(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 111819829 A
(43)申请公布日 2020.10.23

(21)申请号 201980015964.4
(22)申请日 2019.02.06
(30)优先权数据
15/909,393 2018.03.01 US
(85)PCT国际申请进入国家阶段日
2020.08.28
(86)PCT国际申请的申请数据
PCT/US2019/016875 2019.02.06
(87)PCT国际申请的公布数据
WO2019/168640 EN 2019.09.06
(71)申请人 施瓦哲工程实验有限公司
地址 美国华盛顿州
(72)发明人 贾森·A·迪里恩 雷特·史密斯 罗伯特·迈因
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 陆建萍 杨明钊
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 12/46(2006.01)

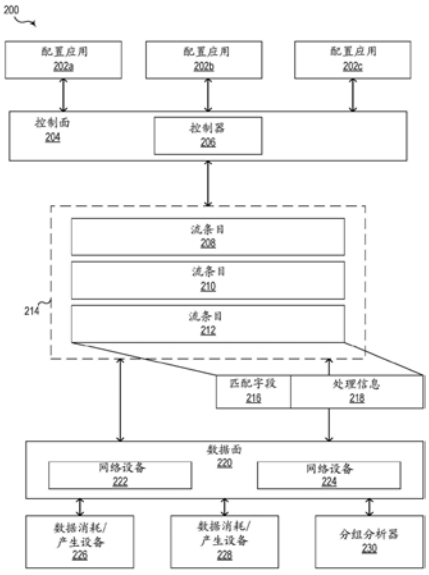
权利要求书2页 说明书9页 附图7页

(54)发明名称

用于检查的网络通信的选择性端口镜像和带内传输

(57)摘要

本公开涉及监测软件定义网络(SDN)中的通信设备和通信链路的系统和方法。网络分组可以被标注或标记,以便路由到分组分析器。可以将VLAN位掩码添加到分组中,以标识分组用于检查,并且可选地,提供标识交换机和/或来源端口的来源信息。可以利用端口镜像和/或将网络分组最终路由到它们的原始目的地可以确保网络流量不被中断。在一个示例中,匹配规则可以使用VLAN位掩码的最高有效位来标识预期用于分组分析器的分组,而不考虑原始分组路由指令和/或分组内容。



CN 111819829 A

1.一种在软件定义网络中经由网络分组的带内传输进行分组分析的方法,包括:

经由软件定义网络(SDN)内的第一联网设备接收网络分组;

经由所述第一联网设备标识所述网络分组用于转发给连接到所述SDN的分组分析器;

将所述网络分组的VLAN ID写入所述网络分组,从而标识所述网络分组用于由所述分组分析器分析;

将所述网络分组转发至所述SDN内的多个后续联网设备中的第一个;

由所述多个后续联网设备中的每一个读取所述网络分组的VLAN ID,所述VLAN ID标识所述网络分组用于由所述分组分析器分析;以及

由所述多个后续联网设备中的一个将所述网络分组转发到所述分组分析器进行分析。

2.根据权利要求1所述的方法,其中,标识所述网络分组用于由所述分组分析器分析的所述VLAN ID还标识所述第一联网设备。

3.根据权利要求1所述的方法,其中,标识所述网络分组用于由所述分组分析器分析的所述VLAN ID还标识:(i)所述第一联网设备,以及(ii)所述第一联网设备上的多个端口中的哪一个接收到所述网络分组。

4.根据权利要求1所述的方法,其中,所述VLAN ID的至少一个位被保留用于标识所述网络分组,以转发给所述分组分析器。

5.根据权利要求4所述的方法,其中,所述网络分组包括现有的VLAN标记,并且其中,将所述VLAN ID写入所述网络分组包括将包括所述VLAN ID的另一个VLAN标记推送到所述网络分组上,而不修改所述现有的VLAN标记。

6.根据权利要求1所述的方法,其中,所述分组分析器包括深度分组检查(DPI)系统。

7.根据权利要求1所述的方法,其中,所述分组分析器包括入侵检测系统(IDS)。

8.根据权利要求1所述的方法,还包括:

经由所述分组分析器检查所述网络分组。

9.根据权利要求8所述的方法,还包括:在经过所述分组分析器的检查之后丢弃所述网络分组。

10.根据权利要求8所述的方法,还包括:

在经过所述分组分析器的检查之后,转发所述网络分组到所述SDN中的原始预期设备。

11.根据权利要求10所述的方法,还包括:

移除标识所述网络分组用于由所述分组分析器分析的所述VLAN ID。

12.根据权利要求1所述的方法,其中,所述SDN包括基于以太网的SDN。

13.根据权利要求1所述的方法,其中,转发所述网络分组到所述SDN内的所述多个后续联网设备中的第一个包括将所述网络分组从所述第一联网设备的专用嗅探端口传出到所述多个后续联网设备中的第一个。

14.根据权利要求1所述的方法,还包括在写入所述VLAN ID之前,镜像由所述第一联网设备接收的网络分组。

15.根据权利要求14所述的方法,还包括转发所镜像的分组到所述网络分组的原始预期目的地。

16.一种软件定义网络,包括:

软件定义网络(SDN)控制器,其用于在经由网络连接到分组分析器的多个联网设备中

的每一个上选择性地实现分组分析流规则；

所述多个联网设备中的第一联网设备，其用于接收网络分组并标识所述网络分组用于经由所述分组分析器进行检查；

位写入器，其用于将VLAN ID写入所述网络分组，从而标识所述网络分组用于经由所述分组分析器进行检查；以及

所述第一联网设备的分组转发模块，其用于经由网络中的所述多个联网设备中的至少一些将所标记的网络分组转发到所述分组分析器。

17.根据权利要求16所述的软件定义网络，其中，能够选择性地实现的所述分组分析流规则允许对所述多个联网设备的至少一个上的任一端口进行选择性端口镜像。

18.根据权利要求16所述的软件定义网络，其中，网络分组包括现有的VLAN标记，并且其中，所述位写入器被配置成通过将包括所述VLAN ID的附加VLAN标记推送到所述网络分组上来写入标识所述网络分组以进行检查的所述VLAN ID，而不修改所述现有的VLAN标记。

19.根据权利要求16所述的软件定义网络，其中，所述VLAN ID包括标识接收到所述网络分组的至少所述第一联网设备的信息。

20.根据权利要求16所述的软件定义网络，其中，所述位写入器被配置成通过将包含所述VLAN ID的VLAN标记推送到所述网络分组上来写入标识所述网络分组以进行检查的所述VLAN ID。

用于检查的网络通信的选择性端口镜像和带内传输

技术领域

[0001] 本公开涉及用于在软件定义网络(“SDN”)中管理网络安全性的系统和方法。更特别地,但不排他地,本申请中公开的技术允许系统对分组(packet)进行标记(tag)(或“标注(color)”)以用于检查,并向分组分析器提供分组来源信息。

[0002] 附图简述

[0003] 本文中的书面公开内容描述了非限制性且非穷举的说明性实施例。本公开参考在下述附图中描绘的某些这样的说明性实施例。

[0004] 图1图示了电力传输和配电系统的简化的单线图的示例,其中多个通信设备促进软件定义网络(“SDN”)中的通信。

[0005] 图2图示了根据一个实施例的SDN架构的概念表示的示例。

[0006] 图3图示了简化过程的示例,通过该过程,SDN用VLAN对分组进行标记(或“标注”),以指示该分组应该被发送到分组分析器和/或提供来源信息。

[0007] 图4图示了SDN架构的概念表示的另一个示例。

[0008] 图5图示了SDN架构的概念表示,包括配置应用、控制面(control plane)、数据面(data plane)、多个数据消耗者/产生者设备以及选择性启用的端口镜像(port mirroring)功能。

[0009] 图6图示了用于通过SDN处理分组以进行DPI分组分析的方法的示例的流程图。

[0010] 图7图示了用于通过SDN处理分组的方法的示例的流程图,该SDN被配置成用于使用端口镜像进行分组分析。

[0011] 详细描述

[0012] 各种各样的商业和工业机构利用软件定义网络(“SDN”)。本文描述的系统和方法可以用于各种各样的应用,并且不限于任何特定的行业。本文提供的一些具体示例涉及纳入了SDN联网技术的电力传输和配电系统。

[0013] 例如,现代配电和传输系统纳入了各种通信技术,以监测并保护系统。系统可以利用通信装备以促进对电力系统上的状况进行监测并实现控制动作以维持电力系统的稳定性的各种设备之间的数据交换。通信网络携带用于对电力系统状况进行适当评估并用于基于这些状况实现控制动作有用的信息。通常希望监测和/或控制系统快速响应电力传输和配电系统中的状况改变。相应地,经由通信网络传输的消息在具体的时间帧内被路由到它们的目的地可能是有用的。

[0014] 在各种实施例中,控制器可用于配置联网设备、建立网络流并监测网络状况。SDN联网技术为电力系统提供了各种优势。例如,SDN联网技术允许可快速配置的默认拒绝(deny-by-default)安全性、更好的延迟控制、对称传输能力、冗余和故障转移计划等。

[0015] SDN支持程序化的改变控制平台,其允许将整个通信网络作为单一资产进行管理,这简化了对网络的理解,并能够对网络进行持续监测。在SDN中,决定将流量路由到哪里的系统(即,控制面)与执行流量在网络中的转发的系统(即,数据面)可以是不同的。

[0016] 控制面可以被修改以通过通信网络创建具体的数据流来实现网络资源的最佳或

目标使用。“流条目(flow entry)”用于指控制数据流的一组或多组参数。“数据流”或简称为“流”用于指网络中任何类型的数据转移,诸如从特定源发送到特定单播、任播或多播目的地的一组或一系列IP分组。数据流条目可以准许基于各种标准的具体网络路径,这些标准为网络运营商提供显著和精确的控制。相比之下,在大型传统网络中,尝试使网络发现路径与应用期望的数据路径匹配可能是涉及改变许多设备中的配置的具有挑战性的任务。为了解决这个问题,很多设备上使用的管理接口和特征组都不是标准化的。

[0017] 在电力传输和配电系统的背景下管理传统网络的明显的复杂性是由于每个网络设备(例如,交换机或路由器)具有集成的控制逻辑和数据转发逻辑的事实。例如,在传统的网络路由器中,诸如路由信息协议(RIP)或开放式最短路径优先(OSPF)的路由协议构成确定应该如何转发分组的控制逻辑。路由表标识网络路径,以根据路由协议的规定在网络内转发分组。类似地,在诸如网桥(或网络交换机)的2层设备(Layer 2device)中,配置参数和/或生成树算法(STA)提供确定分组路径的控制逻辑。因此,传统网络中的控制面分布在交换结构(网络或联网设备)中。因此,改变网络的转发行为包括单独改变许多(可能是所有)联网设备的配置,而不是通过集中的控制面以编程方式改变。

[0018] 在许多SDN实施例中,SDN控制器实施网络控制面并确定分组(或帧)应该如何在网络中流动(或转发)。SDN控制器通过设定联网设备的转发表和/或其他配置设置将该信息传送给数据面中的联网设备。相应地,SDN实现了对网络的集中化配置和管理。SDN中的数据面包括分组转发设备,该分组转发设备具有通信接口,以从控制器接收转发信息。

[0019] 区分并转发分组的一种方法包括VLAN标记。虚拟局域网络(VLAN)可以在具有共享拓扑的网络中隔离流量。分组可以有VLAN ID或标记来指示该分组应该转发到哪里。除了简化网络的管理之外,SDN架构也实现了监测和故障排除特征,这些功能有利于在配电系统中使用。

[0020] 在一些实施例中,系统可以利用各种SDN特征来监测网络中的物理和/或逻辑通信链路。逻辑通信链路可以包含用于在通信主机之间建立连接的任何数量的物理链路和转发元件。用于创建实现逻辑通信链路的特定通信路径的物理链路和转发元件可以基于网络中的状况进行调整和改变。

[0021] 在以太网中,网络运营商可能需要深入了解网络流量。网络可以通过入侵检测系统(IDS)和/或深度分组检查(DPI)系统来路由流量。端口镜像可以将网络流量定向到IDS或DPI系统,其中网络交换机复制通过交换机端口的分组,并将复制的分组发送到IDS或DPI系统。匹配系统可以基于匹配规则标识用于检查的分组。联网设备(例如,网络交换机)可以对匹配的分组进行“标记”或“标注”,以标识它用于路由到IDS或DPI系统进行分析。可以使用多种匹配算法中的任何算法,并且可以根据所需的网络安全级别而变化。标识用于检查的分组的匹配算法被广泛理解,并且适用于与本文描述的系统和方法结合使用。分组检查器可以是基于处理器的设备,独立于联网设备或作为联网设备的一部分集成,以实现标识分组用于经由IDS或DPI系统进行分组检查的匹配算法。然而,为了不模糊本文阐述的系统和方法的描述,这种匹配算法的细节在本公开中被省略。一旦分组被“匹配”用于进一步检查或分析,本文描述的系统和方法允许动态端口镜像和/或路由到IDS或DPI系统。

[0022] 各种通信设备可以利用本文描述的各种实施例。如本文使用的术语“通信设备”包括能够在数据通信网络中接受和转发数据流量的任何设备。除了接受和转发数据流量的功

能之外，通信设备还可以执行各种各样的其他功能，并且范围可以从简单的设备到复杂的设备。

[0023] 适用于本文所描述的系统和方法的通信设备的具体示例包括但不限于交换机、集线器、中继器、网关、路由器、网桥、调制解调器、无线接入点和线路驱动器。如本文所使用的，术语“通信设备”在上下文允许的情况下，还可以包括各种各样的混合联网设备，诸如多层交换机、协议转换器、终端适配器、桥接路由器、代理服务器、防火墙设备、网络地址译码器(network address translators)、多路复用器、网络接口控制器等。因此，虽然在本文使用网络交换机作为示例描述了系统和方法的许多原理，但是应当理解，这些原理可以适用于许多其他联网设备类型。

[0024] 通过参照附图能够进一步理解本公开的实施例，其中通篇相似的部分由相似的数字标记。如在本文中的附图中一般性地描述和示出的，所公开实施例的部件可以以各种不同的配置来布置和设计。因此，本公开的系统和方法的实施例的以下详细的描述不旨在限制本公开所要求保护的范围，而是仅代表本公开的可能实施例。此外，除非另有说明，否则方法的步骤不一定需要按照任何特定的顺序或甚至依次序地执行，这些步骤也不需要仅执行一次。

[0025] 所描述的实施例的几个方面可作为软件模块或部件来实现。如本文中所使用的，软件模块或部件可包括任何类型的计算机指令或计算机可执行代码，这些指令或代码位于存储器设备内和/或作为电子信号通过系统总线或者有线或无线网络传输。例如，软件模块或部件可包括计算机指令的一个或更多个物理块或逻辑块，其可被组织为例程、程序、对象、部件、数据结构等，其执行一个或更多个任务或实现特定的抽象数据类型。

[0026] 在某些实施例中，特定的软件模块或部件可包括被存储在存储器设备的不同位置中的不同指令，其共同实现模块的所描述的功能。事实上，模块或部件可包括单一指令或许多指令，并且可以分布在几个不同的代码段上、分布在不同的程序之间以及跨几个存储器设备分布。一些实施例可在分布式计算环境中实践，其中任务由通过通信网络链接的远程处理设备执行。在分布式计算环境中，软件模块或部件可位于本地存储器存储设备和/或远程存储器存储设备中。另外，在数据库记录中绑定或呈现在一起的数据可驻留在相同的存储器设备中或跨几个存储器设备驻留，并且可以跨网络在数据库中的记录字段中链接在一起。

[0027] 实施例可作为计算机程序产品来被提供，包括具有在其上所存储的指令的非暂态计算机和/或机器可读介质，该指令可用于对计算机(或另一电子设备)进行编程以执行本文中所描述的过程。例如，非暂态计算机可读介质可存储指令，当该指令由计算机系统的处理器执行时，使处理器执行本文中所公开的某些方法。非暂态计算机可读介质可包括但不限于硬盘、软盘、光盘、CD-ROM、DVD-ROM、ROM、RAM、EPROM、EEPROM、磁卡或光卡、固态存储器设备、或适用于存储电子器件和/或处理器可执行指令的其他类型的机器可读介质。

[0028] 图1图示了电力传输和配电系统100的简化的单线图的实施例的示例，其中多个通信设备可以促进软件定义网络中的通信。电力输送系统100可以被配置成生成、传输电能，并将电能分配给负载。电力输送系统可包括装备，诸如电力发电机(例如，发电机110、112、114和116)、电力变压器(例如，变压器117、120、122、130、142、144和150)、电力传输和输送线(例如，线124、134和158)、电路断路器(例如，断路器152、160、176)、总线(例如，总线118、

126、132和148)、负载(例如,负载140和138)等等。各种其他类型的装备也可被包括在电力输送系统100中,诸如电压调节器、电容器组以及各种其他类型的装备。

[0029] 变电站(substation)119可以包括发电机114(其可以是分布式发电机),该发电机114可以通过升压变压器(step-up transformer)117连接到总线126。降压变压器(step-down transformer)130将总线126连接到配电总线132。各种配电线136和134可以连接到配电总线132。配电线136可以通向变电站141,并且IED 106可以监测和/或控制配电线106。例如,IED 106可以选择性地打开和闭合断路器152。配电线136A可以给负载140馈电。附加的降压变压器144被示出经由配电线136与配电总线132通信,并可用于逐步降低由负载140消耗的电压。

[0030] 配电线134可以通向变电站151,并向总线148输送电力。总线148也可经由变压器150接收来自分布式发电机116的电力。配电线158可以将电力从总线148输送到负载138,并且可以包括另一个降压变压器142。电路断路器160可以选择性地将总线148连接到配电线134。IED 108可以监测和/或控制电路断路器160以及配电线158。

[0031] 中央监测系统172和智能电子设备(IED)(诸如IED 104、106、108、115和170)可以监测、控制、自动操作和/或保护电力输送系统100。通常,发电和传输系统可以利用IED进行装备的保护、控制、自动操作和/或监测。例如,系统可以使用IED监测许多类型的装备,包括输电线、配电线、电流互感器、总线、交换机、电路断路器、自动开关(recloser)、变压器、自耦变压器、抽头变换器(tap changer)、电压调节器、电容器组、发电机、电动机、泵、压缩机、阀以及各种其他类型的受监测装备。

[0032] 如本文所使用的,IED(如IED 104、106、108、115和170)可指监测、控制、自动操作和/或保护系统100内的受监测装备的任何基于微处理器的设备。例如,这样的设备可包括远程终端单元、差动继电器(differential relay)、距离继电器、方向继电器、馈电继电器、过电流继电器、电压调节器控件、电压继电器、断路器故障继电器、发电机继电器、电动机继电器、自动化控制器、间隔控制器(bay controller)、计量器、自动开关控件(recloser controls)、通信处理器、计算平台、可编程逻辑控制器(PLC)、可编程自动化控制器、输入和输出模块等等。术语IED可用于描述单个IED或包括多个IED的系统。

[0033] 公共时间信号可分配在整个系统100中。利用公共或通用的时间源可确保IED具有可用于生成时间同步数据(如同步相量)的同步时间信号。在各个实施例中,IED 104、106、108、115和170可接收公共时间信号168。时间信号可使用网络162或使用公共的时间源(诸如全球导航卫星系统(“GNSS”)等)而被分配在系统100中。

[0034] 根据各个实施例,中央监测系统172可包括多种类型的系统中的一个或更多个。例如,中央监测系统172可以包括监控与数据采集(SCADA)系统和/或广域控制与态势感知(WACSA)系统。中央IED 170可以与各个IED 104、106、108和115进行通信。IED 104、106、108和115可以远离中央IED 170,并且可以通过各种介质进行通信,诸如来自IED 106的直接通信或通过通信网络162进行通信。根据各个实施例,某些IED可以与其他IED直接进行通信(例如,IED 104与中央IED 170直接进行通信),或者可以经由网络162进行通信(例如,IED 108经由通信网络162与中央IED 170进行通信)。

[0035] 包括但不限于多路复用器、路由器、集线器、网关、防火墙和交换机的联网设备可用于促进网络162。在一些实施例中,IED和网络设备可包括物理上不同的设备。在其他实施

例中,IED和网络设备可以是复合设备,或者可被配置成用多种方式来执行重叠的功能。IED和网络设备可包括多功能硬件(例如,处理器、计算机可读存储介质、通信接口等),其可被利用以执行关于系统100内的装备的操作和/或网络通信的各种任务。

[0036] SDN控制器180可以被配置成与网络162中的装备对接以创建促进各个IED 170、115和108、监测系统172、和/或其他联网的设备之间的通信的SDN。在各个实施例中,SDN控制器180可以被配置成设置用于控制网络162中的数据流的流条目。

[0037] 在各个实施例中,SDN控制器可以实现被配置成允许动态端口镜像的SDN应用。在各个实施例中,系统(或用户)可以利用SDN应用来选择性地镜像来自一个或更多个联网设备的一个或更多个流。在一些实施例中,SDN应用使得多个联网设备上的端口之一充当"嗅探端口(sniffing port)",该"嗅探端口"仅用于将被标记或标注以供检查的分组转发到分组分析器设备,诸如IDS或DPI系统。

[0038] 图2图示了SDN架构的概念表示的示例,该SDN架构包括多个配置应用、控制面、数据面、多个数据消耗者/产生者设备、以及包括分组处理信息和数据分组内容的数据分组的高级图。应用202a、202b和202c表示用于配置控制面204内(或实施控制面204)的控制器206的各种应用中的任何应用。这些应用可以被定制以满足各种系统需求。

[0039] 路径214可用于在数据面220和控制面204之间传递信息。在一些实施例中,路径214可以使用例如开放流协议(OpenFlow protocol)。开放流协议通过配置交换机的行为的方式来操作和控制分组如何被转发,在图2中通过流条目208、210和212来表示。路径214因此可以将流量导向预期的联网设备,诸如数据面220上的联网设备222和224。对流条目212的详细查看图示了流条目212包括匹配字段216和分组处理信息218。

[0040] 分组处理信息218可以包括但不限于:分组优先级、计量信息、分组指令以及分组或流超时指令。匹配字段216可以与分组信息进行比较,并随后用于将分组过滤成对应的流。匹配字段可以包括但不限于:入口端口号;以太网源、目的地和类型;IP源、目的地和协议;源端口;目的地端口;以及VLAN标识(VLAN ID)。可选的匹配字段可用于匹配数据分组的VLAN ID。

[0041] 可以用标识分组的来源(origin)、分组进入网络的点和/或分组已经穿过的网络路径的信息来对分组进行标记或"标注"。可以使用各种方法和技术来进行标记,包括使用被推送到分组上的包含源信息的VLAN ID。SDN上被配置成向分组分析器发送流量的每个软件定义交换机都可以通过将VLAN ID推送到分组上来"标记"该分组。如果存在现有的VLAN ID,则可以将第二VLAN ID添加到(例如,推送到)分组,该第二VLAN ID包括标识分组的来源和/或目的地信息的信息。

[0042] 例如,可以使用已知的位掩码模式的组合来生成由SDN中的交换机添加的VLAN ID。例如,第一位掩码模式可以用于指示网络分组应该由分组分析器进行分析。SDN中的交换机上的端口可以通过唯一的位掩码模式来标识。VLAN ID可以被构造成包含关于分组的源的信息以及转发信息。可以有多种方法将VLAN与对应的交换机和端口进行匹配,包括但不限于,使用组合位掩码的结构来标识端口以及带有交换机列表和对应VLAN的查找表。位掩码中的一个位(例如,位掩码中的最高有效位或最高位(highest order bit))可以标识要进行检查并要发送到分组分析器230的分组。在一些实施例中,VLAN值中的最高位用于防止分组根据原始指令被路由。可以由位掩码提供另外的分组区分。例如,可以使用具体的位

掩码或基本掩码来指定用于端口镜像和/或用于转发到DPI系统的分组。

[0043] 数据面220包括彼此通信的联网设备222和224。在各个实施例中，联网设备222和224可以实施为交换机、多路复用器以及其他类型的通信设备。通信链路可以实施为以太网、光纤和/或其他形式的数据通信信道。数据消耗/产生设备226和228可以表示电力传输和配电系统内的产生或消耗数据的各种设备。

[0044] 例如，数据消耗/产生设备可以实施为被配置成监测电力传输线的一对传输线继电器。传输线继电器可以监测流过传输线的电力的各个方面(例如，电压测量结果、电流测量结果、相位测量结果、同步相量等)，并且可以传送测量结果以实现对传输线的保护策略。传输线继电器之间的流量可以使用由控制器实现的多个数据流来路由通过数据面220。数据消耗/产生设备226和228可以实施为多种设备中的任何设备。

[0045] 图3图示了简化过程的示例，通过该过程，SDN用VLAN标记一个分组，以指示该分组应当被发送到分组分析器。网络设备可以接收原始数据分组302。原始数据分组302包括分组信息(例如，有效载荷)。原始数据分组302可以包括也可以不包括VLAN ID 304。初始分组分析系统可以确定该分组应该被进一步检查。位掩码310可用于生成新的VLAN ID 316。新的VLAN ID 316可用于对该分组进行标记或“标注”，以指示该分组应当被路由到分组分析器。

[0046] 如前所述，原始数据分组302可以具有或不具有将保持完整的现有VLAN ID 304。作为具体示例，网络管理员可以选择位掩码0x800或100000000000来指示分组应当被发送到分组分析器。最高有效位(位12)为高(1)，其指示分组应被路由到分组分析器。另一个位掩码，诸如000000001010，可以指示特定网络交换机上的第10个端口最初接收到了分组。当这两个位掩码经由例如“或(OR)”门与分组信息逻辑地组合时，可以使用写动作将新的VLAN ID 316推送到分组上。新的VLAN ID 316标识用于转发到分组分析器的分组，并且还提供具体的来源信息。在该实施例中，掩码中的最高位被SDN用来标识分组要被发送到分组分析器，而不管分组中的其他位和/或现有的VLAN ID 304。实际上，基于与预期路由和/或来源相关的一个或更多个位掩码的新VLAN ID 316被添加到原始数据分组302。新的数据分组350包括分组信息306、原始VLAN ID 304和新的VLAN ID 316。在一些实施例中，不同的位掩码可以用于不同的目的。例如，第一位掩码值可以用于路由到DPI系统，第二位掩码值可以用于端口镜像，而第三位掩码值可以用于另一种类型的分组检查。

[0047] 如前所述，位掩码还可以提供来源信息。被标识用于进一步检查的分组可以在交换机5的端口3上被接收。作为具体示例，通过将标识交换机的二进制值移位6位，可以将交换机标识编码在VLAN ID的第7-11位中。交换机5的二进制值是101。该值左移6位，使得最低有效位在第7位上，并与原始位掩码进行“或”运算，得到二进制值100101000000。最后6位可以被保留来编码分组的端口标识信息。由于端口3的二进制值是000011，位掩码的逻辑“或”值变为100101000011。位掩码的最高有效位指示分组应当被发送到分组分析器。第7-11位对分组所源自于的交换机的标识信息进行编码。第1-6位对分组所源自于的端口的标识信息进行编码。这些位掩码的组合用于生成新的VLAN ID 316，然后该新的VLAN ID 316被推送到原始数据分组302上以形成新的数据分组350。

[0048] 应当理解，根据网络的需要，位掩码中的位数可以更大或更小。上面的示例允许标识多达32个联网设备(第7-11位)和每个联网设备上的多达64个端口(第1-6位)。在其他实

施例中，可能希望对分组所源自于的每个网络设备的整个序列号或mac地址进行编码。标准协议可以限制VLAN ID中的可用位的总数。然而，本文中公开的概念可以被修改和/或扩展以符合多种协议和用例中的任意协议和用例。

[0049] 在一些实施例中，可以分配额外的位来编码分组是否已经被镜像或从其预期的目的地重新路由。由于原始分组被路由到其原始的预期目的地，镜像分组在检查后可以被丢弃。一旦分组检查完成，为检查而重新路由的分组可以被转发到其原始目的地。这样的分组可以被检查，然后返回到交换机和/或来源的端口，在这个点处，新的VLAN ID被去除，并且分组被转发到其原始的预期目的地。

[0050] 在一些实施例中，系统可以不需要标识交换机和/或来源端口。在这样的实施例中，可以将较少的位分配给位掩码。例如，如果网络中只有25个联网设备，并且端口标识信息不是必需的，那么位掩码可以只包括6位——一个最高有效位指示分组应该被发送到分组分析器，并且5个额外的位用于编码分组所源自于的交换机的标识信息。

[0051] 上面的示例仅仅表示众多可能的编码组合中的一些，这些编码组合用于标记或标注分组以进一步分析和提供一些来源信息。基于系统的目标，可以使用可替代的标记或标注方法。

[0052] 图4图示了SDN架构的概念表示的示例。所图示的实施例包括配置应用、控制面、数据面、多个数据消耗者/产生者设备、以及高级图VLAN分组分段和路由。一旦分组被标识作为应当被发送到分组分析器的分组，VLAN值可以被分配给该分组，以将该分组路由到分组分析器422。也可以包括网络分组路由规范。例如，VLAN值可以指示分组应该通过指定的嗅探端口被路由，和/或可以为要被路由到分组分析器422的分组指定特定的流量流。

[0053] 初始步骤可以包括确定分组是否满足要被发送到分组分析器422的匹配标准(例如，确定VLAN ID的最高有效位是否是1)。如果分组满足匹配标准，该匹配规则的动作可以是将分组发送到分组分析器422，而不是将其发送到原始目的地。不具有满足匹配规则的VLAN ID(例如，最高有效位不是1)的分组可以被路由到它们的原始目的地(例如，数据消耗/产生设备414、416、418和420之一)。

[0054] 在一些实施例中，分组检查可以是单向功能，其中分组被检查并丢弃。端口镜像可用于确保这种检查不会导致数据面通信的分组丢失。其他形式的分组检查可以是双向的，并且导致分组在检查之后返回到它们的来源和/或路由到它们的预期目的地。例如，当在网络上配置了IDS时，发送到IDS的分组可以是来自具体联网设备上具体端口的分组的副本(例如，通过端口镜像实现)。复制的分组典型地在分析后被丢弃。

[0055] 相比之下，DPI系统可能打算在检查后将分组发送回其源。当然，如果该分组被标识为不期望的，则该分组可以被丢弃和/或可以采取其他保护性动作。否则，如果DPI系统确定该分组在网络上是允许的，则该分组可以被发送回来源的交换机，并返回到其原始的预期目的地。将分组从分组分析器422发送回来源入口交换机(例如，410)的动作可以经由与典型的流匹配规则方向相反的一组流匹配规则来实现。分组路由的下一个步骤是通过数据面408发回。当分组回到其来源时，可以从分组移除分组分析VLAN ID，并且分组可以被正常处理。为了促进该动作，被标记为要发送到深度分组分析器的分组的典型流可以在表2中，或者可以稍后，使得匹配的写动作可以是发送分组用于进一步处理。

[0056] 图5图示了SDN架构500的概念表示的另一个示例，该SDN架构500包括控制面504、

数据面508、多个数据消耗者/产生者设备528-540、以及选择性启用的端口镜像功能。分组可以经由数据面508内的一个或更多个网络设备(510、512和/或514)从一个数据产生设备528-540传递到另一个数据消耗设备528-540。分组可以进入SDN的数据面508。数据面508可以包含多个网络设备510-514。每个网络设备可以具有指定的路由路径516-520。根据本文所描述的系统和方法,选择性端口镜像可以通过编程方式为SDN内的一个或更多个(或所有)端口启用。因此,可以选择性地使每个联网设备能够通过路径522-526将它们的流量镜像到分组分析器534。选择性的流量镜像允许从单个端口对单个流的流量进行动态粒度数据收集。这一过程可以在不中断正常网络流的情况下远程地按需完成。

[0057] 分组路由的细节可以取决于网络管理员的需要。如果使用专用端口来确定应当进一步分析哪些分组,则该“嗅探”端口上的传入流量可以被路由到分组分析器。如果其他流量共享该嗅探端口,则接收交换机可以有一个匹配规则,该匹配规则使用位掩码来标识被标记要进行检查的分组,这些分组应该被路由到分组分析器。利用SDN,网络设备510-514可以使用第一个最高有效位来确定分组是否需要被发送到分组分析器。该匹配过程可以包括速率限制特征,该速率限制特征限制被发送到分组分析器的流量总量。例如,如果分析器被流量淹没,一些最初指定给分组分析器的分组可以简单地被丢弃。

[0058] 图6图示了用于通过SDN来处理分组的方法的示例的流程图,该SDN被配置用于分组分析。在604,在网络上接收入口分组。在606,系统的部件(诸如联网设备)可以确定分组是否满足用于分组分析的匹配标准。如果分组没有被标识用于传输到分组分析器,则在607,该分组可以根据现有指令被路由。然后,在604,方法可以通过接收另一个入口分组而再次开始。

[0059] 然而,如果分组满足匹配标准,则在608,可以创建VLAN ID。VLAN ID的最高有效位可以“标记”或“标注”分组,以便由随后的联网设备自动路由到分组分析器。VLAN ID的其他位可用于标识数据分组的来源信息(例如,交换机和/或端口标识信息)。在610,VLAN ID被添加到数据分组(和任何现有的VLAN标记),以在611将分组路由到分组分析器。

[0060] 在一些实施例中,在612,分组可以通过任意数量的联网设备和/或专用端口被路由到分组分析器。沿途的每个联网设备可以使用匹配规则来确定该分组是打算给分组分析器的,而不考虑原始分组路由指令。例如,后续联网设备可以确定VLAN ID的最高有效位是1,因此自动将分组路由到分组分析器,而无需进一步分析或检查。然后,在613,分组分析器可以分析分组。在一些实施例中,系统然后可以在614确定分组是否需要被发送回其来源。如果不需要,则可以在618丢弃该分组。如果它确实需要被发回,则分组可以在615被路由回其来源。在616,系统可以从分组去除“标记”或“标注”,然后在607,根据分组的原始指令来路由分组。在一些实施例中,在618,可以简单地丢弃该分组,而不需要确定该分组是否应当被发送回去的步骤。

[0061] 图7图示了用于通过SDN处理分组的方法的示例的流程图,该SDN被配置成用于使用端口镜像进行分组分析。在704,系统可以接收分组。在706,系统可以确定接收到的分组是否应该被复制(镜像)并进一步分析。如果不需要进一步分析,则不对该分组进行镜像,而是在708,根据现有的原始路由指令简单地路由该分组。然而,如果分组需要进一步分析,则在710,该分组可以被镜像。在708,原始分组可以被路由到其原始的预期目的地。在712,可以创建镜像VLAN ID,该镜像VLAN ID将分组标识为镜像分组,标识该分组用于路由到IPS或

DPI系统，和/或标识分组最初被接收的交换机和/或端口。在714，VLAN ID被推送到镜像分组上，并且在716，镜像分组被路由到镜像目的地(例如，IPS或DPI系统)。在分析之后，镜像分组可以被丢弃。

[0062] 本文公开的方法包括用于执行所描述的方法的一个或更多个步骤或动作。方法的步骤和/或动作可以彼此互换。换句话说，除非实施例的恰当操作要求步骤或动作的具体顺序，否则可以修改具体的步骤和/或动作的顺序和/或使用，和/或可以省略步骤或动作。

[0063] 在一些情况下，众所周知的特征、结构或操作没有被详细示出或描述。此外，所描述的特征、结构或操作可以以任何合适的方式组合在一个或更多个实施例中。还将容易理解的是，如在本文中的附图中一般性地描述和图示的实施例的部件可以以各种不同的配置来布置和设计。因此，设想了实施例的所有可行的排列和组合。

[0064] 所描述实施例的几个方面可以使用硬件、固件和/或软件模块或部件来实现。如本文中所使用的，模块或部件可以包括各种硬件部件、固件代码、和/或任何类型的计算机指令或计算机可执行代码，这些指令或代码位于存储器设备内和/或作为暂态或非暂态电子信号通过系统总线，或者有线或无线网络传输。本文中所描述的许多实施例以框图形式和/或使用逻辑符号示出。应当理解，每个示出和描述的实施例的各个元件可以使用FPGA、定制的专用集成电路(ASIC)和/或作为硬件/软件组合来实现。

[0065] 在上述描述中，为了简化本公开的目的，有时在单一实施例、附图或其描述中将各种特征分组在一起。然而，本公开的这个方法不应被解释为反映以下意图：任何权利要求需要比在该权利要求中明确陈述的特征更多的特征。相反，如所附权利要求所反映的，创造性方面在于比任意单一前述公开实施例的所有特征更少的特征的组合。因此，权利要求特此被明确纳入该详细描述中，其中每个权利要求独立地作为单独的实施例。本公开也包括独立权利要求及其从属权利要求的所有排列和组合。

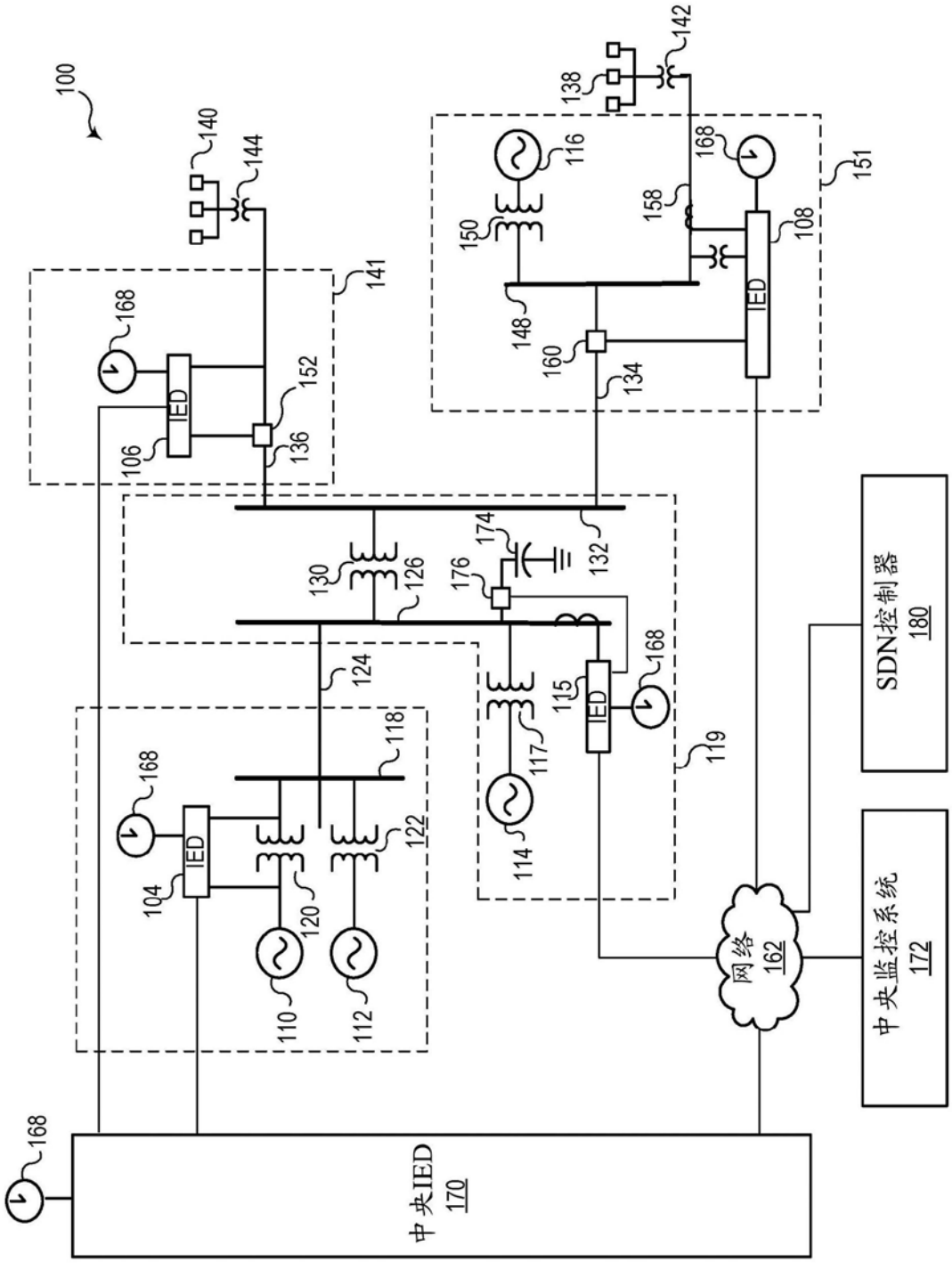

100
140
144
141
168
IED
106
152
136
142
138
116
150
158
168
151
108
148
160
134
IED
132
174
130
126
176
124
118
168
IED
104
120
122
110
112
115
117
114
119
168
SDN控制器
180
网络
162
中央监控系统
172
168
中央IED
170

图1

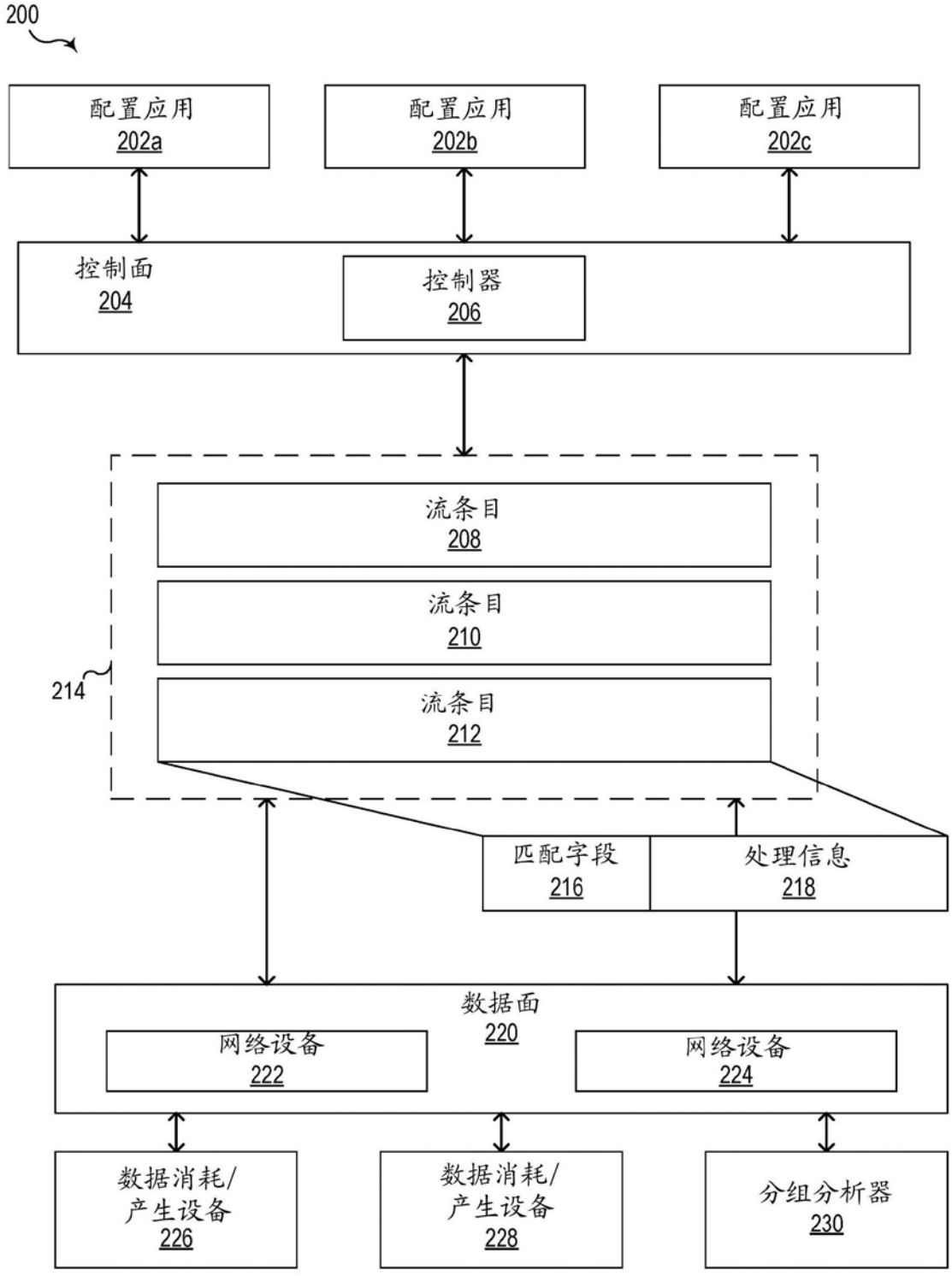

200
配置应用
202a
配置应用
202b
配置应用
202c
控制面
204
控制器
206
流条目
208
流条目
210
214
流条目
212
匹配字段
216
处理信息
218
数据面
220
网络设备
222
网络设备
224
数据消耗/
产生设备
226
数据消耗/
产生设备
228
分组分析器
230

图2

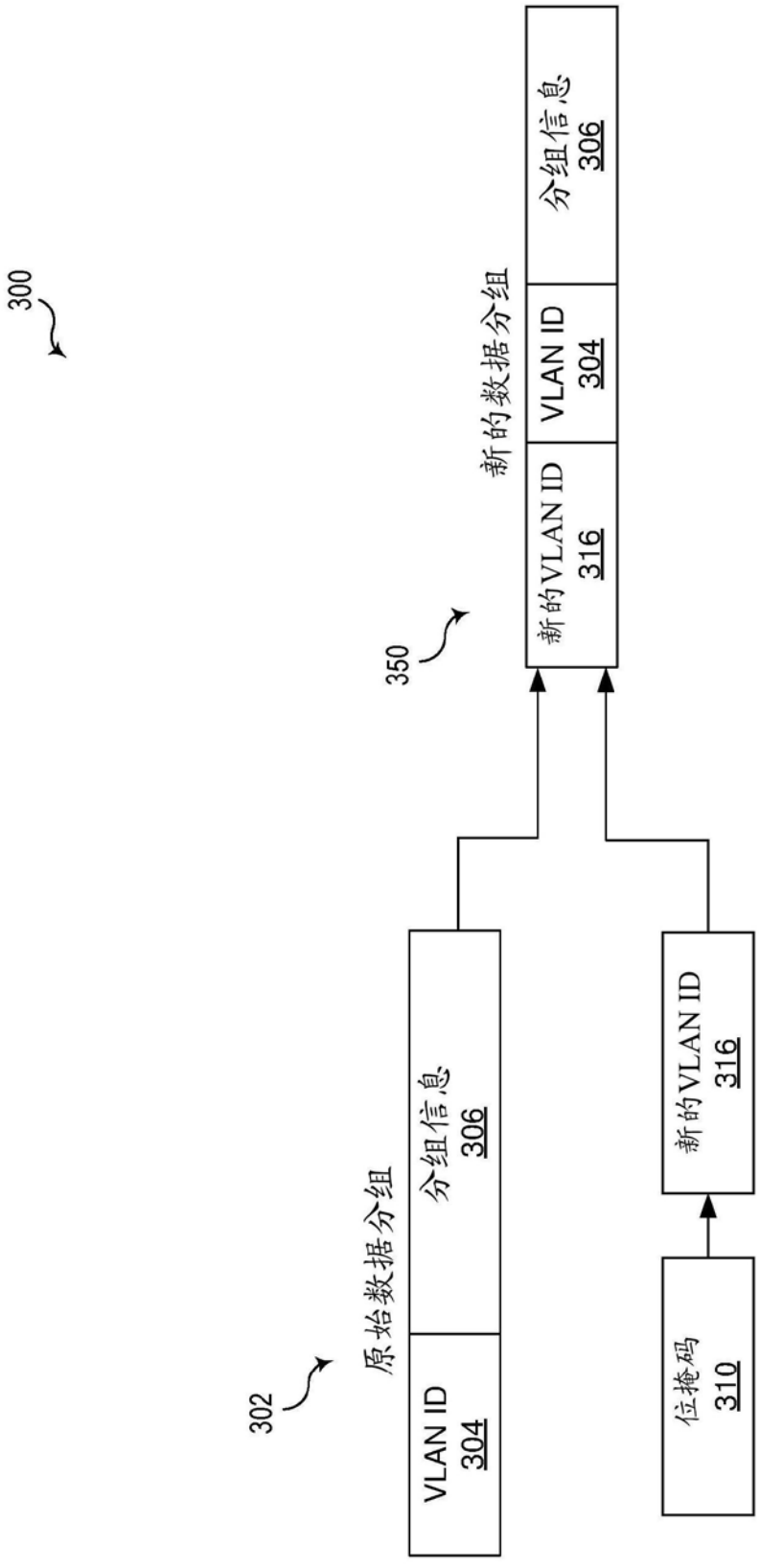

300
302
原始数据分组
VLAN ID
304
分组信息
306
350
新的数据分组
新的VLAN ID
316
VLAN ID
304
分组信息
306
位掩码
310
新的VLAN ID
316

图3

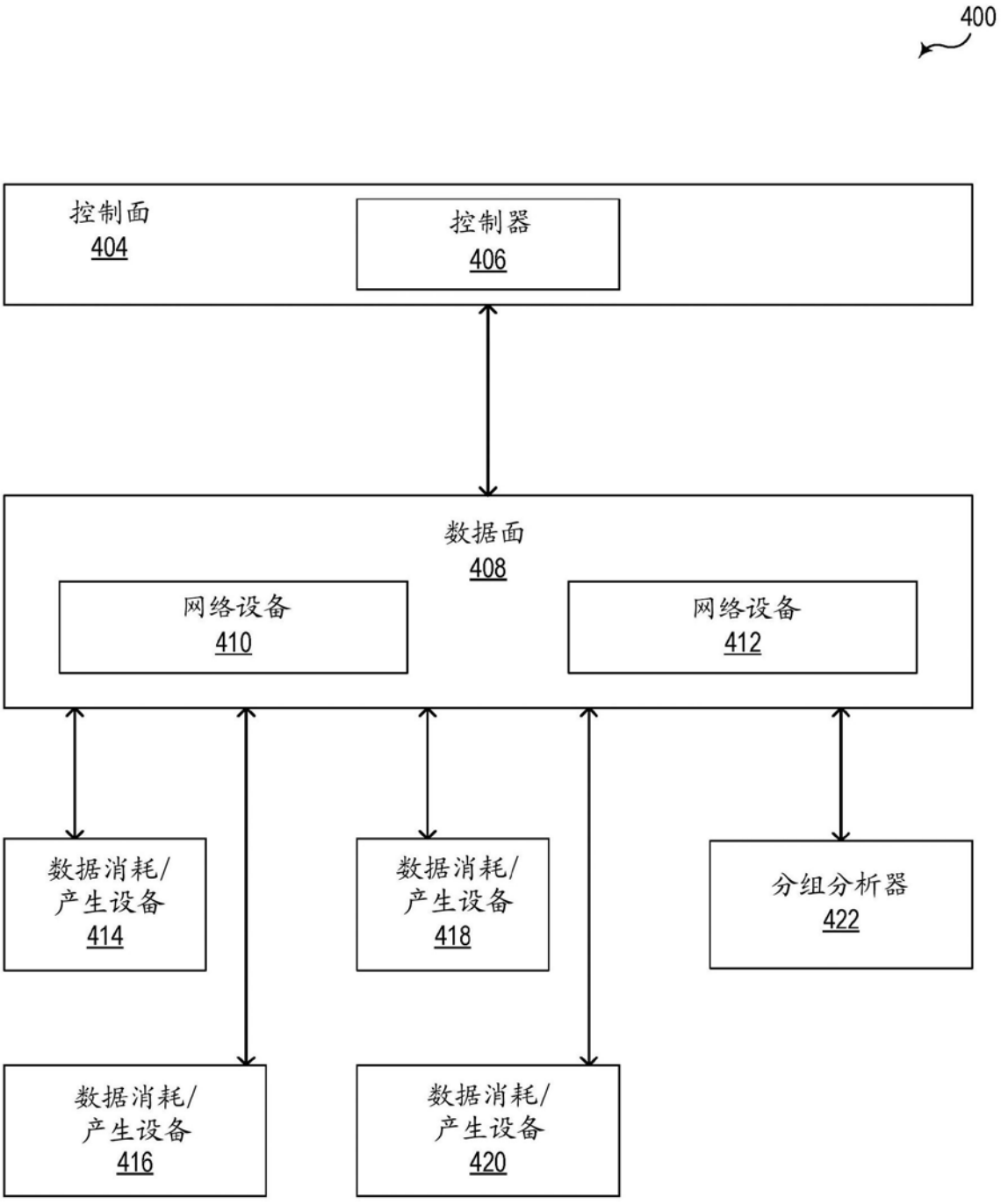

400
控制面
404
控制器
406
数据面
408
网络设备
410
网络设备
412
数据消耗/
产生设备
414
数据消耗/
产生设备
418
分组分析器
422
数据消耗/
产生设备
416
数据消耗/
产生设备
420

图4

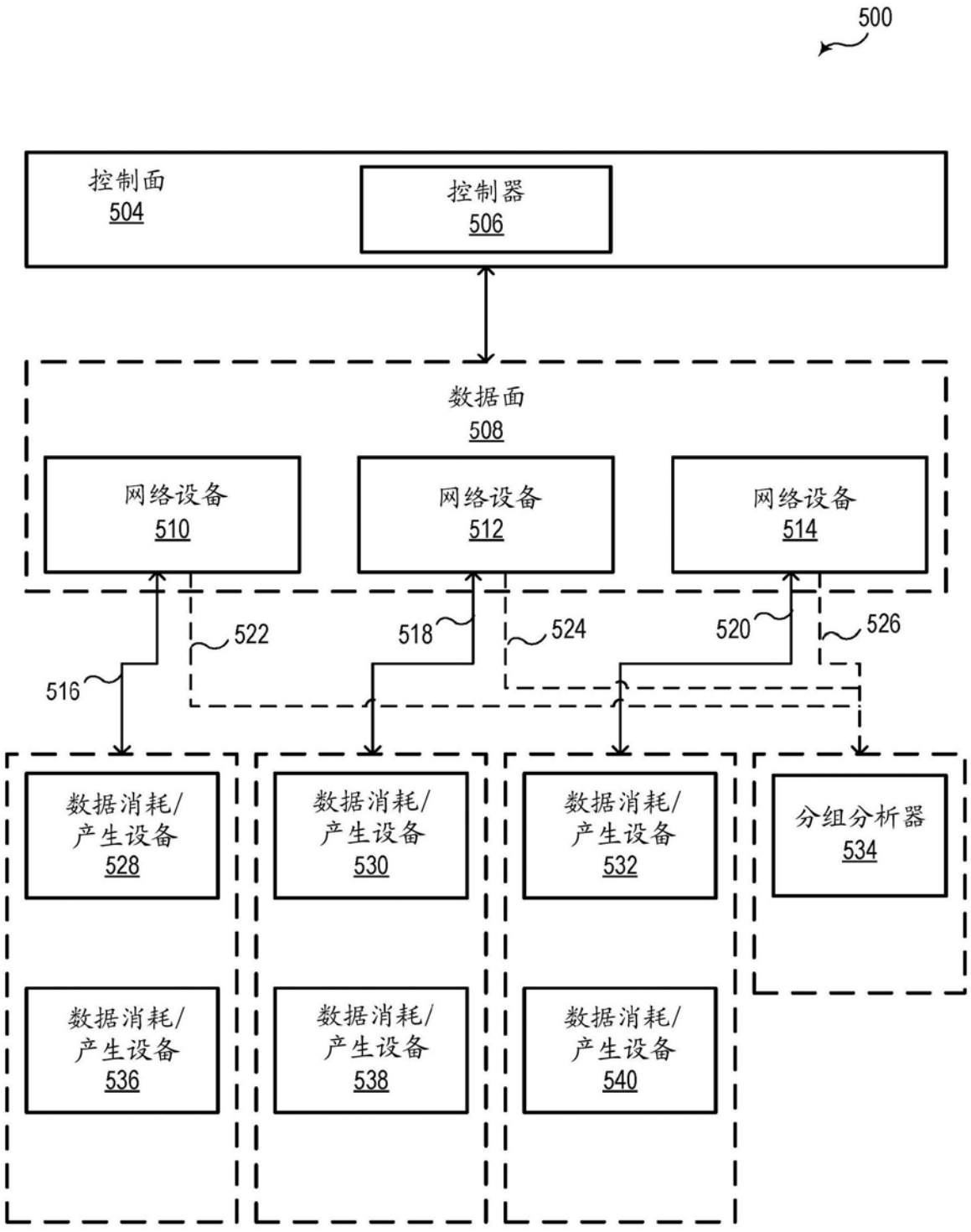

500
控制面
504
控制器
506
数据面
508
网络设备
510
网络设备
512
网络设备
514
516
522
518
524
520
526
数据消耗/
产生设备
528
数据消耗/
产生设备
530
数据消耗/
产生设备
532
分组分析器
534
数据消耗/
产生设备
536
数据消耗/
产生设备
538
数据消耗/
产生设备
540

图5

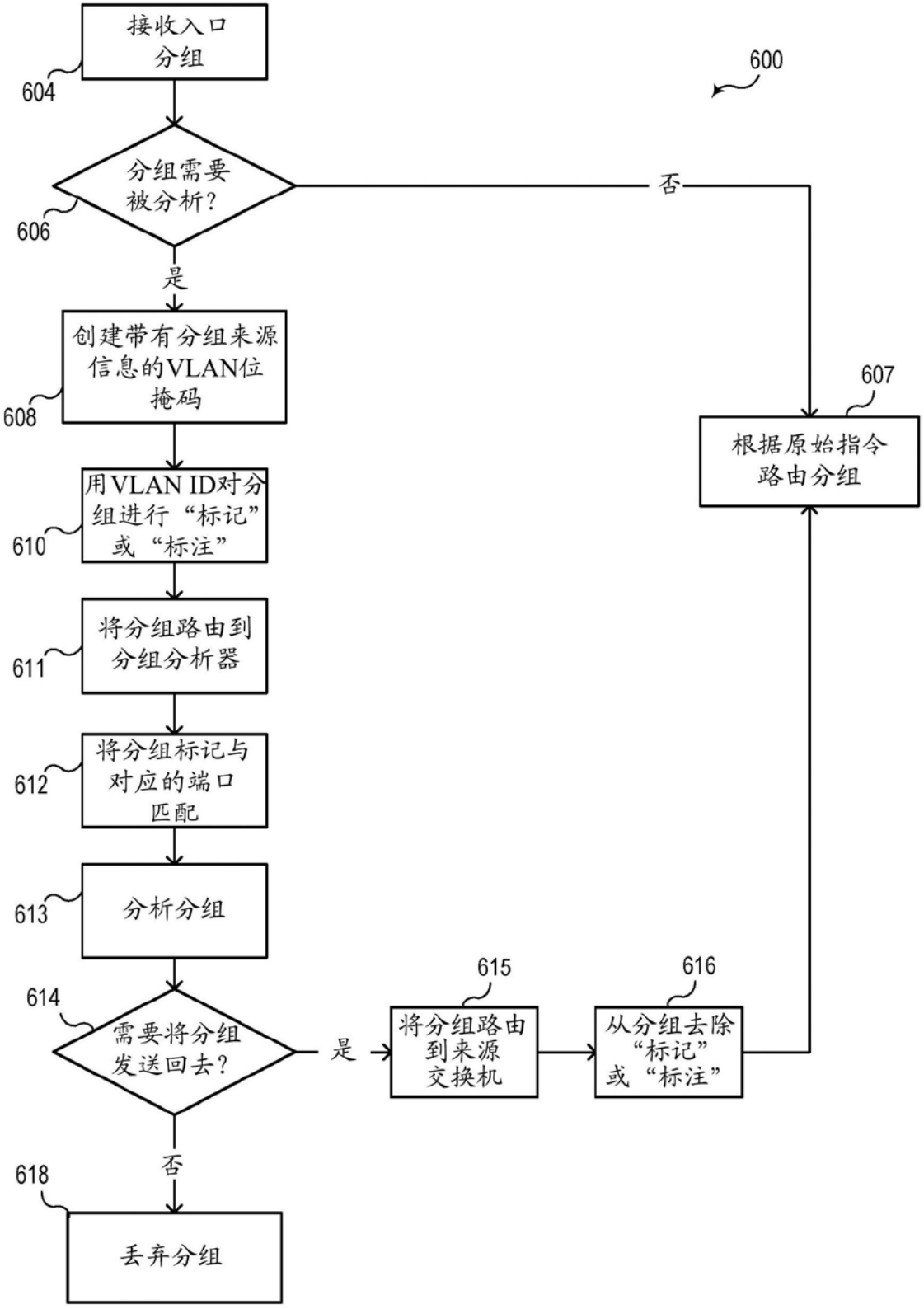

接收入口分组
604
600
分组需要被分析?
606
否
是
创建带有分组来源信息的VLAN位掩码
608
607
根据原始指令路由分组
用VLAN ID对分组进行“标记”或“标注”
610
将分组路由到分组分析器
611
将分组标记与对应的端口匹配
612
分析分组
613
615
616
614
需要将分组发送回去?
是
将分组路由到来源交换机
从分组去除“标记”或“标注”
否
618
丢弃分组

图6

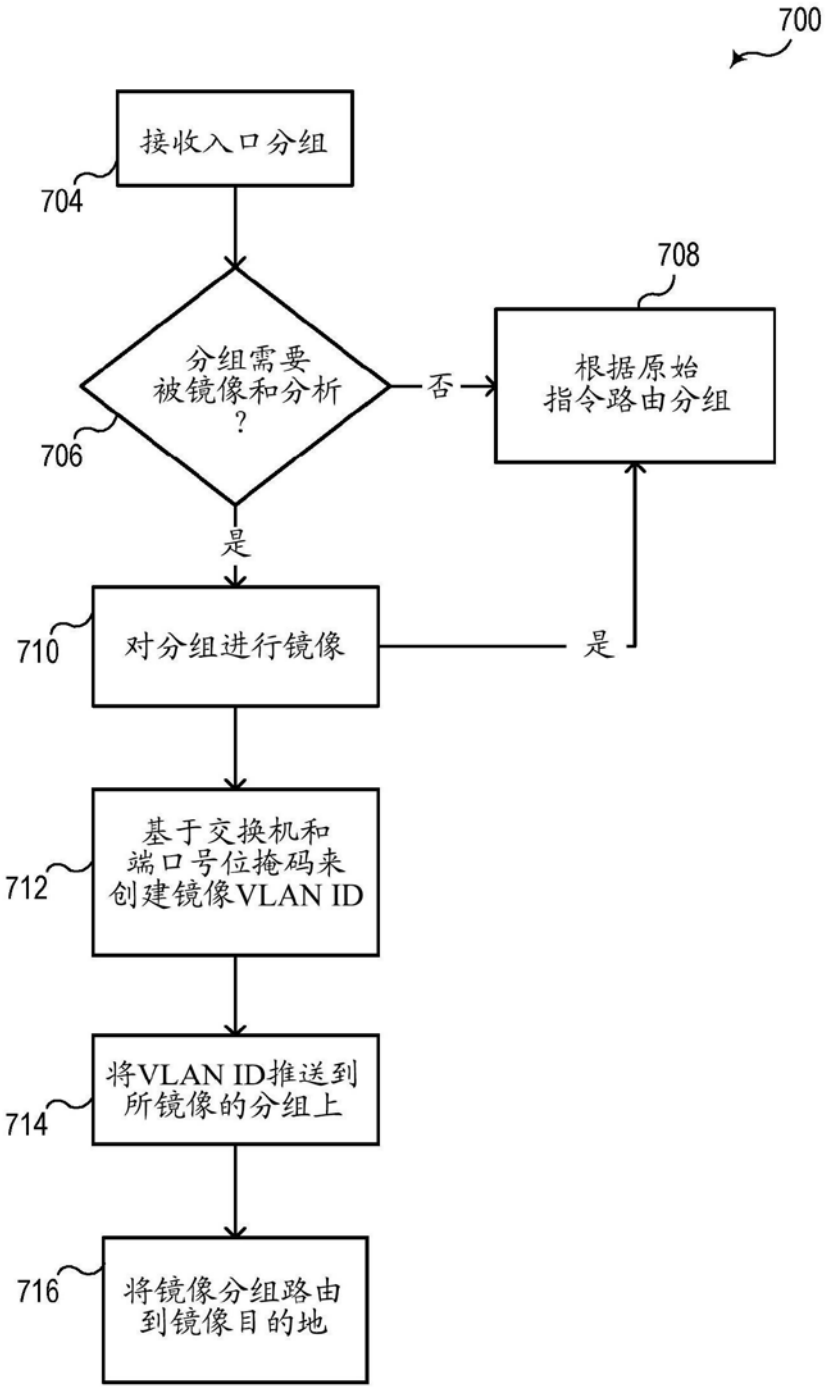

700
接收入口分组
704
分组需要被镜像和分析？
706
否
708
根据原始指令路由分组
是
710
对分组进行镜像
是
基于交换机和端口号位掩码来创建镜像VLAN ID
712
将VLAN ID推送到所镜像的分组上
714
716
将镜像分组路由到镜像目的地

图7