效率不高。

发明内容

[0005] 本发明为了解决现有控制器发现网络设备的效率不高的问题,提出一种设备发现方法及装置,用以提升控制器发现网络设备的效率。

[0006] 为实现上述发明目的,本发明提供了如下技术方案:

[0007] 第一方面,本发明提供一种设备发现方法,应用于云平台,所述方法包括:

[0008] 接收探测指令,所述探测指令中包括待探测的地址段;

[0009] 对所述地址段中每一个IP地址执行如下操作:

[0010] 发送用于探测当前IP地址是否存在对应的网络设备的第一报文,所述第一报文的目的IP地址为所述当前IP地址;

[0011] 若接收到所述网络设备回应的第二报文,且所述第二报文中包括第一数据中心的标识,从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中,查找与所述第一数据中心的标识对应的第一控制器的IP地址,其中,所述第一数据中心为所述网络设备所属的数据中心;

[0012] 向所述第一控制器发送第三报文,所述第三报文中包括所述第二报文中包括的所述网络设备的设备信息。

[0013] 第二方面,本发明提供一种设备发现装置,应用于云平台,所述装置包括:

[0014] 接收单元,用于接收探测指令,所述探测指令中包括待探测的地址段;

[0015] 发送单元,用于发送用于探测当前IP地址是否存在对应的网络设备的第一报文,所述第一报文的目的IP地址为所述当前IP地址;

[0016] 查找单元,用于若接收到所述网络设备回应的第二报文,且所述第二报文中包括第一数据中心的标识,从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中,查找与所述第一数据中心的标识对应的第一控制器的IP地址,其中,所述第一数据中心为所述网络设备所属的数据中心;

[0017] 所述发送单元，还用于向所述第一控制器发送第三报文，所述第三报文中包括所述第二报文中包括的所述网络设备的设备信息。

[0018] 由以上描述可以看出，本发明中，云平台基于待探测地址段中的每一个IP地址探测网络设备，并在探测过程中获取网络设备所属数据中心的标识以及网络设备的设备信息，将网络设备的设备信息通知给网络设备所属数据中心的控制器，使控制器本地添加与其属于同一数据中心的网络设备的设备信息。实现网络设备的自动发现，提升控制器发现网络设备的效率。

附图说明

[0019] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0020] 图1是本发明实施例示出的一种设备发现方法流程图；

[0021] 图2是本发明实施例示出的跨数据中心网络示意图；

[0022] 图3A是本发明实施例示出的Packet1中包括的ICMP报文的示例；

[0023] 图3B是本发明实施例示出的Packet2中包括的ICMP报文的示例；

[0024] 图3C是本发明实施例示出的Packet3中包括的ICMP报文的示例；

[0025] 图3D是本发明实施例示出的Packet4中包括的ICMP报文的示例；

[0026] 图4是本发明实施例示出的一种设备发现装置的结构示意图。

具体实施方式

[0027] 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发明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、本发明的一些方面相一致的装置和方法的例子。

[0028] 在本发明使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明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。

[0029] 应当理解，尽管在本发明可能采用术语第一、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，在不脱离本发明范围的情况下，协商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协商信息。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”。

[0030] 在跨数据中心的网络中，网络管理员需要在每一个数据中心的控制器上，手动录入与控制器属于同一数据中心的网络设备的设备信息，工作量极大，出错率较高。即使采用文件方式将设备信息批量导入控制器，但文件中的设备信息仍需网络管理员手动维护，导致控制器发现网络设备的效率不高。

[0031] 针对上述问题，本发明实施例提供一种设备发现方法，该方法中，云平台基于待探测地址段中的每一个IP地址探测网络设备，并在探测过程中获取网络设备所属数据中心的标识以及网络设备的设备信息，将网络设备的设备信息通知给网络设备所属数据中心的控制器，使控制器本地添加与其属于同一数据中心的网络设备的设备信息。实现网络设备的自动发现，提升控制器发现网络设备的效率。

[0032] 为了使本发明实施例的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明实施例执行详细描述：

[0033] 参见图1，为本发明实施例提供的设备发现方法的流程图。该流程应用于云平台。

[0034] 如图1所示，该流程可包括以下步骤：

[0035] 步骤101，云平台接收探测指令。

[0036] 该探测指令中包括待探测的地址段。

[0037] 在具体实现时，可由网络管理员在云平台上输入待探测的地址段，生成探测指令，触发云平台执行后续的探测操作。

[0038] 这里，需要补充说明的是，在网络初始规划时，已预先划分可供网络设备使用的IP地址范围(即地址段)。当网络设备加入时，从预先划分的IP地址范围中为网络设备分配IP地址。

[0039] 步骤102，云平台发送用于探测是否存在与当前IP地址对应的网络设备的第一报文。

[0040] 其中，第一报文的目的IP地址为当前IP地址，当前IP地址即为云平台当前正在执行探测的IP地址。这里，第一报文只是为便于描述而进行的命名，并非用于限定。

[0041] 在本发明中，云平台对待探测地址段内的每一个IP地址均执行探测操作。作为一个实施例，本发明可基于对ICMP(Internet Control Message Protocol，网际控制报文协议)的扩展实现探测过程。具体报文格式在下文中会有描述，这里暂不赘述。

[0042] 步骤103，若接收到网络设备回应的第二报文，且第二报文中包括第一数据中心的标识，云平台从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中，查找与第一数据中心的标识对应的第一控制器的IP地址。

[0043] 这里，第一数据中心为网络设备所属的数据中心。也就是说，网络设备通过第二报文将自己所属数据中心(即第一数据中心)的信息(标识)通告给云平台。

[0044] 若云平台接收到网络设备回应的第二报文，说明网络中存在与当前IP地址对应的网络设备，则本地查找网络设备所属数据中心(第一数据中心)的控制器(第一控制器)。

[0045] 这里，第二报文、第一数据中心、第一控制器只是为便于描述而进行的命名，并非用于限定。

[0046] 步骤104，云平台向第一控制器发送第三报文。

[0047] 该第三报文中包括第二报文中包括的网络设备的设备信息，比如，网络设备的IP地址、网络设备支持的配置协议的用户账号和密码。这里，第三报文只是为便于描述而进行的命名，并非用于限定。

[0048] 第一控制器本地添加接收到的网络设备的设备信息，可根据添加的设备信息对网络设备执行纳管等操作。

[0049] 至此，完成图1所示流程。

[0050] 通过图1所示流程可以看出，在本发明实施例中，云平台基于待探测地址段中的每一个IP地址探测网络设备，并在探测过程中获取网络设备所属数据中心的标识以及网络设备的设备信息，将网络设备的设备信息通知给网络设备所属数据中心的控制器，使控制器本地添加与其属于同一数据中心的网络设备的设备信息。实现网络设备的自动发现，提升控制器发现网络设备的效率。

[0051] 作为一个实施例，第一报文中包括用于标识云平台身份的认证信息。网络设备基于该认证信息确认云平台身份合法时，向云平台回应第二报文。以提升探测过程的安全性。

[0052] 作为一个实施例，用于标识云平台身份的认证信息可为云平台的数字证书。网络设备利用数字证书的公钥对第一信息进行加密，这里，第一信息包括网络设备所属第一数据中心的标识以及网络设备的设备信息，之所以称为第一信息，只是为便于描述而进行的命名，并非用于限定。网络设备将加密后的第一信息通过第二报文发送至云平台。

[0053] 云平台接收到网络设备回应的第二报文之后，利用数字证书的私钥对第一信息进行解密，以获取网络设备通告的第一数据中心的标识和网络设备的设备信息。当前，第一信息中还可包括其它交互内容，本发明不对第一信息的具体内容进行限定。

[0054] 现有技术中，设备信息由网络管理员手动录入控制器，不涉及信息传输安全性问题。而本发明实施例中，设备信息需要在网络设备与云平台之间传输，因此，需要考虑信息传输的安全性。本发明实施例利用数字证书对设备信息进行加密，从而提升设备信息传输的安全性。

[0055] 作为一个实施例，云平台接收网络设备回应的第二报文之后，可向网络设备发送第四报文，该第四报文中包括第一控制器的IP地址。这里，第四报文只是为便于描述而进行的命名，并非用于限定。

[0056] 网络设备基于第一控制器的IP地址，确认自身需要通过第一控制器接入数据中心。从而在后续接收到控制器发送的携带配置协议账号和密码的配置连接请求时，基于控制器的IP地址确定发起配置连接请求的控制器是否为第一控制器，若为第一控制器且配置协议的账号和密码正确，则确定当前控制器身份合法，允许当前控制器对其进行配置管理，即仅允许经过身份验证的控制器对其进行配置管理，以提升配置管理的安全性。

[0057] 作为一个实施例，第一报文中还包括云平台支持的加密算法。网络设备接收到第一报文后，从云平台支持的加密算法中选择一个加密算法(记为第一加密算法)，并将第一加密算法以及用于后续信息加密的密钥通过第二报文发送至云平台。

[0058] 云平台向网络设备发送第四报文，包括：利用网络设备通告的第一加密算法以及密钥，对第一控制器的IP地址进行加密，将加密后的第一控制器的IP地址，通过第四报文发送至网络设备。网络设备利用第一加密算法和密钥解密后，获取到第四报文中包括的第一控制器的IP地址。

[0059] 现有技术中，控制器的IP地址直接配置在网络设备中，不需要通过网络传输，因此，不涉及传输安全性问题。而本发明实施例中，控制器的IP地址需要在网络设备与云平台之间传输，因此，需要考虑传输安全性。本发明实施例利用加密算法和密钥对控制器的IP地址进行加密，从而提升控制器的IP地址通过网络传输的安全性。

[0060] 此外，网络设备在接收到第四报文之后，可向云平台回应第五报文，用以通告云平台允许第一控制器对其进行配置管理。这里，第五报文只是为便于描述而进行的命名，并非

用于限定。

[0061] 云平台可在接收到第五报文之后，向第一控制器发送第三报文(该第三报文中包括网络设备的设备信息)，以触发第一控制器对网络设备进行配置管理。

[0062] 值得一提的是，在跨数据中心的网络中，还存在一些不属于任一数据中心的汇聚设备。这些汇聚设备负责连接各数据中心的边缘设备。本发明实施例可实现对汇聚设备的发现。具体为，若云平台接收到网络设备回应的第二报文，且第二报文中不包括数据中心的标识，则确定该网络设备为不属于任一数据中心的汇聚设备。云平台本地添加第二报文中包括的网络设备的设备信息。即本发明实施例可实现云平台对汇聚设备的自动发现，而无需在云平台上手动配置汇聚设备的设备信息。

[0063] 下面通过具体实施例对本发明实施例提供的方法进行描述：

[0064] 参见图2，为跨数据中心网络示意图。该网络包含云平台Platform2000、数据中心1、数据中心2。其中，数据中心1包含控制器Controll2101(通常为控制器集群)、网络设备SW2201～SW2230以及用户服务器Server2301～Server2500；数据中心2包含控制器Controll2102(通常为控制器集群)、网络设备SW2231～SW2260以及用户服务器Server2501～Server2700。用户服务器通过网络设备接入数据中心。

[0065] 网络管理员在Platform2000上输入网络设备的地址段，以一个地址段为例，比如，该地址段为172.15.1.0-172.15.10.255，生成包括该地址段的探测指令。

[0066] Platform2000基于该探测指令中包括的地址段(172.15.1.0-172.15.10.255)，对该地址段中的每一个IP地址进行探测。

[0067] 以IP地址172.15.1.1为例，Platform2000发送用于探测IP地址172.15.1.1是否存在对应的网络设备的报文，记为Packet1。Packet1的源IP地址为Platform2000的IP地址，目的IP地址为172.15.1.1。Packet1可基于扩展的ICMP报文实现，具体参见图3A，为Packet1中包括的ICMP报文的示例。其中，类型字段、代码字段、校验和字段、序列号字段均为现有ICMP字段，在此不再赘述；标识字段用于表示当前ICMP报文属于云平台进行设备探测的ICMP报文，以区别于现有ICMP报文；数据字段可携带Platform2000的数字证书、支持的配置协议、支持的加密算法。

[0068] 若网络中存在IP地址为172.15.1.1的网络设备，比如，数据中心1中的SW2201的IP地址为172.15.1.1，则SW2201接收到Packet1后，通过识别Packet1中的标识字段，确定当前ICMP报文属于云平台进行设备探测的ICMP报文，因此，获取Packet1中携带的ICMP报文的数据。如前所述，该数据包括Platform2000的数字证书、支持的配置协议、支持的加密算法。

[0069] SW2201验证接收到的数字证书是否有效，若该证书有效，则认为Platform2000的身份合法。同时，SW2201可确认Platform2000支持的配置协议中是否包括本设备支持的配置协议(比如，NETCONF协议)；并从Platform2000支持的加密算法中选择一种加密算法(记为A1)。

[0070] SW2201在确认Platform2000身份合法后，利用Platform2000的数字证书的公钥对SW2201所属数据中心(数据中心1)的标识(记为Center1)、SW2201的配置协议的用户账号和密码、加密算法A1、以及用于后续信息加密的密钥(记为Key1)进行加密，并通过Packet2发送至Platform2000。该Packet2中包括的ICMP报文格式，如图3B所示。

[0071] Platform2000接收到Packet2(源IP地址为172.15.1.1)后，可确认网络中存在IP

地址为172.15.1.1的网络设备(SW2201)。Platform2000利用自身数字证书的私钥对Packet2中包括的ICMP报文的数据字段进行解密，获取SW2201所属数据中心的标识(Center1)、SW2201的配置协议的用户账号和密码、加密算法(A1)、密钥(Key1)。

[0072] Platform2000查询本地记录的数据中心的标识与控制器的IP地址的对应关系，如表1所示。

[0073]

数据中心的标识	控制器的IP地址
Center1	IP2101
Center2	IP2102

[0074] 表1

[0075] 从表1中可查询到，SW2201所属数据中心(标识为Center1)的控制器的IP地址为IP2101(图2中Controller2101的IP地址)，则Platform2000利用加密算法(A1)、密钥(Key1)对IP2101进行加密，并通过Packet3发送至SW2201。该Packet3中包括的ICMP报文格式，如图3C所示。

[0076] SW2201接收到Packet3后，利用加密算法(A1)、密钥(Key1)对Packet3中包括的ICMP报文的数据字段进行解密，获取待接入控制器的IP地址(IP2101)并记录。SW2201向Platform2000发送Packet4，Packet4中包括的ICMP报文格式，如图3D所示。其中，数据字段为空(Null)。

[0077] Platform2000接收到Packet4后，向Controller2101(IP地址为IP2101)发送Packet5，Packet5中包括SW2201的IP地址(172.15.1.1)、SW2201的配置协议的用户账号和密码。

[0078] Controller2101向SW2201发送配置连接请求(源IP地址为IP2101，目的IP地址为172.15.1.1)，该配置连接请求中携带SW2201的配置协议的用户账号和密码。SW2201将配置连接请求的源IP地址与本地记录的控制器的IP地址(IP2101)进行比对，若IP地址一致，且配置协议的用户账号和密码正确，则允许控制器(Controller2101)对其下发配置信息(包括Openflow协议配置等)。SW2201基于配置信息与Controller2101建立连接，即接入数据中心1。

[0079] 至此，完成对本实施例的描述。

[0080] 以上对本发明实施例提供的方法进行了描述，下面对本发明实施例提供的装置进行描述：

[0081] 参见图4，为本发明实施例提供的装置的结构示意图。该设备发现装置包括：接收单元401、发送单元402以及查找单元403，其中：

[0082] 接收单元401，用于接收探测指令，所述探测指令中包括待探测的地址段；

[0083] 发送单元402，用于发送用于探测当前IP地址是否存在对应的网络设备的第一报文，所述第一报文的目的IP地址为所述当前IP地址；

[0084] 查找单元403，用于若接收到所述网络设备回应的第二报文，且所述第二报文中包括第一数据中心的标识，从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中，查找与所述第一数据中心的标识对应的第一控制器的IP地址，其中，所述第一数据中心为所述网络设备所属的数据中心；

[0085] 所述发送单元402,还用于向所述第一控制器发送第三报文,所述第三报文中包括所述第二报文中包括的所述网络设备的设备信息。

[0086] 作为一个实施例,所述第一报文中包括用于标识所述云平台身份的认证信息,以使所述网络设备基于所述认证信息确认所述云平台身份合法时,向所述云平台回应所述第二报文。

[0087] 作为一个实施例,所述认证信息为所述云平台的数字证书,所述第二报文中包括所述网络设备利用所述数字证书的公钥加密的第一信息,所述第一信息包括所述第一数据中心的标识和所述网络设备的设备信息;

[0088] 所述装置还包括:

[0089] 解密单元,用于利用所述数字证书的私钥对所述第一信息进行解密。

[0090] 作为一个实施例,所述发送单元402,还用于向所述网络设备发送第四报文,所述第四报文中包括所述第一控制器的IP地址,以使所述网络设备基于所述第一控制器的IP地址,允许所述第一控制器对其进行配置管理。

[0091] 作为一个实施例,所述第一报文中包括所述云平台支持的加密算法,所述第二报文中包括所述网络设备从所述云平台支持的加密算法中选择的第一加密算法和密钥;

[0092] 所述发送单元402,具体用于利用所述第一加密算法和所述密钥,对所述第一控制器的IP地址进行加密;将加密后的所述第一控制器的IP地址,通过所述第四报文发送至所述网络设备。

[0093] 作为一个实施例,所述装置还包括:

[0094] 确定单元,用于若接收到所述网络设备回应的第二报文,且所述第二报文中不包括数据中心的标识,确定所述网络设备为不属于任一数据中心的汇聚设备;

[0095] 添加单元,用于本地添加所述第二报文中包括的所述网络设备的设备信息。

[0096] 至此,完成图4所示装置的描述。

[0097] 本发明实施例中,云平台基于待探测地址段中的每一个IP地址探测网络设备,并在探测过程中获取网络设备所属数据中心的标识以及网络设备的设备信息,将网络设备的设备信息通知给网络设备所属数据中心的控制器,使控制器本地添加与其属于同一数据中心的网络设备的设备信息,实现网络设备的自动发现,提升控制器发现网络设备的效率。

[0098] 以上所述仅为本发明实施例的较佳实施例而已,并不用以限制本发明,凡在本发明实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明保护的范围之内。

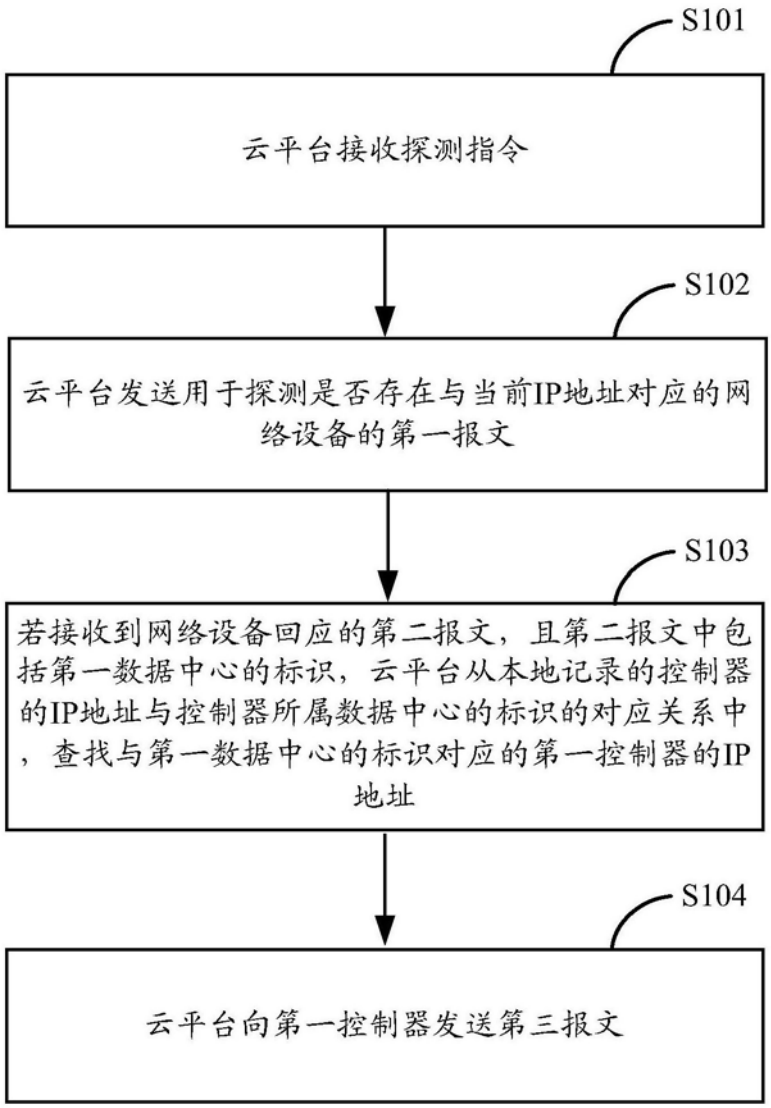

S101
云平台接收探测指令
S102
云平台发送用于探测是否存在与当前IP地址对应的网络设备的第一报文
S103
若接收到网络设备回应的第二报文，且第二报文中包括第一数据中心的标识，云平台从本地记录的控制器的IP地址与控制器所属数据中心的标识的对应关系中，查找与第一数据中心的标识对应的第一控制器的IP地址
S104
云平台向第一控制器发送第三报文

图1

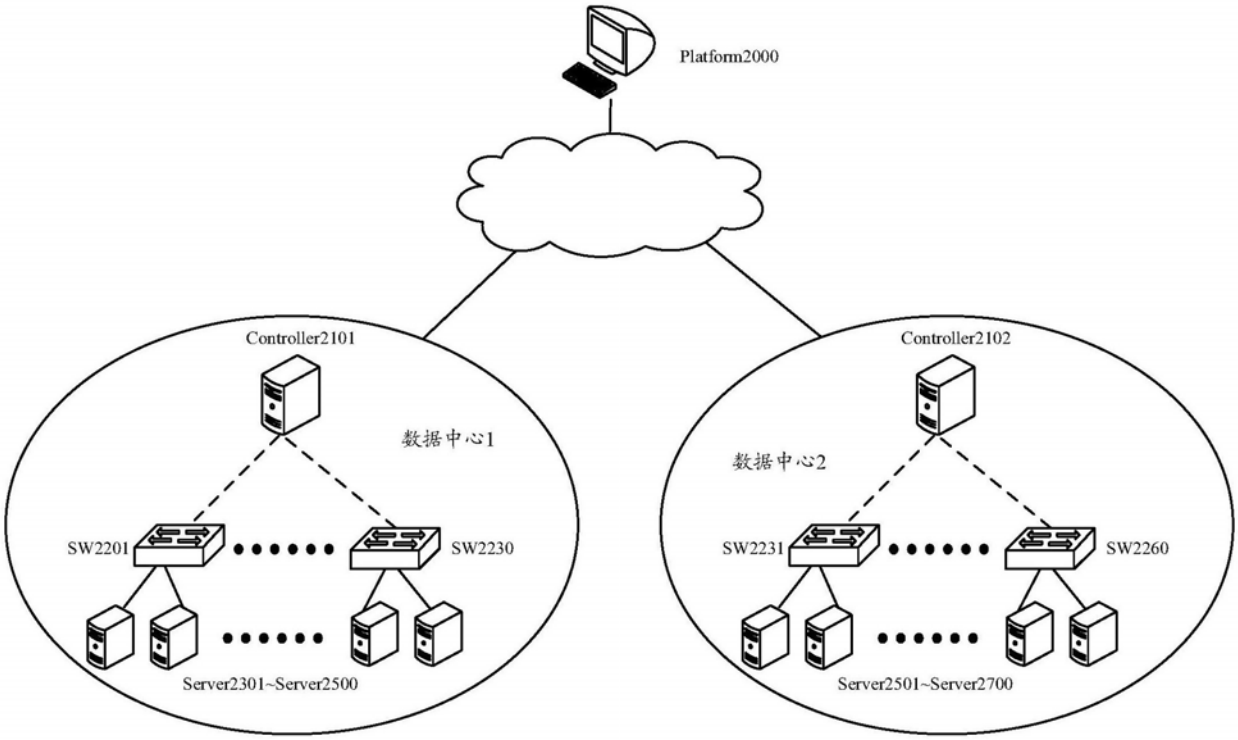


图2

类型	代码	校验和
标识		序列号
数据（包括数字证书、支持的配置协议、支持的加密算法）		

图3A

类型	代码	校验和
标识		序列号
数据（包括数据中心的标识、配置协议的用户账号和密码、加密算法和密钥）		

图3B

类型	代码	校验和
标识		序列号
数据（包括控制器的IP地址）		

图3C

类型	代码	校验和
标识		序列号
数据（Null）		

图3D

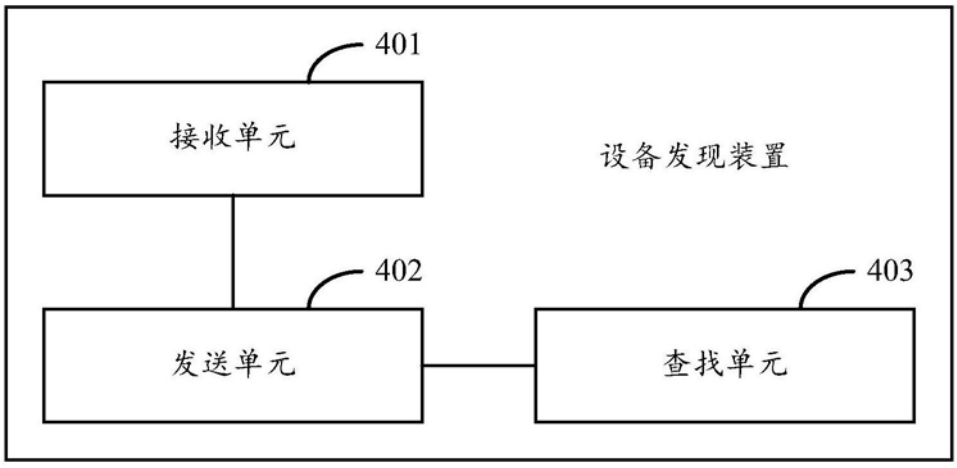


图4