(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 106982149 B
(45)授权公告日 2019.10.01

(21)申请号 201611242762.8

(22)申请日 2016.12.29

(65)同一申请的已公布的文献号
申请公布号 CN 106982149 A

(43)申请公布日 2017.07.25

(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号银联大厦

(72)发明人 袁航 周雍恺 祖立军 陈华俊 严峻岭 刘国宝 何朔

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王星 付曼

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 12/931(2013.01)
H04L 29/08(2006.01)

(56)对比文件
CN 104168144 A,2014.11.26,
CN 104601432 A,2015.05.06,
CN 103973481 A,2014.08.06,
CN 103684922 A,2014.03.26,
US 2014328180 A1,2014.11.06,

审查员 薛乐梅

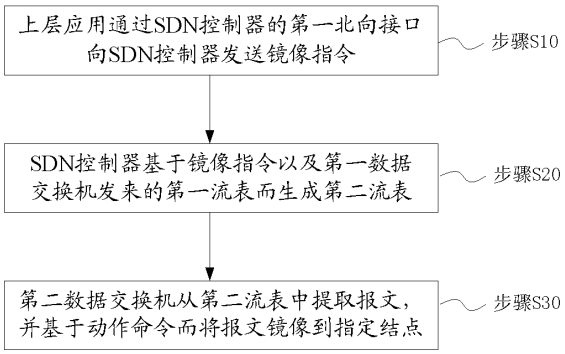
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于SDN的报文镜像方法及网络流量监控管理系统

(57)摘要

本发明涉及一种基于SDN的报文镜像方法，其中，SDN控制器与上层应用、及至少一个数据交换机分别耦合，方法包括如下步骤：a)、上层应用通过SDN控制器的第一北向接口向SDN控制器发送镜像指令；b)、SDN控制器基于镜像指令以及第一数据交换机发来的第一流表而生成第二流表；其中，第一数据交换机发起报文的传输，第一流表封装报文，第二流表至少包括对应于镜像指令的动作命令；以及c)、第二数据交换机从第二流表中提取报文，并基于动作命令而将报文镜像到指定结点。该方法能够实现较细粒度的流量监控，同时减轻了监控服务器的负载。



CN 106982149 B

1.一种基于SDN的报文镜像方法,其中,SDN控制器与上层应用、及至少一个数据交换机分别耦合,所述方法包括如下步骤:

a)、所述上层应用通过所述SDN控制器的第一北向接口向所述SDN控制器发送镜像指令;

b)、所述SDN控制器基于所述镜像指令以及第一数据交换机发来的第一流表而生成第二流表;其中,所述第一数据交换机发起报文的传输,所述第一流表封装所述报文,所述第二流表至少包括对应于所述镜像指令的动作命令;以及

c)、第二数据交换机从所述第二流表中提取所述报文,并基于所述动作命令而将所述报文镜像到指定结点。

2.根据权利要求1所述的方法,其特征在于,所述第一、第二流表采用OpenFlow协议。

3.根据权利要求2所述的方法,其特征在于,所述第一、第二流表分别至少包括匹配域项、动作集合项,其中所述匹配域项用于对所述报文进行匹配,所述动作集合项包括用于控制所述数据交换机的动作的至少一个所述动作命令。

4.根据权利要求1所述的方法,其特征在于,所述第一北向接口由用户进行编程配置。

5.根据权利要求1至4中任一项所述的方法,其特征在于,其还包括:监控系统根据所述指定结点接收到的所述报文对网络流量进行监控管理。

6.一种网络流量监控管理系统,至少与第一、第二数据交换机分别耦合,所述系统包括:

上层应用控制单元,其通过SDN控制器的第一北向接口向所述SDN控制器发送镜像指令;

所述SDN控制器,其基于所述镜像指令以及所述第一数据交换机发来的第一流表而生成第二流表;其中,所述第一数据交换机发起报文的传输,所述第一流表封装所述报文,所述第二流表至少包括对应于所述镜像指令的动作命令,所述第二数据交换机从所述第二流表中提取所述报文,并基于所述动作命令而将所述报文镜像到指定结点;以及

监控管理单元,其根据所述指定结点接收到的所述报文对网络流量进行监控管理。

7.根据权利要求6所述的系统,其特征在于,其按照分布式系统来部署。

基于SDN的报文镜像方法及网络流量监控管理系统

技术领域

[0001] 本发明涉及网络流量监控技术领域，更具体地说，涉及一种基于SDN的报文镜像方法。

背景技术

[0002] 软件定义网络(Software Defined Network,简称SDN)，是网络一种新型网络创新架构，是网络虚拟化的一种实现方式，其核心是通过将网络设备控制面与数据面分离开来，实现了网络流量的灵活控制，使网络作为管道变得更加智能。

[0003] 端口镜像技术是通过配置交换机或路由器，将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”。端口镜像并不影响源端口和目的端口的报文交换，只是将所有进入和从源端口输出的报文原样复制了一份到目的端口，并且通过镜像端口对网络的流量进行监控分析。在企业内利用镜像功能，可以很好地对企业内部的网络数据进行监控管理，在网络出故障的时候，可以快速地定位故障。

[0004] 现有的端口镜像技术存在一些缺陷。一方面，现有技术往往通过人工操作的方式对交换机进行相关的参数配置，才能实现对端口或者报文的镜像。这种方式自动化程度较低，不能对镜像端口进行灵活控制，且容易出现误操作，增加了运维风险。

[0005] 另一方面，当前流量镜像是针对某一个端口来进行的，所有经过该端口的流量都会被镜像到监控系统中。但是这些流量中许多报文都是监控系统所不需要的，所以要对流量进行进一步的匹配、过滤后才能得到真正需要的报文数据。特别是在当前的云计算环境下，一个交换机端口会承载许多虚拟机的通讯流量，但是监控系统可能只是需要其中一台虚拟机甚至仅是一个应用所涉及的流量。如果将经过该端口的所有流量都镜像的话，不仅会增加网络的负担，影响网络的稳定性，而且对监控服务器的压力也非常大。

发明内容

[0006] 本发明的目的在于提供一种能够克服上述缺陷、并实现较细粒度流量监控的报文镜像方法。

[0007] 为实现上述目的，本发明提供一种技术方案如下：

[0008] 一种基于SDN的报文镜像方法，其中，SDN控制器与上层应用、及至少一个数据交换机分别耦合，方法包括如下步骤：a)、上层应用通过SDN控制器的第一北向接口向SDN控制器发送镜像指令；b)、SDN控制器基于镜像指令以及第一数据交换机发来的第一流表而生成第二流表；其中，第一数据交换机发起报文的传输，第一流表封装报文，第二流表至少包括对应于镜像指令的动作命令；以及c)、第二数据交换机从第二流表中提取报文，并基于动作命令而将报文镜像到指定结点。

[0009] 优选地，第一、第二流表采用OpenFlow协议。

[0010] 优选地，第一、第二流表分别至少包括匹配域项、动作集合项，其中匹配域项用于

对报文进行匹配，动作集合项包括用于控制数据交换机的动作的至少一个动作命令。

[0011] 优选地，第一北向接口由用户进行编程配置。

[0012] 本发明还提供一种网络流量监控管理系统，至少与第一、第二数据交换机分别耦合，该系统包括：上层应用控制单元，其通过SDN控制器的第一北向接口向SDN控制器发送镜像指令；SDN控制器，其基于镜像指令以及第一数据交换机发来的第一流表而生成第二流表；其中，第一数据交换机发起报文的传输，第一流表封装报文，第二流表至少包括对应于镜像指令的动作命令，第二数据交换机从第二流表中提取报文，并基于动作命令而将报文镜像到指定结点；以及监控管理单元，其根据指定结点接收到的报文对网络流量进行监控管理。

[0013] 本发明各实施例提供的报文镜像方法不需要对数据交换机进行人工配置，而由SDN控制器实现对数据交换机的控制；就网络流量监控来说，该方法能够聚焦于与特定端口、虚拟机甚至是特定应用相对应的报文，而将不需要监控的报文排除在外，从而可以实现较细粒度的流量监控，同时减轻了监控服务器的负载。该方式实施简单、便利，利于在行业内推广应用。

附图说明

[0014] 图1示出本发明第一实施例提供的基于SDN的报文镜像方法的流程图。

[0015] 图2示出本发明第二实施例提供的网络流量监控管理系统的模块结构示意图。

具体实施方式

[0016] 为便于说明，在本发明各实施例中，例示性地说明一个SDN控制器、以及第一、第二数据交换机，SDN控制器分别与第一、第二数据交换机在通信上耦合。但是，可以理解，根据特定的应用场合，本发明可以在包括多个SDN控制器以及更多的数据交换机的情况下实现，只要该多个SDN控制器以及该更多的数据交换机彼此耦合，并按照协定的协议来通信。

[0017] SDN北向接口是SDN控制器向上层业务应用开放的接口，其目标是使得业务应用能够便利地调用底层的网络资源和能力。通过北向接口，网络业务的开发者能以软件编程的形式调用各种网络资源。

[0018] SDN南向接口是SDN控制器向底层交换设备开放的接口，一方面通过上行通道对底层交换设备上报的信息进行监控和统计，另一方面SDN控制器也利用南向接口的下行通道对下游网络设备进行控制。

[0019] 如图1所示，本发明第一实施例提供一种基于SDN的报文镜像方法，其包括如下各步骤。

[0020] 步骤S10、上层应用通过SDN控制器的第一北向接口向SDN控制器发送镜像指令。

[0021] 具体地，SDN控制器为上层应用提供了封装好的北向接口，通过调用这些北向接口，上层应用可实现对网络资源的调用、分配以及释放等功能。对北向接口的调用则会影响SDN控制器通过南向接口协议对数据交换机下发相应的控制策略。

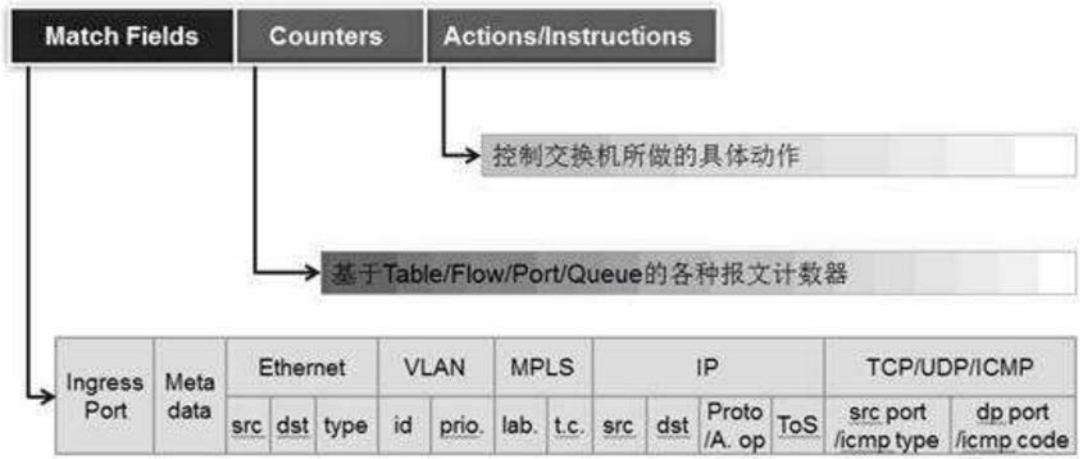
[0022] 根据该步骤S10，第一北向接口由用户进行编程配置。

[0023] 步骤S20、SDN控制器基于镜像指令以及第一数据交换机发来的第一流表而生成第二流表。

[0024] 其中，第一数据交换机发起报文的传输，第一流表封装报文，第二流表至少包括对应于镜像指令的动作命令。该动作命令指示接收到第二流表的交换机如何进行报文镜像，如下所述。

[0025] 根据优选实施方式，第一、第二流表采用OpenFlow协议。具体地，OpenFlow协议的报文结构(以下简称流表)如下表所示。

[0026]



[0027] Match Fields:匹配域，对数据包进行匹配，匹配完成后方才执行该流表中的动作；

[0028] Counters:计数器，在说明书中没有讨论；

[0029] Actions:动作集合，包括至少一个动作命令，以用于控制数据交换机的动作，如封装/去封装，多路径转发，输出到一个或几个端口等等。

[0030] 关于第二流表的生成，作为示例，在流表的动作集合中，可以在正常转发动作后面加入将数据输出到指定端口的命令:output。如将数据转发到端口1(连接应用的端口)和端口5(连接控制系统的端口)，即可加入动作命令:output 1 5;换言之，第二流表将包括对应于镜像指令的动作命令。

[0031] 步骤S30、第二数据交换机从第二流表中提取报文，并基于动作命令而将报文镜像到指定结点。

[0032] 继续上述示例，收到第二流表的数据交换机在解析第二流表之后，获得动作命令output 1 5，根据该命令第二数据交换机会将报文镜像到端口5。

[0033] 进一步地，监控系统根据指定结点接收到的各个报文来对网络流量进行监控管理。这种监控管理是以报文为单位来甄别进行的，而报文可对应于特定端口、虚拟机甚至是特定应用，将不需要监控的报文排除在外，本发明可以实现较细粒度的流量监控。

[0034] 如图2所示，本发明第二实施例提供一种网络流量监控管理系统，其至少包括上层应用控制单元101、SDN控制器102以及监控管理单元103。该网络流量监控管理系统通过SDN控制器102与第一、第二数据交换机201、202在通信上耦合。其中，第一数据交换机201发起报文的传输，第二数据交换机202期望获得报文，监控管理单元103期望获得报文镜像以对网络流量进行监控。

[0035] 具体地，上层应用控制单元101通过SDN控制器102的第一北向接口向SDN控制器102发送镜像指令。

[0036] SDN控制器102基于镜像指令以及第一数据交换机201发来的第一流表而生成第二

流表;第一流表封装有待传输的报文,第二流表至少包括对应于镜像指令的动作命令,

[0037] 收到第二流表后,第二数据交换机202从第二流表中提取报文,并基于动作命令而将报文镜像到指定结点。

[0038] 最后,监控管理单元103根据指定结点接收到的报文对网络流量进行监控管理。

[0039] 作为一种改进实施方式,SDN控制器102可向第一、第二数据交换机201、202下发控制策略,以指示数据交换机201、202执行除了镜像动作之外的其他动作。

[0040] 根据优选实施方式,该网络流量监控管理系统可以按照分布式系统来部署,例如,将上层应用控制单元、SDN控制器设置于本地端,而将监控管理单元设置于远程端。而第一、第二数据交换机201、202也可以设置于另一远程端。

[0041] 进一步地,该网络流量监控管理系统还可以按照云计算方式来部署。

[0042] 上述说明仅针对于本发明的优选实施例,并不在于限制本发明的保护范围。本领域技术人员可作出各种变形设计,而不脱离本发明的思想及附随的权利要求。

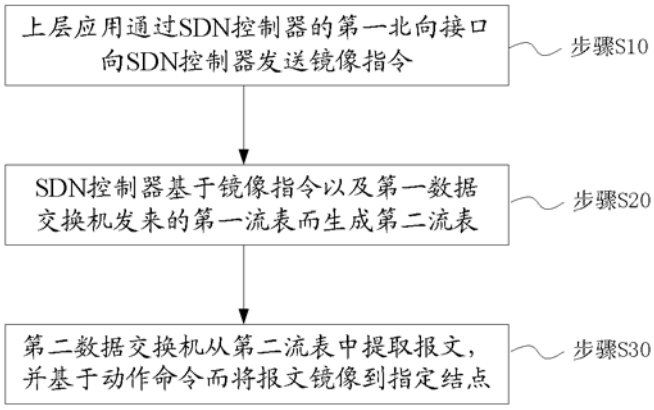

上层应用通过SDN控制器的第一北向接口
向SDN控制器发送镜像指令
步骤S10
SDN控制器基于镜像指令以及第一数据
交换机发来的第一流表而生成第二流表
步骤S20
第二数据交换机从第二流表中提取报文，
并基于动作命令而将报文镜像到指定结点
步骤S30

图 1

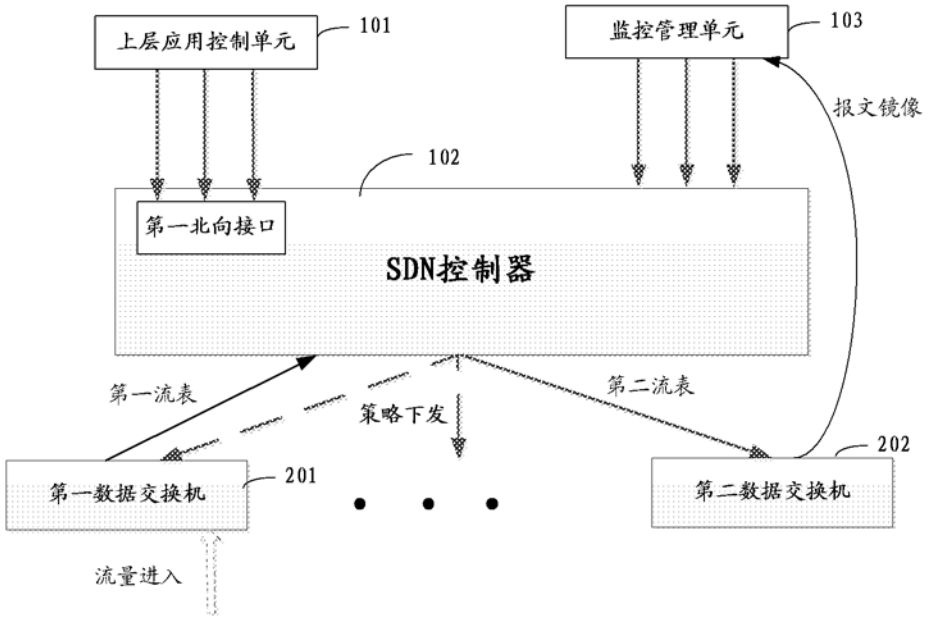

上层应用控制单元
101
监控管理单元
103
报文镜像
102
第一北向接口
SDN控制器
第一流表
策略下发
第二流表
202
第一数据交换机
201
第二数据交换机
流量进入

图 2