(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 111010362 B
(45)授权公告日 2021.09.21

(21)申请号 201910212398.8

(22)申请日 2019.03.20

(65)同一申请的已公布的文献号
申请公布号 CN 111010362 A

(43)申请公布日 2020.04.14

(73)专利权人 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 侯叶飞

(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 29/06(2006.01)
H04L 12/46(2006.01)
H04L 29/12(2006.01)

(56)对比文件
CN 106506534 A,2017.03.15
CN 107995162 A,2018.05.04
CN 105430113 A,2016.03.23
CN 105812502 A,2016.07.27
CN 102694876 A,2012.09.26
CN 101370019 A,2009.02.18
CN 103259732 A,2013.08.21
CN 106506200 A,2017.03.15
CN 104780139 A,2015.07.15
KR 20070081116 A,2007.08.14
Laizhong Cui F. Richard Yu Qiao Yan.When big data meets software-defined networking SDN for big data and big data for SDN.pdf.《IEEE Network》.2016,

审查员 张宁

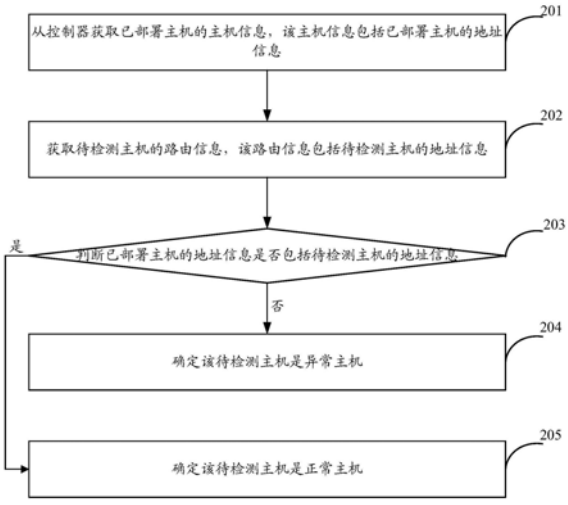
权利要求书2页 说明书14页 附图4页

(54)发明名称

一种异常主机的监控方法及装置

(57)摘要

本申请提供一种异常主机的监控方法及装置，该方法包括：从控制器获取已部署主机的主机信息，所述主机信息包括所述已部署主机的地址信息；获取待检测主机的路由信息，所述路由信息包括所述待检测主机的地址信息；判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息；如果否，则确定所述待检测主机是异常主机。通过本申请的技术方案，充分发挥大数据处理系统的数据收集能力和数据处理能力，并准确分析主机是否为异常主机。



CN 111010362 B

1.一种异常主机的监控方法,其特征在于,应用于数据处理设备,包括:

从控制器获取已部署主机的主机信息,所述主机信息包括所述已部署主机的地址信息;以及,从所述控制器获取所述已部署主机的链路层发现协议LLDP信息,所述LLDP信息包括所述已部署主机关联的第一边缘设备的设备信息;

获取待检测主机的路由信息,所述路由信息包括所述待检测主机的地址信息,所述路由信息还包括所述待检测主机关联的第二边缘设备的设备信息;

判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息;

如果否,则确定所述待检测主机是异常主机;

如果是,则从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息;若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息不同,则确定所述待检测主机是异常主机。

2.根据权利要求1所述的方法,其特征在于,

所述获取待检测主机的路由信息之前,所述方法还包括:

与路由管理设备协商建立边界网关协议BGP邻居;

所述获取待检测主机的路由信息,具体包括:

接收所述路由管理设备通过所述BGP邻居发送的待检测主机的路由信息。

3.根据权利要求1所述的方法,其特征在于,所述主机信息还包括所述已部署主机的主机标识,所述LLDP信息还包括所述已部署主机的主机标识;从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息,包括:

通过所述已部署主机的地址信息查询所述主机信息,得到所述已部署主机的主机标识;

通过所述已部署主机的主机标识查询所述LLDP信息,得到所述已部署主机关联的第一边缘设备的设备信息。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息相同,则确定所述待检测主机是正常主机。

5.根据权利要求1所述的方法,其特征在于,

所述获取待检测主机的路由信息之后,所述方法还包括:

判断历史数据库中是否存在所述待检测主机对应的表项;

如果存在,则在所述表项中存储所述路由信息和所述路由信息的获取时间;

如果不存在,则在所述历史数据库中添加所述待检测主机对应的表项,并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

6.一种异常主机的监控装置,其特征在于,应用于数据处理设备,包括:

获取模块,用于从控制器获取已部署主机的主机信息,其中,所述主机信息包括所述已部署主机的地址信息;以及,从所述控制器获取所述已部署主机的链路层发现协议LLDP信息,所述LLDP信息包括所述已部署主机关联的第一边缘设备的设备信息;以及,获取待检测主机的路由信息,其中,所述路由信息包括所述待检测主机的地址信息,所述路由信息还包括所述待检测主机关联的第二边缘设备的设备信息;

判断模块,用于判断所述已部署主机的地址信息是否包括所述待检测主机的地址信

息；

确定模块，用于当判断结果为否时，确定所述待检测主机是异常主机；

所述获取模块，还用于当所述判断模块的判断结果为是时，则从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息；所述确定模块，还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息不同，确定待检测主机是异常主机。

7.根据权利要求6所述的装置，其特征在于，还包括：

建立模块，用于与路由管理设备协商建立边界网关协议BGP邻居；

所述获取模块获取待检测主机的路由信息时具体用于：接收所述路由管理设备通过所述BGP邻居发送的待检测主机的路由信息。

8.根据权利要求6所述的装置，其特征在于，所述主机信息还包括所述已部署主机的主机标识，所述LLDP信息还包括所述已部署主机的主机标识；

所述获取模块从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息时具体用于：通过所述已部署主机的地址信息查询所述主机信息，得到所述已部署主机的主机标识；通过所述已部署主机的主机标识查询所述LLDP信息，得到所述已部署主机关联的第一边缘设备的设备信息。

9.根据权利要求6所述的装置，其特征在于，所述确定模块，还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息相同，则确定所述待检测主机是正常主机。

10.根据权利要求6所述的装置，其特征在于，

所述判断模块，还用于在所述获取模块获取待检测主机的路由信息之后，判断历史数据库中是否存在所述待检测主机对应的表项；

所述装置还包括：存储模块，用于当判断结果为存在时，则在所述表项中存储所述路由信息和所述路由信息的获取时间；当判断结果为不存在时，则在所述历史数据库中添加所述待检测主机对应的表项，并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

一种异常主机的监控方法及装置

技术领域

[0001] 本申请涉及通信技术领域,尤其是涉及一种异常主机的监控方法及装置。

背景技术

[0002] 以太网虚拟专用网络(Ethernet Virtual Private Network,EVPN)是二层虚拟专用网络(Virtual Private Network,VPN)技术,控制平面采用多协议边界网关协议(Multi Protocol-Border Gateway Protocol,MP-BGP)通告路由信息,数据平面采用可扩展虚拟局域网络(Virtual eXtensible Local Area Network,VXLAN)封装方式转发报文。其中,VXLAN是一种基于IP网络、采用介质访问控制(Media Access Control,MAC)和用户数据报协议(User Datagram Protocol,UDP)封装形式的二层VPN技术,VXLAN可以基于已有的服务提供商或者企业IP网络,为分散的站点提供二层互联,并能够为不同的租户提供业务的隔离。

[0003] EVPN网络包括主机和边缘设备,边缘设备可以学习主机的转发表项,利用转发表项将数据报文发送给主机。例如,边缘设备A收到主机A发送的地址解析协议(Address Resolution Protocol,ARP)报文后,学习主机A的转发表项1,将主机A的地址通告给边缘设备B,边缘设备B学习主机A的转发表项2。边缘设备B收到主机B发送给主机A的数据报文时,利用转发表项2将数据报文发送给边缘设备A,边缘设备A利用转发表项1将数据报文发送给主机A。

[0004] 但是,若攻击者通过主机发送大量攻击ARP报文,则边缘设备将学习到大量转发表项,从而造成表项资源的浪费,影响边缘设备的处理性能。为了解决上述问题,在传统方式中,边缘设备在接收到ARP报文后,可以将ARP报文发送给控制器,由控制器分析ARP报文是否为攻击者发送。若ARP报文是攻击者发送,则控制器可以产生告警信息,由管理人员对攻击行为进行处理。

[0005] 但是,EVPN网络中存在大量ARP报文,由控制器分析这些ARP报文是否为攻击者发送,工作量很大,消耗控制器的大量资源,降低处理性能。

发明内容

[0006] 本申请提供一种异常主机的监控方法,应用于数据处理设备,包括:

[0007] 从控制器获取已部署主机的主机信息,所述主机信息包括所述已部署主机的地址信息;获取待检测主机的路由信息,所述路由信息包括所述待检测主机的地址信息;判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息;如果否,则确定所述待检测主机是异常主机。

[0008] 可选地,所述获取待检测主机的路由信息之前,所述方法还包括:

[0009] 与路由管理设备协商建立边界网关协议BGP邻居;

[0010] 所述获取待检测主机的路由信息,具体包括:

[0011] 接收所述路由管理设备通过所述BGP邻居发送的待检测主机的路由信息。

[0012] 可选地，所述方法还包括：

[0013] 从所述控制器获取所述已部署主机的链路层发现协议LLDP信息，所述LLDP信息包括所述已部署主机关联的第一边缘设备的设备信息；判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息之后，所述方法还包括：如果是，则从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息；所述路由信息还包括所述待检测主机关联的第二边缘设备的设备信息，若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息不同，则确定所述待检测主机是异常主机。

[0014] 可选地，所述主机信息还包括所述已部署主机的主机标识，所述LLDP信息还包括所述已部署主机的主机标识；从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息，包括：通过已部署主机的地址信息查询所述主机信息，得到所述已部署主机的主机标识；通过所述已部署主机的主机标识查询所述LLDP信息，得到所述已部署主机关联的第一边缘设备的设备信息。

[0015] 可选地，所述方法还包括：

[0016] 若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息相同，则确定所述待检测主机是正常主机。

[0017] 可选地，所述获取待检测主机的路由信息之后，所述方法还包括：

[0018] 判断历史数据库中是否存在所述待检测主机对应的表项；

[0019] 如果存在，则在所述表项中存储所述路由信息和所述路由信息的获取时间；

[0020] 如果不存在，则在所述历史数据库中添加所述待检测主机对应的表项，并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

[0021] 本申请提供一种异常主机的监控装置，应用于数据处理设备，包括：

[0022] 获取模块，用于从控制器获取已部署主机的主机信息，其中，所述主机信息包括所述已部署主机的地址信息；以及，获取待检测主机的路由信息，其中，所述路由信息包括所述待检测主机的地址信息；判断模块，用于判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息；确定模块，用于当判断结果为否时，确定所述待检测主机是异常主机。

[0023] 可选地，还包括：建立模块，用于与路由管理设备协商建立边界网关协议BGP邻居；所述获取模块获取待检测主机的路由信息时具体用于：接收所述路由管理设备通过所述BGP邻居发送的待检测主机的路由信息。

[0024] 可选地，所述获取模块，还用于从所述控制器获取所述已部署主机的链路层发现协议LLDP信息，所述LLDP信息包括所述已部署主机关联的第一边缘设备的设备信息；所述获取模块，还用于当所述判断模块的判断结果为是时，则从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息；

[0025] 所述路由信息还包括所述待检测主机关联的第二边缘设备的设备信息；所述确定模块，还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息不同，确定待检测主机是异常主机。

[0026] 可选地，所述主机信息还包括所述已部署主机的主机标识，所述LLDP信息还包括所述已部署主机的主机标识；

[0027] 所述获取模块从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设

备信息时具体用于:通过所述已部署主机的地址信息查询所述主机信息,得到所述已部署主机的主机标识;通过所述已部署主机的主机标识查询所述LLDP信息,得到所述已部署主机关联的第一边缘设备的设备信息。

[0028] 可选地,所述确定模块,还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息相同,则确定所述待检测主机是正常主机。

[0029] 可选地,所述判断模块,还用于在所述获取模块获取待检测主机的路由信息之后,判断历史数据库中是否存在所述待检测主机对应的表项;

[0030] 所述装置还包括:存储模块,用于当判断结果为存在时,则在所述表项中存储所述路由信息和所述路由信息的获取时间;当判断结果为不存在时,则在所述历史数据库中添加所述待检测主机对应的表项,并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

[0031] 基于上述技术方案,本申请实施例中,数据处理设备(通常为大数据处理系统)可以从控制器获取主机信息,从路由管理设备获取路由信息,并根据主机信息和路由信息分析主机是否为异常主机,从而充分发挥大数据处理系统的数据收集能力和数据处理能力,并准确分析主机是否为异常主机。上述方式不需要由控制器分析主机是否为异常主机,减轻控制器的工作量,节约控制器的处理资源,提高控制器的处理性能。在上述方式中,基于大数据技术分析主机是否为异常主机,进行主机行为的分析、异常检测和错误纠正,使得网络维护人员精确掌握每个主机的网络接入信息、快速感知主机的异常接入行为。

附图说明

[0032] 为了更加清楚地的说明本申请实施例或者现有技术中的技术方案,下面将对本申请实施例或者现有技术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申请中记载的一些实施例,对于本领域普通技术人员来讲,还可以根据本申请实施例的这些附图获得其他的附图。

[0033] 图1是本申请一种实施方式中的应用场景示意图;

[0034] 图2是本申请一种实施方式中的异常主机的监控方法的流程图;

[0035] 图3是本申请另一种实施方式中的异常主机的监控方法的流程图;

[0036] 图4是本申请一种实施方式中的异常主机的监控装置的结构图;

[0037] 图5是本申请一种实施方式中的数据处理设备的硬件结构图。

具体实施方式

[0038] 在本申请实施例使用的术语仅仅是出于描述特定实施例的目的,而非限制本申请。本申请和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它含义。还应当理解,本文中使用的术语“和/或”是指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。

[0039] 应当理解,尽管在本申请实施例可能采用术语第一、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，此外，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”。

[0040] 本申请实施例中提出一种异常主机的监控方法，该方法可以应用于包括主机、边缘设备、控制器、云平台、路由管理设备和数据处理设备的网络中，如EVPN网络等。参见图1所示，为本申请实施例的应用场景示意图。在图1中，是以两个主机为例进行说明，在实际应用中，主机的数量可以更多。此外，以两个边缘设备为例进行说明，在实际应用中，边缘设备的数量可以更多。

[0041] 其中，主机可以是物理服务器上部署的虚拟机，也可以是物理服务器，还可以是其它类型的主机，例如，个人计算机、终端设备、移动终端等。

[0042] 边缘设备可以是可扩展虚拟局域网络隧道端点(VXLAN Tunnel End Point，VTEP)设备，也可以是其它类型的边缘设备。进一步的，VTEP设备可以作为EVPN网络的边缘设备，与VXLAN有关的处理均在VTEP设备进行。

[0043] 控制器可以是软件定义网络(Soft Define Network，SDN)控制器，也可以是其它类型的控制器。云平台可以是Openstack云平台，也可以是其它类型的云平台。EVPN网络使用Openstack云平台和SDN控制器实现控制平面的功能。

[0044] 路由管理设备用于收集EVPN网络中的所有路由信息，例如，路由管理设备可以是路由反射器(Route Reflector，RR)，也可以是其它类型的设备。

[0045] 数据处理设备可以是大数据处理系统中的设备，数据处理设备可以采用大数据技术实现数据收集、数据分析、数据存储、数据统计、数据挖掘等功能。

[0046] 在介绍本申请实施例中的异常主机的监控方法之前，先介绍如下技术。

[0047] 1、主机类型。本实施例中的主机可以划分为已部署主机和待检测主机，已部署主机是真正部署在网络的主机，是合法的主机。已部署主机可以包括已在线主机和未在线主机，已在线主机是已经访问网络的主机，未在线主机是未访问网络的主机，已在线主机和未在线主机均是真正部署在网络的合法的主机。

[0048] 待检测主机是需要进行检测的主机，本实施例中的异常主机的监控方法，正是检测该待检测主机是否为异常主机。若待检测主机是异常主机，则待检测主机不属于已部署主机，需要进行异常处理。若待检测主机不是异常主机，即待检测主机是正常主机，则待检测主机属于已部署主机，允许其访问网络。

[0049] 2、控制器获取已部署主机的主机信息，并在本地存储该主机信息。

[0050] 在一个例子中，可以由云平台为租户创建主机(例如，在物理服务器上为租户创建虚拟机，或者，将物理服务器分配给租户)，并为该主机分配主机信息，为了区分方便，将云平台为租户创建的所有主机均称为已部署主机。然后，云平台将已部署主机的主机信息发送给控制器，由控制器存储该主机信息。

[0051] 需要注意的是，EVPN网络中的所有已部署主机均可以由云平台创建，也就是说，云平台向控制器发送的主机信息，包括所有已部署主机的主机信息。

[0052] 其中，主机信息可以包括但不限于：地址信息和主机标识。进一步的，该地址信息可以包括但不限于：IP地址、MAC地址和网络标识(如VNI(VXLAN Network Identifier，可扩展虚拟局域网的网络标识)等)。若主机是物理服务器上部署的虚拟机，则该主机标识可以是该虚拟机所在的物理服务器的设备标识，若主机是物理服务器，则该主机标识可以是该

物理服务器的设备标识。

[0053] 参见表1所示，为控制器存储的主机信息的示例，这些主机信息是EVPN网络中的所有已部署主机的主机信息，后续以这些主机信息为例进行说明。

[0054] 表1

[0055]

序号	IP地址	MAC地址	网络标识	主机标识
1	IP地址A	MAC地址A	VNI1	aaa
2	IP地址B	MAC地址B	VNI1	bbb
3	IP地址C	MAC地址C	VNI2	ccc
4	IP地址D	MAC地址D	VNI2	ddd
…	…	…	…	…

[0056] 3、控制器可以获取上述已部署主机的链路层发现协议(Link Layer Discovery Protocol，LLDP)信息，并在本地存储已部署主机的LLDP信息。其中，该LLDP信息可以包括但不限于已部署主机对应的主机标识、与已部署主机关联的边缘设备的设备信息，该设备信息可以包括IP地址和/或MAC地址等。

[0057] 在一个例子中，若已部署主机是物理服务器上部署的虚拟机，则已部署主机对应的主机标识可以是该物理服务器的设备标识，与已部署主机关联的边缘设备可以是与该物理服务器连接的边缘设备。或者，若已部署主机是物理服务器，则已部署主机对应的主机标识可以是该已部署主机的设备标识，与已部署主机关联的边缘设备可以是与该已部署主机连接的边缘设备。

[0058] 参见上述实施例，已部署主机可以包括已在线主机和未在线主机，针对已在线主机来说，为了获取已在线主机的LLDP信息，则可以采用如下方式：

[0059] 参见图1所示，当主机111上线后，即主机111成为已在线主机，则主机111可以向与主机111连接的边缘设备121发送LLDP报文，该LLDP报文包括主机111的管理地址、主机标识等内容。边缘设备121在接收到LLDP报文后，将该LLDP报文发送给控制器141。

[0060] 其中，控制器141可以向边缘设备121下发控制流表，这个控制流表用于使边缘设备121将LLDP报文发送给控制器141，例如，这个控制流表的匹配选项包括协议类型是LLDP类型，动作项包括上送控制器。基于此，边缘设备121在接收到LLDP报文后，由于该LLDP报文与该控制流表匹配，因此，可以将LLDP报文发送给控制器141。

[0061] 控制器141在接收到LLDP报文后，从LLDP报文中获取主机111的管理地址、主机标识等内容。此外，由于控制器141能够管理所有的边缘设备，因此，控制器141在接收到边缘设备121发送的LLDP报文后，还可以获取边缘设备121的设备信息(如IP地址、MAC地址等)。综上所述，控制器141可以获取到主机111的主机标识和边缘设备121的设备信息，而该主机标识和该设备信息就是主机111的LLDP信息。

[0062] 针对未在线主机来说，为了获取未在线主机的LLDP信息，采用如下方式：

[0063] (1)假设主机112未在线，且未在线主机112是物理服务器上部署的虚拟机，假设该物理服务器已经在线，则物理服务器可以向与该物理服务器连接的边缘设备122发送LLDP报文，该LLDP报文包括物理服务器的主机标识，这个主机标识也就是该物理服务器上部署的所有已部署主机的主机标识。

[0064] 边缘设备122在接收到LLDP报文后，将该LLDP报文发送给控制器141。控制器141在

接收到LLDP报文后，从LLDP报文中获取物理服务器的主机标识，并获取边缘设备122的设备信息(如IP地址、MAC地址等)，而物理服务器的主机标识和边缘设备122的设备信息就是主机112的LLDP信息。

[0065] (2)假设主机111未在线，且未在线主机111是物理服务器，则边缘设备121可以向主机111发送LLDP报文，该LLDP报文可以携带边缘设备121的设备信息(如IP地址、MAC地址等)。主机111在接收到LLDP报文后，可以将边缘设备121的设备信息、主机111的主机标识发送给云平台151，云平台151将边缘设备121的设备信息、主机111的主机标识发送给控制器141，而边缘设备121的设备信息、主机111的主机标识就是主机111的LLDP信息。

[0066] 综上所述，控制器141可以获取每个已部署主机的LLDP信息，并存储每个已部署主机的LLDP信息，参见表2所示，为LLDP信息的一个示例。

[0067] 表2

[0068]

主机标识	边缘设备的设备信息

[0069]

aaa	IP 地址 1 和 MAC 地址 1
bbb	IP 地址 2 和 MAC 地址 2
ccc	IP 地址 3 和 MAC 地址 3
ddd	IP 地址 4 和 MAC 地址 4
…	…

[0070] 4、路由管理设备接收路由信息，并向边缘设备同步该路由信息。

[0071] 在一个例子中，参见图1所示，当主机111上线时，主机111向边缘设备121发送ARP报文(如ARP请求报文或者免费ARP报文等)。边缘设备121在接收到ARP报文后，可以在转发表项中记录ARP报文的源地址(即主机111的地址，如IP地址和/或MAC地址等)与ARP报文的入接口的对应关系。

[0072] 进一步的，边缘设备121在接收到该ARP报文后，还可以生成BGP消息(如MP-BGP消息)，该BGP消息可以包括路由信息，该路由信息可以包括但不限于：主机111的地址信息(该地址信息可以包括IP地址、MAC地址和网络标识)，边缘设备121的设备信息(该设备信息可以包括IP地址、MAC地址等)。

[0073] 边缘设备121在生成BGP消息后，可以将BGP消息发送给边缘设备122。边缘设备122在接收到BGP消息后，可以从BGP消息中获取主机111的地址信息，并在转发表项中记录主机111的地址信息(如IP地址、MAC地址和网络标识等)与隧道A的对应关系，对此转发表项的学习过程不做限制。其中，隧道A可以是边缘设备122与边缘设备121之间的隧道，如VXLAN隧道等。

[0074] 边缘设备121将BGP消息发送给边缘设备122，可以包括但不限于：

[0075] 方式一、边缘设备121可以直接将BGP消息发送给边缘设备122。

[0076] 方式二、边缘设备121可以将BGP消息发送给路由管理设备131，路由管理设备131在接收到BGP消息后，将该BGP消息发送给边缘设备122。

[0077] 为了实现方式一，则任意两个边缘设备之间需要建立BGP邻居，如存在100个边缘

设备时，则每个边缘设备均需要与其它99个边缘设备建立BGP邻居，对网络资源和CPU资源的消耗很大。

[0078] 因此，在实施方式二中，可以在EVPN网络部署路由管理设备131(即路由反射器)，这样，每个边缘设备只需要与路由管理设备131建立BGP邻居，不再与其它边缘设备建立BGP邻居，减少网络资源和CPU资源的消耗。

[0079] 当在EVPN网络中部署路由管理设备131时，可以采用方式二传输BGP消息，即，每个边缘设备在发送BGP消息时，将BGP消息发送给路由管理设备131，由路由管理设备131将BGP消息发送给其它边缘设备。

[0080] 本申请实施例中，以采用方式二为例进行说明。在采用方式二时，路由管理设备131可以收集到EVPN网络中产生的所有BGP消息，每个BGP消息均包括发布者发布的路由信息，如主机的地址信息、边缘设备的设备信息等。

[0081] 在上述应用场景下，参见图2所示，为异常主机的监控方法的流程示意图，该方法可以应用于数据处理设备，该方法可以包括以下步骤：

[0082] 步骤201，从控制器获取已部署主机的主机信息，该主机信息包括已部署主机的地址信息。此外，该主机信息还可以包括已部署主机的主机标识。

[0083] 参见上述实施例，控制器中已经存储EVPN网络中的所有已部署主机的主机信息，因此，数据处理设备可以从控制器获取EVPN网络中的所有已部署主机的主机信息，参见表1所示，这些主机信息可以包括但不限于地址信息和主机标识，该地址信息可以包括IP地址、MAC地址和网络标识等。

[0084] 步骤202，获取待检测主机的路由信息，该路由信息包括待检测主机的地址信息。其中，待检测主机是需要进行检测的主机，为异常主机或者正常主机。

[0085] 在一个例子中，数据处理设备可以与路由管理设备协商建立BGP邻居。具体的，可以在数据处理设备配置BGP协议，这样，数据处理设备就可以与路由管理设备协商建立BGP邻居，对此BGP邻居的建立过程不做限制。

[0086] 在一个例子中，获取待检测主机的路由信息，可以包括但不限于：接收路由管理设备通过BGP邻居发送的待检测主机的路由信息。

[0087] 具体的，由于数据处理设备已经与路由管理设备协商建立BGP邻居，因此，路由管理设备每次接收到路由信息时，就可以通过BGP邻居将该路由信息发送给数据处理设备，这样，数据处理设备可以接收路由管理设备通过BGP邻居发送的路由信息。

[0088] 具体的，参见上述实施例，路由管理设备可以收集EVPN网络中产生的所有BGP消息，每个BGP消息包括路由信息，该路由信息包括待检测主机的地址信息、与待检测主机关联的边缘设备的设备信息。由于数据处理设备已经与路由管理设备协商建立BGP邻居，因此，路由管理设备在收集到每个BGP消息时，将该BGP消息发送给数据处理设备。数据处理设备接收到BGP消息后，可以从BGP消息中获取路由信息，如待检测主机的地址信息、边缘设备的设备信息。

[0089] 步骤203，判断已部署主机的地址信息是否包括待检测主机的地址信息。

[0090] 如果否，则可以执行步骤204，如果是，则可以执行步骤205。

[0091] 步骤204，确定该待检测主机是异常主机。

[0092] 步骤205，确定该待检测主机是正常主机。

[0093] 在一个例子中，数据处理设备可以从控制器获取EVPN网络中所有已部署主机的主机信息，参见表1所示，基于此，当表1所示的主机信息包括待检测主机的地址信息，则可以确定待检测主机是正常主机，当表1所示的主机信息不包括待检测主机的地址信息，则可以确定待检测主机是异常主机。

[0094] 在一种情况中，参见图1所示，当主机111(即待检测主机)上线后，向边缘设备121发送ARP报文。若主机111是正常主机，则ARP报文携带的是真实的地址信息，如IP地址A和MAC地址A。

[0095] 边缘设备121在接收到ARP报文后，可以生成针对主机111的BGP消息，并将该BGP消息发送给路由管理设备131，路由管理设备131在接收到该BGP消息后，可以将该BGP消息发送给数据处理设备161。

[0096] 其中，该BGP消息可以包括路由信息，该路由信息可以包括但不限于：主机111的IP地址A和MAC地址A，主机111的网络标识(如VNI1)，边缘设备121的设备信息(IP地址1和MAC地址1)。

[0097] 在上述情况中，路由信息包括的主机111的地址信息是：IP地址A、MAC地址A和网络标识VNI1，则判断表1所示的主机信息中是否包括上述地址信息。由于主机信息中包括上述地址信息，因此，可以确定主机111是正常主机。

[0098] 在另一种情况中，参见图1所示，当主机111(即待检测主机)上线后，向边缘设备121发送ARP报文。若主机111是异常主机(即攻击者)，则ARP报文携带的是攻击者伪造的地址信息，如IP地址AAA和MAC地址AAA。

[0099] 边缘设备121在接收到ARP报文后，可以生成针对主机111的BGP消息，并将该BGP消息发送给路由管理设备131，路由管理设备131在接收到该BGP消息后，可以将该BGP消息发送给数据处理设备161。

[0100] 其中，该BGP消息可以包括路由信息，该路由信息可以包括但不限于：主机111的IP地址AAA和MAC地址AAA，主机111的网络标识(如VNI1)，边缘设备121的设备信息(IP地址1和MAC地址1)。

[0101] 在上述情况中，路由信息包括的主机111的地址信息是：IP地址AAA、MAC地址AAA和网络标识VNI1，则判断表1所示的主机信息中是否包括上述地址信息。由于主机信息中不包括上述地址信息，因此，可以确定主机111是异常主机。

[0102] 在一个例子中，数据处理设备161确定主机111是异常主机时，还可以产生告警信息，由管理人员对攻击行为进行处理，对此处理过程不再赘述。

[0103] 基于上述技术方案，本申请实施例中，数据处理设备(通常为大数据处理系统)可以从控制器获取主机信息，从路由管理设备获取路由信息，并根据主机信息和路由信息分析主机是否为异常主机，从而充分发挥大数据处理系统的数据收集能力和数据处理能力，并准确分析主机是否为异常主机。上述方式不需要由控制器分析主机是否为异常主机，减轻控制器的工作量，节约控制器的处理资源，提高控制器的处理性能。在上述方式中，基于大数据技术分析主机是否为异常主机，进行主机行为的分析、异常检测和错误纠正，使得网络维护人员精确掌握每个主机的网络接入信息、快速感知主机的异常接入行为。

[0104] 在上述应用场景下，参见图3所示，为异常主机的监控方法的流程示意图，该方法可以应用于数据处理设备，该方法可以包括以下步骤：

[0105] 步骤301，从控制器获取已部署主机的主机信息，该主机信息包括已部署主机的地址信息。此外，该主机信息还可以包括已部署主机的主机标识。

[0106] 其中，步骤301的实现过程可以参见步骤201，在此不再赘述。

[0107] 步骤302，从控制器获取已部署主机的LLDP信息，该LLDP信息包括已部署主机的主机标识、已部署主机关联的第一边缘设备的设备信息。

[0108] 参见上述实施例，控制器中已经存储EVPN网络中的所有已部署主机的LLDP信息，因此，数据处理设备可以从控制器获取EVPN网络中的所有已部署主机的LLDP信息，参见表2所示，这些LLDP信息可以包括但不限于：已部署主机的主机标识、与该已部署主机关联的第一边缘设备的设备信息。

[0109] 步骤303，获取待检测主机的路由信息，该路由信息包括待检测主机的地址信息、与待检测主机关联的第二边缘设备的设备信息，如IP地址和/或MAC地址。其中，步骤303的实现过程可以参见步骤202，在此不再赘述。

[0110] 步骤304，判断已部署主机的地址信息是否包括待检测主机的地址信息。

[0111] 如果否，则可以执行步骤305，如果是，则可以执行步骤306。

[0112] 步骤305，确定该待检测主机是异常主机。

[0113] 在一个例子中，数据处理设备可以从控制器获取EVPN网络中所有已部署主机的主机信息，参见表1所示，基于此，当表1所示的主机信息不包括待检测主机的地址信息，则可以确定待检测主机是异常主机。当表1所示的主机信息包括待检测主机的地址信息，则可以执行步骤306及后续步骤。

[0114] 步骤306，从LLDP信息中获取已部署主机关联的第一边缘设备的设备信息。

[0115] 参见上述实施例，已部署主机的主机信息包括已部署主机的地址信息、已部署主机的主机标识，LLDP信息包括已部署主机的主机标识、已部署主机关联的第一边缘设备的设备信息，路由信息包括待检测主机的地址信息。

[0116] 基于此，从LLDP信息中获取已部署主机关联的第一边缘设备的设备信息，可以包括：通过已部署主机的地址信息(这个地址信息与待检测主机的地址信息相同)查询主机信息，得到已部署主机的主机标识。通过已部署主机的主机标识查询LLDP信息，得到已部署主机关联的第一边缘设备的设备信息。

[0117] 例如，参见表1所示，由于主机信息包括地址信息与主机标识的对应关系，因此，数据处理设备可以通过待检测主机的地址信息查询表1所示的主机信息，确定出已部署主机的地址信息对应的主机标识。

[0118] 例如，若待检测主机的地址信息为IP地址A、MAC地址A和网络标识VNI1，则通过待检测主机的地址信息查询表1所示的主机信息，可以命中得到表1中已部署主机的主机标识为aaa(即待检测主机的主机标识)。又例如，若待检测主机的地址信息为IP地址B、MAC地址B和网络标识VNI1，则通过待检测主机的地址信息查询表1所示的主机信息，可以命中得到已部署主机的主机标识为bbb。

[0119] 在得到已部署主机的主机标识aaa后，通过主机标识aaa查询表2所示的LLDP信息，得到已部署主机关联的第一边缘设备的设备信息为IP地址1和MAC地址1。

[0120] 步骤307，判断待检测主机关联的第二边缘设备的设备信息(即路由信息中携带的设备信息)与已部署主机关联的第一边缘设备的设备信息是否相同。

[0121] 如果否，则可以执行步骤308，如果是，则可以执行步骤309。

[0122] 参见上述实施例，在待检测主机的路由信息中，包括待检测主机关联的第二边缘设备的设备信息，而且，已经获取已部署主机关联的第一边缘设备的设备信息，因此，在本步骤307中，可以判断待检测主机关联的第二边缘设备的设备信息与已部署主机关联的第一边缘设备的设备信息是否相同。

[0123] 步骤308，确定该待检测主机是异常主机。

[0124] 步骤309，确定该待检测主机是正常主机。

[0125] 在一种情况中，参见图1所示，当主机111(即待检测主机)上线后，主机111可以向边缘设备121发送ARP报文。若主机111是正常主机，则ARP报文携带的是真实的地址信息，如IP地址A和MAC地址A。

[0126] 边缘设备121在接收到ARP报文后，可以生成针对主机111的BGP消息，并将该BGP消息发送给路由管理设备131，路由管理设备131在接收到该BGP消息后，可以将该BGP消息发送给数据处理设备161。

[0127] 其中，该BGP消息可以包括路由信息，该路由信息可以包括但不限于：主机111的IP地址A和MAC地址A，主机111的网络标识(如VNI1)，边缘设备121的设备信息(IP地址1和MAC地址1)。其中，边缘设备121的设备信息是待检测主机关联的第二边缘设备的设备信息。

[0128] 在上述情况中，路由信息包括的主机111的地址信息是：IP地址A、MAC地址A和网络标识VNI1，则数据处理设备161可以判断表1所示的主机信息中是否包括上述地址信息。由于主机信息中包括上述地址信息，因此，可以从主机信息中获取与上述地址信息对应的主机标识，如主机标识aaa。然后，数据处理设备161可以通过主机标识aaa查询表2所示的LLDP信息，得到与主机标识aaa对应的设备信息，即该设备信息为IP地址1和MAC地址1。其中，与主机标识aaa对应的设备信息是已部署主机关联的第一边缘设备的设备信息。

[0129] 综上所述，待检测主机关联的第二边缘设备的设备信息为IP地址1和MAC地址1，已部署主机关联的第一边缘设备的设备信息为IP地址1和MAC地址1，也就是说，上述两个设备信息相同，因此，可以确定主机111是正常主机。

[0130] 在另一种情况中，参见图1所示，当主机111(即待检测主机)上线后，主机111可以向边缘设备121发送ARP报文。若主机111是异常主机(即攻击者)，则ARP报文携带的是攻击者伪造的地址信息，假设攻击者伪造的是主机112的地址信息，则ARP报文携带的是IP地址B和MAC地址B。

[0131] 边缘设备121在接收到ARP报文后，可以生成针对主机111的BGP消息，并将该BGP消息发送给路由管理设备131，路由管理设备131在接收到该BGP消息后，可以将该BGP消息发送给数据处理设备161。

[0132] 其中，该BGP消息可以包括路由信息，该路由信息可以包括但不限于：主机111的IP地址B和MAC地址B，主机111的网络标识(如VNI1)，边缘设备121的设备信息(IP地址1和MAC地址1)。

[0133] 在上述情况中，假设路由信息包括的主机111的地址信息是：IP地址B、MAC地址B和网络标识VNI1，则数据处理设备161可以判断表1所示的主机信息中是否包括上述地址信息。由于主机信息中包括上述地址信息，因此，可以从主机信息中获取与上述地址信息对应的主机标识，如主机标识bbb。然后，数据处理设备161可以通过主机标识bbb查询表2所示的

LLDP信息，得到与主机标识bbb对应的设备信息，即该设备信息为IP地址2和MAC地址2。其中，与主机标识bbb对应的设备信息是已部署主机关联的第一边缘设备的设备信息。

[0134] 综上所述，待检测主机关联的第二边缘设备的设备信息为IP地址1和MAC地址1，已部署主机关联的第一边缘设备的设备信息为IP地址2和MAC地址2，也就是说，上述两个设备信息不同，因此，可以确定主机111是异常主机。

[0135] 综上所述，主机111在发送ARP报文时，即使ARP报文携带的是攻击者伪造的合法主机的地址信息，数据处理设备161也可以识别主机111为异常主机。

[0136] 在一个例子中，数据处理设备161确定主机111是异常主机时，还可以产生告警信息，由管理人员对攻击行为进行处理，对此处理过程不再赘述。

[0137] 基于上述技术方案，本申请实施例中，即使攻击者伪造的是正常主机的地址信息，数据处理设备(通常为大数据处理系统)也可以分析这个主机是否为异常主机，从而准确识别出正常主机和异常主机，能够充分发挥大数据处理系统的数据收集能力和数据处理能力。上述方式不需要由控制器分析主机是否为异常主机，减轻控制器的工作量，节约控制器的处理资源，提高控制器的处理性能。在上述方式中，基于大数据技术分析主机是否为异常主机，进行主机行为的分析、异常检测和错误纠正，使得网络维护人员精确掌握每个主机的网络接入信息、快速感知主机的异常接入行为。

[0138] 在上述实施例中，数据处理设备获取待检测主机的路由信息(如地址信息、待检测主机关联的边缘设备的设备信息)之后，还可以包括：

[0139] 判断历史数据库中是否存在该待检测主机对应的表项；

[0140] 如果存在，在该表项中存储所述路由信息和所述路由信息的获取时间；

[0141] 如果不存在，在历史数据库中添加该待检测主机对应的表项，并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

[0142] 例如，参见表3所示，为历史数据库的一个示例，该历史数据库用于记录路由信息。当然，表3只是一个示例，还可以包括其它内容，对此不做限制。

[0143] 表3

[0144]

序号	主机的地址信息	主机下一跳边缘设备的设备信息	获取时间	状态
A	IP地址A、MAC地址A和网络标识VNI1	IP地址1和MAC地址1	时刻A	正常
B	IP地址B、MAC地址B和网络标识VNI1	IP地址2和MAC地址2	时刻B	正常
	IP地址B、MAC地址B和网络标识VNI1	IP地址3和MAC地址3	时刻C	异常

[0145]

[0146] 在一个例子中，假设主机111下线后重新上线，则主机111可以重新发送ARP报文，边缘设备121在接收到该ARP报文后，可以向路由管理设备131发送BGP消息，路由管理设备131可以将BGP消息发送给数据处理设备161，数据处理设备161最终获取到主机111的路由信息，对此过程不再赘述，可以参见上述实施例。其中，该路由信息包括主机111的地址信息(如IP地址A、MAC地址A和网络标识VNI1)，边缘设备121的设备信息(如IP地址1和MAC地址1)。数据处理设备161还可以确定该路由信息的获取时间，如时刻D。

[0147] 本申请实施例中，数据处理设备161还可以判断表3所示的历史数据库中是否存在

地址信息(如IP地址A、MAC地址A和网络标识VNI1)对应的表项。由于存在,因此,在该表项中存储IP地址A、MAC地址A和网络标识VNI1、IP地址1和MAC地址1、时刻D的对应关系,参见表4所示。

[0148] 表4

[0149]

序号	主机的地址信息	主机下一跳边缘设备的设备信息	获取时间	状态
a	IP地址A、MAC地址A和网络标识VNI1	IP地址1和MAC地址1	时刻A	正常
	IP地址A、MAC地址A和网络标识VNI1	IP地址1和MAC地址1	时刻D	正常
b	IP地址B、MAC地址B和网络标识VNI1	IP地址2和MAC地址2	时刻B	正常
	IP地址B、MAC地址B和网络标识VNI1	IP地址3和MAC地址3	时刻C	异常

[0150] 综上所述,本实施例中,由于大数据系统可以存储海量信息,因此,数据处理设备161可以在表项中添加路由信息,而不是替换表项中已存在的路由信息,即可以长时间的保存路由信息,可以按照时间顺序保存、快速检索信息。由于可以存储海量信息,因此,可以方便按照历史时间进行查询,可以支持长时间接入行为异常的原因回溯,例如,IP地址B、MAC地址B和网络标识VNI1对应的主机在时刻C发生异常。而且,基于大数据系统保存的海量带有时间序列属性的信息,可以快速回溯历史上任意时间点的异常接入行为。

[0151] 在上述实施例中,数据处理设备161可以包括数据收集器和数据分析器,数据收集器用于实现数据的收集,而数据分析器用于实现数据的分析。基于此,可以由数据收集器执行步骤301-步骤303,由数据分析器执行步骤304-步骤309。

[0152] 基于与上述方法同样的申请构思,本申请实施例中还提出一种异常主机的监控装置,应用于数据处理设备,如图4所示,为所述装置的结构图,包括:

[0153] 获取模块41,用于从控制器获取已部署主机的主机信息,其中,所述主机信息包括所述已部署主机的地址信息;以及,获取待检测主机的路由信息,其中,所述路由信息包括所述待检测主机的地址信息;

[0154] 判断模块42,用于判断所述已部署主机的地址信息是否包括所述待检测主机的地址信息;

[0155] 确定模块43,用于当判断结果为否时,确定所述待检测主机是异常主机。

[0156] 在一个例子中,所述装置还包括(在图中未示出):

[0157] 建立模块,用于与路由管理设备协商建立边界网关协议BGP邻居;

[0158] 所述获取模块41获取待检测主机的路由信息时具体用于:接收所述路由管理设备通过所述BGP邻居发送的待检测主机的路由信息。

[0159] 所述获取模块41,还用于从所述控制器获取所述已部署主机的链路层发现协议LLDP信息,所述LLDP信息包括所述已部署主机关联的第一边缘设备的设备信息;所述获取模块41,还用于当所述判断模块的判断结果为是时,则从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息;

[0160] 所述路由信息包括所述待检测主机关联的第二边缘设备的设备信息;所述确定模块43,还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息不同,确定待检测主机是异常主机。

[0161] 所述主机信息还包括所述已部署主机的主机标识，所述LLDP信息还包括所述已部署主机的主机标识；所述获取模块41从所述LLDP信息中获取所述已部署主机关联的第一边缘设备的设备信息时具体用于：

[0162] 通过所述已部署主机的地址信息查询所述主机信息，得到所述已部署主机的主机标识；通过所述已部署主机的主机标识查询所述LLDP信息，得到所述已部署主机关联的第一边缘设备的设备信息。

[0163] 所述确定模块43，还用于若所述待检测主机关联的第二边缘设备的设备信息与所述已部署主机关联的第一边缘设备的设备信息相同，则确定所述待检测主机是正常主机。

[0164] 所述判断模块42，还用于在所述获取模块获取待检测主机的路由信息之后，判断历史数据库中是否存在所述待检测主机对应的表项；

[0165] 在一个例子中，所述装置还包括(在图中未示出)：存储模块，用于当判断结果为存在时，则在所述表项中存储所述路由信息和所述路由信息的获取时间；当判断结果为不存在时，则在所述历史数据库中添加所述待检测主机对应的表项，并在新添加的表项中存储所述路由信息和所述路由信息的获取时间。

[0166] 本申请实施例中提供一种数据处理设备，从硬件层面而言，数据处理设备的硬件架构示意图具体可以参见图5所示。包括：机器可读存储介质和处理器，其中：所述机器可读存储介质：存储能够被所述处理器执行的机器可执行指令。所述处理器：与机器可读存储介质通信，读取和执行机器可读存储介质中存储的机器可执行指令，实现本申请上述示例公开的异常主机的监控操作。

[0167] 这里，机器可读存储介质可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM(Radom Access Memory，随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、dvd等)，或者类似的存储介质，或者它们的组合。

[0168] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0169] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0170] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0171] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可以由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程

序指令到通用计算机、专用计算机、嵌入式处理机或其它可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其它可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0172] 而且，这些计算机程序指令也可以存储在能引导计算机或其它可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或者多个流程和/或方框图一个方框或者多个方框中指定的功能。

[0173] 这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得在计算机或者其它可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其它可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0174] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

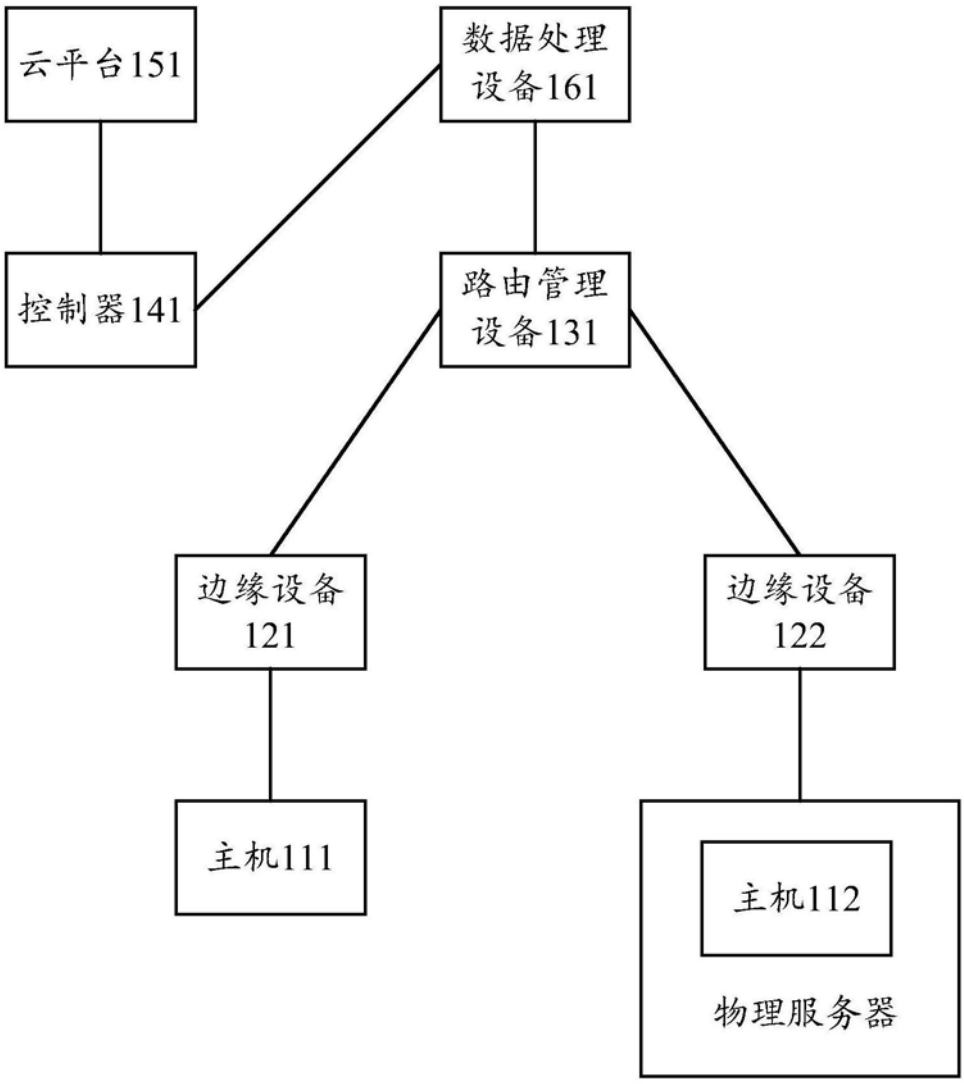

云平台151
数据处理设备161
控制器141
路由管理设备131
边缘设备121
边缘设备122
主机111
主机112
物理服务器

图1

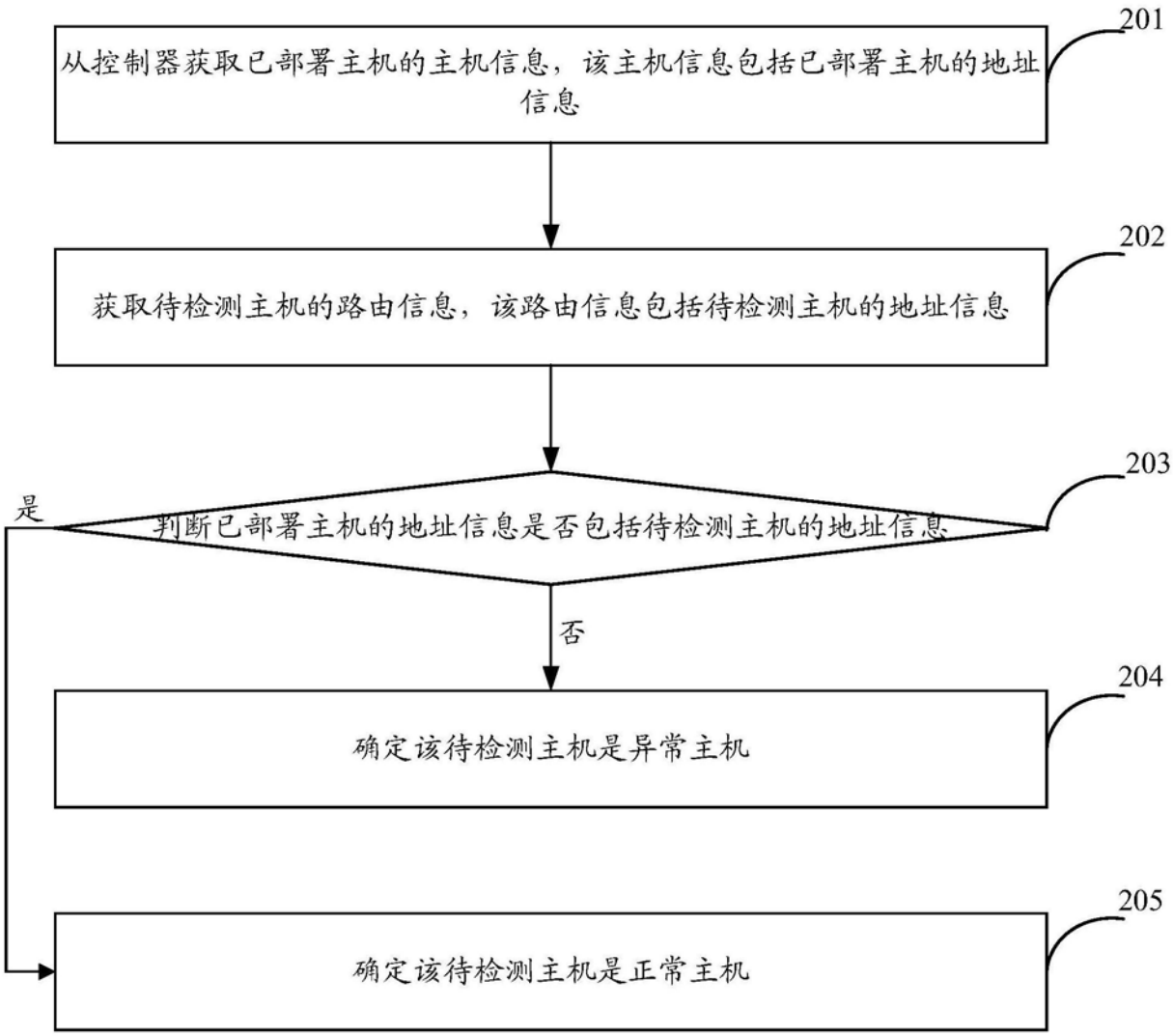

201
从控制器获取已部署主机的主机信息，该主机信息包括已部署主机的地址信息
202
获取待检测主机的路由信息，该路由信息包括待检测主机的地址信息
203
判断已部署主机的地址信息是否包括待检测主机的地址信息
是
否
204
确定该待检测主机是异常主机
205
确定该待检测主机是正常主机

图2

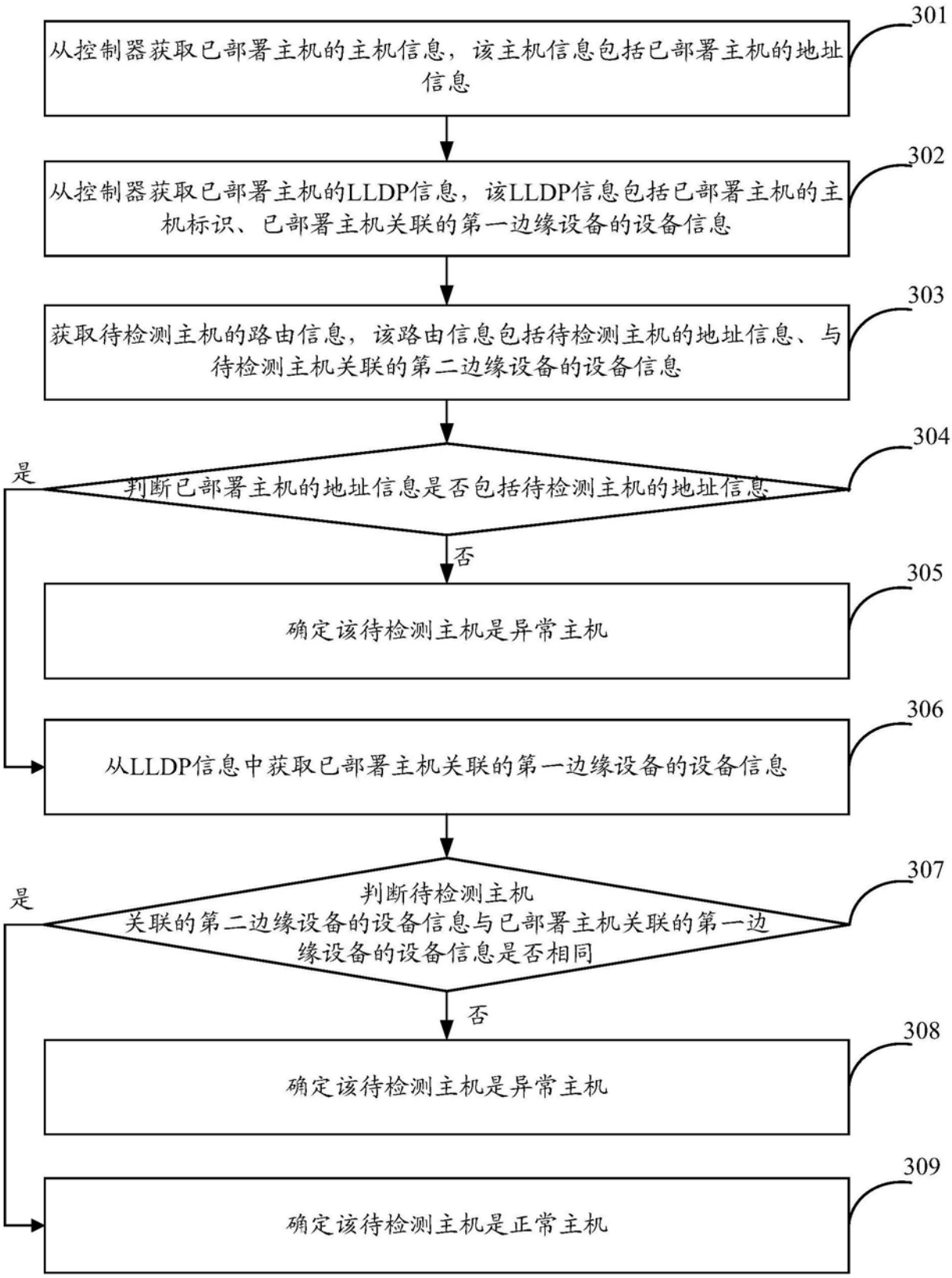

301
从控制器获取已部署主机的主机信息，该主机信息包括已部署主机的地址信息
302
从控制器获取已部署主机的LLDP信息，该LLDP信息包括已部署主机的主机标识、已部署主机关联的第一边缘设备的设备信息
303
获取待检测主机的路由信息，该路由信息包括待检测主机的地址信息、与待检测主机关联的第二边缘设备的设备信息
304
判断已部署主机的地址信息是否包括待检测主机的地址信息
是
否
305
确定该待检测主机是异常主机
306
从LLDP信息中获取已部署主机关联的第一边缘设备的设备信息
307
判断待检测主机关联的第二边缘设备的设备信息与已部署主机关联的第一边缘设备的设备信息是否相同
是
否
308
确定该待检测主机是异常主机
309
确定该待检测主机是正常主机

图3

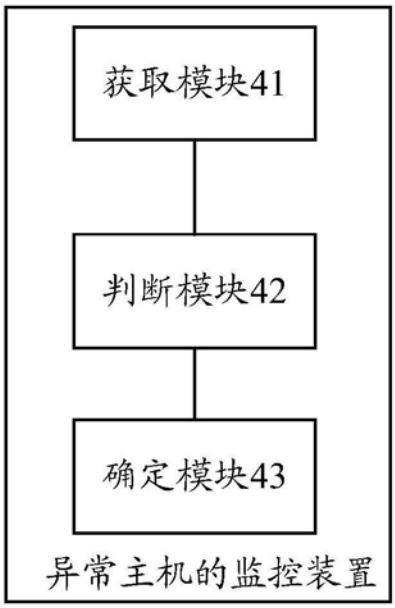

获取模块41
判断模块42
确定模块43
异常主机的监控装置

图4

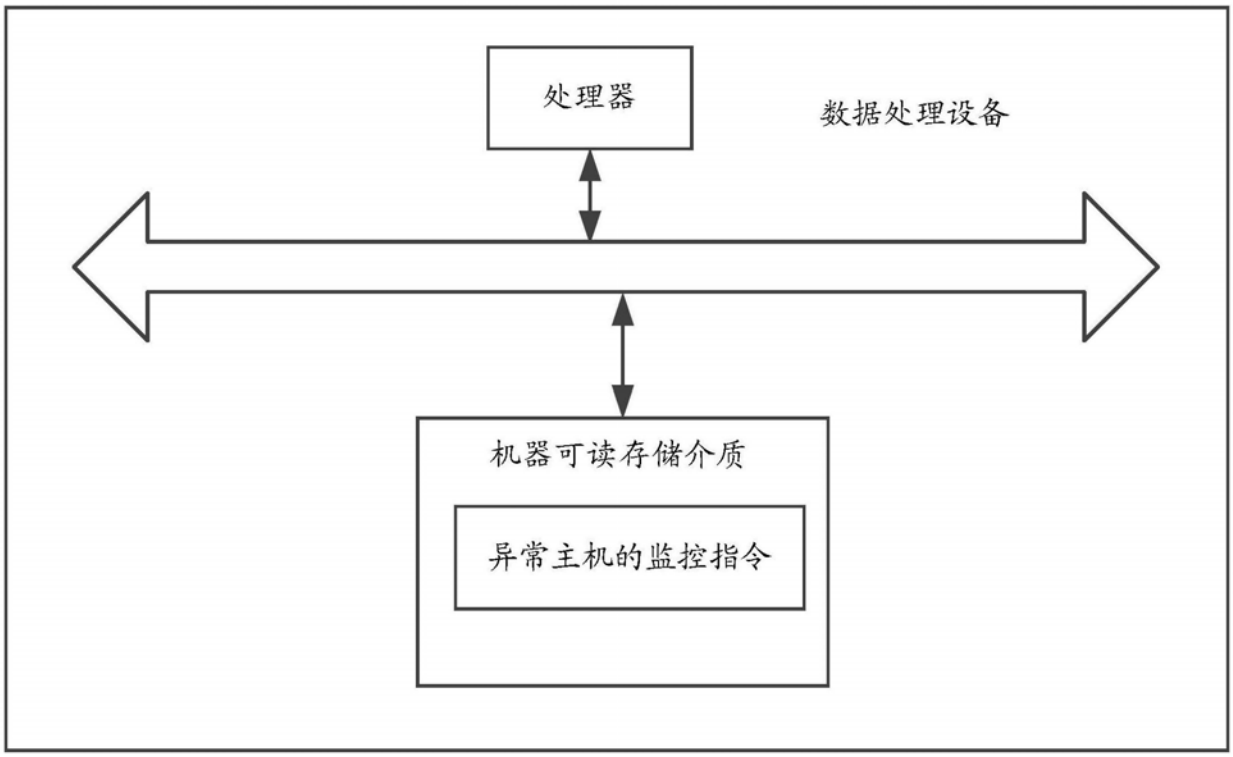

处理器
数据处理设备
机器可读存储介质
异常主机的监控指令

图5