



(12) 发明专利

(10) 授权公告号 CN 111478853 B

(45) 授权公告日 2022.02.08

(21) 申请号 202010255143.2

H04L 9/40 (2022.01)

(22) 申请日 2020.04.02

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 107113229 A, 2017.08.29

申请公布号 CN 111478853 A

CN 109412952 A, 2019.03.01

CN 107078974 A, 2017.08.18

(43) 申请公布日 2020.07.31

US 2017237656 A1, 2017.08.17

(73) 专利权人 广州市品高软件股份有限公司

US 2013182710 A1, 2013.07.18

地址 510000 广东省广州市天河区软件路

WO 2018109550 A1, 2018.06.21

17号第G1栋

CN 108964940 A, 2018.12.07

(72) 发明人 刘忻 林冬艺 袁龙浩

Xiaoliang Zhao; ET ALL. Detection of invalid routing announcement in the Internet. 《Proceedings International Conference on Dependable Systems and Networks》. 2002,

(74) 专利代理机构 广州新诺专利商标事务有限公司 44100

张建宗; 秦华. IPv6路由通告攻击检测. 《网络安全技术与应用》. 2009,

代理人 张玲春

审查员 高焕泽

(51) Int. Cl.

H04L 45/00 (2022.01)

H04L 45/741 (2022.01)

H04L 45/745 (2022.01)

H04L 45/76 (2022.01)

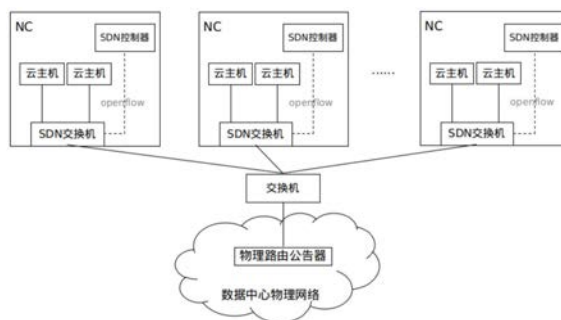
权利要求书2页 说明书5页 附图4页

(54) 发明名称

一种基于SDN的IPv6路由公告方法和系统

(57) 摘要

本发明涉及一种基于SDN的IPv6路由公告方法和系统。该基于SDN的IPv6路由公告方法包括：获取第一路由公告数据包；修改所述第一路由公告数据包的至少一字段信息以组装为第二路由公告数据包；将所述第二路由公告数据包通过SDN交换机转发至云主机。上述的基于SDN的IPv6路由公告方法和系统通过获取第一路由公告数据包，并修改第一路由公告数据包中的字段信息以形成第二路由公告数据包，实现了IPv6路由公告消息数据包的自定义封装，提供了更为全面的数据配置，融合了云VPC的组网逻辑，响应了云网络的自动构建。



1. 一种基于SDN的IPv6路由公告方法,其特征在于,包括以下步骤:

获取第一路由公告数据包;SDN控制器通过对所述第一路由公告数据包的子网信息进行索引,获取云网络的元数据,所述元数据包括SDN交换机的IP地址,Mac地址和无类别域间路由;

修改所述第一路由公告数据包的至少一字段信息以组装为第二路由公告数据包;

修改所述第一路由公告数据包的至少一字段信息包括步骤:

提取所述第一路由公告数据包的前缀信息选项的前缀的值;

如果所述前缀信息选项的前缀的值为0或者与所述无类别域间路由匹配,则将所述无类别域间路由填充为所述前缀信息选项的前缀,并且将前缀信息选项的标识的L标志设置为1,A标志设置为0;以及,

将所述第一路由公告数据包的链路层地址设置为网关的物理地址;

将所述第二路由公告数据包通过SDN交换机转发至云主机。

2. 如权利要求1所述的基于SDN的IPv6路由公告方法,其特征在于,

修改所述第一路由公告数据包的至少一字段信息还包括步骤:

修改所述第一路由公告数据包的MTU阈值,使得MTU阈值大于或等于1280个字节。

3. 如权利要求2所述的基于SDN的IPv6路由公告方法,其特征在于,在获取第一路由公告数据包之后,修改所述第一路由公告数据包的至少一字段信息之前,还包括:

提取所述第一路由公告数据包的信息并结合网络的组网逻辑,对所述第一路由公告数据包进行合法性检查;

如果确定该第一路由公告数据包合法,则修改所述第一路由公告数据包的至少一字段信息,否则丢弃该第一路由公告数据包。

4. 如权利要求3所述的基于SDN的IPv6路由公告方法,其特征在于,获取第一路由公告数据包包括步骤:

数据中心IPv6路由公告服务器发出路由公告消息;

SDN交换机接收该路由公告数据包,按照流表规则进行匹配,生成与该公告数据包对应的首包;

SDN控制器截取所述首包,提取所述首包的目标端口进行比对,确认该首包为路由公告消息是将该首包作为所述第一路由公告数据包。

5. 如权利要求1所述的基于SDN的IPv6路由公告方法,其特征在于,获取第一路由公告数据包包括:

SDN控制器按照IPv6路由公告报文格式封装数据包,设置数据包的目标IP地址为多播地址224.0.0.1,目标Mac地址为33:33:00:00:00:01作为所述第一路由公告数据包。

6. 如权利要求5所述的基于SDN的IPv6路由公告方法,其特征在于,修改所述第一路由数据包的至少一字段信息以形成第二路由公告数据包包括:

SDN控制器的获取SDN交换机所连接的云主机的网卡信息,结合元数据获取所述云主机所在子网的信息;

通过对所述子网的信息进行索引,结合云VPC组网逻辑,获取云网络元数据,其中,所述云网络元数据包括网关IP地址,物理地址和无类别域间路由;

所述SDN控制器将所述无类别域间路由填充为所述第一路由数据包的前缀信息选项的

前缀,并且将前缀信息选项的标识的L标志设置为1,A标志设置为0;以及,
将所述第一路由公告数据包的链路层地址设置为网关的物理地址。

7.如权利要求1所述的基于SDN的IPv6路由公告方法,其特征在于,组装为第二路由公告数据包包括:

根据数据包封装逻辑对修改数据后的第一路由数据包组装出所述第二路由公告数据包。

8.一种基于SDN的IPv6路由公告系统,其特征在于,包括计算节点,所述计算节点包括云主机、SDN交换机和SDN控制器,所述云主机连接于所述SDN交换机,所述SDN控制器连接于所述SDN交换机,所述SDN交换机连接于外网,其中,所述SDN控制器通过如权利要求1-7任一项所述的IPv6路由公告方法进行路由公告。

一种基于SDN的IPv6路由公告方法和系统

技术领域

[0001] 本发明属于数据通信技术领域,具体涉及一种基于SDN的IPv6路由公告方法和系统。

背景技术

[0002] 在IPv4网络中,基于路由器发现技术,使得主机可以通过定位路由器并学习与本地网络操作有关的重要参数。而在IPv6网络中,则是通过路由器定期多播路由器公告消息,以宣布其可用性并将信息传递给相邻节点,从而使主机能够在网络上自动配置。

[0003] 现有的数据中心普遍采用部署一台物理路由公告器来实现相关的服务,这种方式至少存在着以下问题:

[0004] 1) 传统数据中心的单点故障问题,容灾能力不足;

[0005] 2) 考虑路由公告本身的安全,需要相关配置,操作繁琐;

[0006] 3) 现有数据中心路由公告器和云平台路由公告服务融合,配置和对接繁琐,灵活性低,改造成本高。

发明内容

[0007] 本发明的目的是提供一种基于SDN的IPv6路由公告方法和系统,提供了更为全面的数据配置,响应了云网络的自动构建。

[0008] 为此,本发明提供了一种基于SDN的IPv6路由公告方法,包括以下步骤:

[0009] 获取第一路由公告数据包;

[0010] 修改所述第一路由数据包的至少一字段信息以组装为第二路由公告数据包;

[0011] 将所述第二路由公告数据包通过SDN交换机转发至云主机。

[0012] 优选地,在获取所述第一路由公告数据包之前,还包括:SDN控制器通过对所述第一路由公告数据包的子网信息进行索引,获取云网络的元数据,所述元数据包括所述SDN交换机的IP地址,Mac地址和无类别域间路由。

[0013] 优选地,修改所述第一路由数据包的至少一字段信息包括步骤:

[0014] 提取所述第一路由数据包的前缀信息选项的前缀的值;

[0015] 如果所述前缀信息选项的前缀的值为0或者与所述无类别域间路由匹配,则将所述无类别域间路由填充为所述前缀信息选项的前缀,并且将前缀信息选项的标识的L标志设置为1,A标志设置为0;以及,

[0016] 将所述第一路由公告数据包的链路层地址设置为网关的物理地址。

[0017] 优选地,修改所述第一路由数据包的至少一字段信息还包括步骤:

[0018] 修改所述第一路由数据包的MTU阈值,使得MTU阈值大于或等于1280个字节。

[0019] 优选地,在获取第一路由公告数据包之后,修改所述第一路由数据包的至少一字段信息之前,还包括:

[0020] 提取所述第一路由公告数据包的信息并结合网络的组网逻辑,对所述第一路由公

告数据包进行合法性检查；

[0021] 如果确定该第一路由公告数据包合法，则修改所述第一路由数据包的至少一字段信息，否则丢弃该第一路由公告数据包。

[0022] 优选地，获取第一路由公告数据包包括：

[0023] 数据中心IPv6路由公告服务器发出路由公告消息；

[0024] SDN交换机接收该路由公告数据包，按照流表规则进行匹配，生成与该公告数据包对应的首包；

[0025] SDN控制器截取所述首包，提取所述首包的目标端口进行比对，确认该首包为路由公告消息是将该首包作为所述第一路由数据包。

[0026] 优选地，获取第一路由公告数据包包括：

[0027] SDN控制器按照IPv6路由公告报文格式封装数据包，设置数据包的目标IP地址为多播地址224.0.0.1，目标Mac地址为33:33:00:00:00:01作为所述第一路由公告数据包。

[0028] 优选地，修改所述第一路由数据包的至少一字段信息以形成第二路由公告数据包包括：

[0029] SDN控制器的获取SDN交换机所连接的云主机的网卡信息，结合元数据获取所述云主机所在子网的信息；

[0030] 通过对所述子网的信息进行索引，结合云VPC组网逻辑，获取云网络元数据，其中，所述云网络元数据包括网关IP地址，物理地址和无类别域间路由；

[0031] 所述SDN控制器将所述无类别域间路由填充为所述第一路由数据包的前缀信息选项的前缀，并且将前缀信息选项的标识的L标志设置为1，A标志设置为0；以及，

[0032] 将所述第一路由公告数据包的链路层地址设置为网关的物理地址。

[0033] 优选地，组装为第二路由公告数据包包括：

[0034] 根据数据包封装逻辑对修改数据后的第一路由数据包组装出所述第二路由公告数据包。

[0035] 一种基于SDN的IPv6路由公告系统，包括计算节点，所述计算节点包括云主机、SDN交换机和SDN控制器，所述云主机连接于所述SDN交换机，所述SDN控制器连接于所述SDN交换机，所述SDN交换机连接于外网，其中，所述SDN控制器通过上述的IPv6路由公告方法进行路由公告。

[0036] 相较于现有技术，上述的基于SDN的IPv6路由公告方法和系统通过获取第一路由公告数据包，并修改第一路由公告数据包中的字段信息以形成第二路由公告数据包，实现了IPv6路由公告消息数据包的自定义封装，提供了更为全面的数据配置，融合了云VPC的组网逻辑，响应了云网络的自动构建。

[0037] 进一步，上述的基于SDN的IPv6路由公告方法和系统还通过获取IPv6路由公告消息，即第一路由公告数据包的方式，通过比对第一路由公告数据包的字段信息过滤非法、恶意、重复的路由公告消息，有效管控了VPC内的路由公告消息，解决了内网非法路由公告消息导致的主机无法正常获取IP地址，持续发出请求的问题，也有效遏制了外部借助路由公告消息进行的恶意和高频繁攻击，提高了网络的安全性和稳定性。

[0038] 而且，基于SDN控制器对网络进行优化，可以提供了IPv6路由公告的代理模式和接管模式，根据数据中心的物理路由公告器的实际部署情况按需配置，接入灵活，零配置，解

决了传统路由公告器配置繁琐的问题。基于SDN控制器的分布式场景,实现了IPv6路由公告服务的分布式架构,解决了IPv6路由公告服务的单点问题,同时也摆脱了物理线路中断对IPv6路由公告服务带来的影响。

附图说明

- [0039] 图1是基于SDN的IPv6路由公告系统在代理模式下的结构示意图。
- [0040] 图2是基于SDN的IPv6路由公告方法在代理模式下的流程图。
- [0041] 图3是基于SDN的IPv6路由公告系统在接管模式下的结构示意图。
- [0042] 图4是基于SDN的IPv6路由公告方法在接管模式下的流程图。

具体实施方式

- [0043] 下面结合具体较佳实施例结合附图,对本发明做进一步的详细说明。
- [0044] 图1是基于SDN的IPv6路由公告系统在代理模式下的结构示意图。如图1所示,基于SDN的IPv6路由公告系统在代理模式下部署在每个计算节点。每个计算节点部署一个SDN交换机、SDN控制器。云主机连接到SDN交换机,SDN交换机通过计算节点的上行接口连接外网,SDN控制器连接于SDN交换机。
- [0045] 此外,数据中心物理网络部署了一台物理路由公告器,用于数据中心物理网络的统一路由公告。计算节点的云平台虚拟网络(NC)根据业务不同通过代理方式,与现有数据中心物理网络的Ipv6路由公告服务对接,实现云平台虚拟化的路由公告。
- [0046] 图2是基于SDN的IPv6路由公告方法在代理模式下的流程图,如图2所示,该基于SDN的IPv6路由公告方法在代理模式下包括步骤S201~S208。
- [0047] 步骤S201:数据中心物理网络的IPv6物理路由公告器定期发出IPv6路由公告消息。
- [0048] 步骤S202:SDN交换机接收路由公告消息数据包,按照流表规则进行匹配,生成相应的首包。
- [0049] 步骤S203:SDN控制器的数据包接收单元截取首包,提取目标端口通过比对,确认数据包为路由公告消息,将数据包作为第一路由公告数据包传递给SDN控制器的解析单元,完成获得所述第一路由公告数据包的步骤。
- [0050] 步骤S204:SDN控制器的解析单元解析获取的第一路由公告数据包中的路由公告数据,提取IPv6路由公告数据包的信息,结合云VPC组网逻辑,由拦截过滤模块的过滤集对数据包进行合法性检查,将不满足条件的数据包标记成非法,并下发丢弃的流表。
- [0051] 步骤S205:SDN控制器的解析单元通过第一路由公告数据包的子网信息进行索引,结合云VPC组网逻辑,获取云网络元数据,包括网关IP地址,物理地址(即Mac地址)和无类别域间路由(Classless Inter-Domain Routing,CIDR)。
- [0052] 步骤S206:SDN控制器的解析单元修改所述第一路由数据包的至少一字段信息,其中,字段信息包括字段信息本身以及该字段信息的内容,本实施方式中,修改的字段信息包括:
 - [0053] 1) SDN控制器的封装单元在前缀信息选项(Prefix Information Option)部分提取前缀(Prefix)的值,判断是否为0或者与上述获取的CIDR进行匹配。如果为0或者不匹配,

则对数据包进行丢弃。对于合法项,则根据IPv6路由公告报文格式,将前缀信息选项的前缀(Prefix)设置为上述的CIDR。然后,修改前缀的前缀标志(Prefix Flag)的L标志为1,A标志为0,从而可以确定云主机的IP地址不变更,避免对业务造成中断。

[0054] 2) 设置源链接层地址选项(Source Link-Layer Address Option)的默认类型和长度,将链路层地址(Link-Layer Address)设置为网关的物理地址(Mac地址)。

[0055] 3) 修改路由公告消息的MTU阈值,组装MTU option部分,使得MTU大于或者等于1280个字节,对不满足条件的数据包进行丢弃。

[0056] 步骤S207:组合上述部分实现对IPv6路由公告Options的自定义封装,最后根据数据包封装逻辑,组装出新的IPv6路由公告数据包,即第二路由公告数据包,然后,SDN控制器将第二路由公告数据包发给SDN交换机。

[0057] 步骤S208:SDN交换机根据流表逻辑将第二路由公告数据包发送给云主机,完成路由公告功能。

[0058] 图3是基于SDN的IPv6路由公告系统在接管模式下的结构示意图。如图3所示,基于SDN的IPv6路由公告系统在代理模式下部署在每个计算节点。每个计算节点部署一个SDN交换机、SDN控制器。云主机连接到SDN交换机,SDN交换机通过计算节点的上行接口连接外网,SDN控制器连接于SDN交换机。计算节点(NC)根据业务不同通过管控的方式,与现有数据中心物理网络的Ipv6路由公告服务对接,实现云平台虚拟化的路由公告。

[0059] 图4是基于SDN的IPv6路由公告方法在接管模式下的流程图。如图4所示,基于SDN的IPv6路由公告方法在接管模式下包括步骤S401~S406。

[0060] 步骤S401:SDN控制器构建第一路由公告数据包,完成获得所述第一路由公告数据包的步骤。具体而言,SDN控制器开启路由公告定时任务,SDN控制器的封装单元根据IPv6路由公告报文格式封装数据包,设置数据包的目标IP地址为多播地址224.0.0.1,目标Mac地址为33:33:00:00:00:01,形成第一路由公告数据包。

[0061] 步骤S402:SDN控制器的封装单元获取SDN交换机所连接的云主机的网卡信息,结合元数据获取其所在子网的信息。

[0062] 步骤S403:通过子网的信息进行索引,结合云VPC组网逻辑,获取云网络元数据,包括网关IP地址,Mac地址和CIDR。

[0063] 步骤S404:SDN控制器的封装单元结合元数据和VPC组网逻辑修改所述第一路由数据包的至少一字段信息,其中,字段信息包括字段信息本身以及该字段信息的内容。本实施方式中,修改的字段信息包括:

[0064] 1) 将前缀信息选项(Prefix)设置为CIDR,设修改前缀的前缀标志(Prefix Flag)的L标志为1,A标志为0,从而可以确定云主机的IP地址不变更,避免对业务造成中断,完成前缀信息选项(Prefix Information Option)的组装;

[0065] 2) 设置源链接层地址选项(Source Link-Layer Address Option)的默认类型和长度,将链路层地址(Link-Layer Address)设置为网关的物理地址(Mac地址)。

[0066] 3) 修改路由公告消息的MTU阈值,组装MTU option部分,使得MTU大于或者等于1280个字节。

[0067] 步骤S405:组合上述部分,实现对IPv6路由公告Options的自定义封装,最后根据数据包封装逻辑,组装出新的IPv6路由公告数据包,即第二路由公告数据包,发给SDN交换

机。

[0068] 步骤S406:SDN交换机根据流表逻辑将第二路由公告数据包发送给云主机,完成路由公告功能。

[0069] 上述的基于SDN的IPv6路由公告方法和系统通过获取第一路由公告数据包,即在代理模式下接收路由公告数据包以获取该第一路由公告数据包,在接管模式下基于云网络元数据和云VPC的组网逻辑构建路由公告数据包作为该第一路由公告数据包。然后,修改第一路由公告数据包中的字段信息以形成第二路由公告数据包,实现了IPv6路由公告消息数据包的自定义封装,提供了更为全面的数据配置,融合了云VPC的组网逻辑,响应了云网络的自动构建。

[0070] 进一步,上述的基于SDN的IPv6路由公告方法和系统还通过获取IPv6路由公告消息,,即第一路由公告数据包的方式,通过比对第一路由公告数据包的字段信息过滤非法、恶意、重复的路由公告消息,有效管控了VPC内的路由公告消息,解决了内网非法路由公告消息导致的主机无法正常获取IP地址,持续发出请求的问题,也有效遏制了外部借助路由公告消息进行的恶意和高频繁攻击,提高了网络的安全性和稳定性。

[0071] 而且,基于SDN控制器对网络进行优化,可以提供了IPv6路由公告的代理模式和接管模式,根据数据中心的物理路由公告器的实际部署情况按需配置,接入灵活,零配置,解决了传统路由公告器配置繁琐的问题。基于SDN控制器的分布式场景,实现了IPv6路由公告服务的分布式架构,解决了IPv6路由公告服务的单点问题,同时也摆脱了物理线路中断对IPv6路由公告服务带来的影响。

[0072] 应该理解,本发明并不局限于上述实施方式,凡是对本发明的各种改动或变型不脱离本发明的精神和范围,倘若这些改动和变型属于本发明的权利要求和等同技术范围之内,则本发明也意味着包含这些改动和变型。

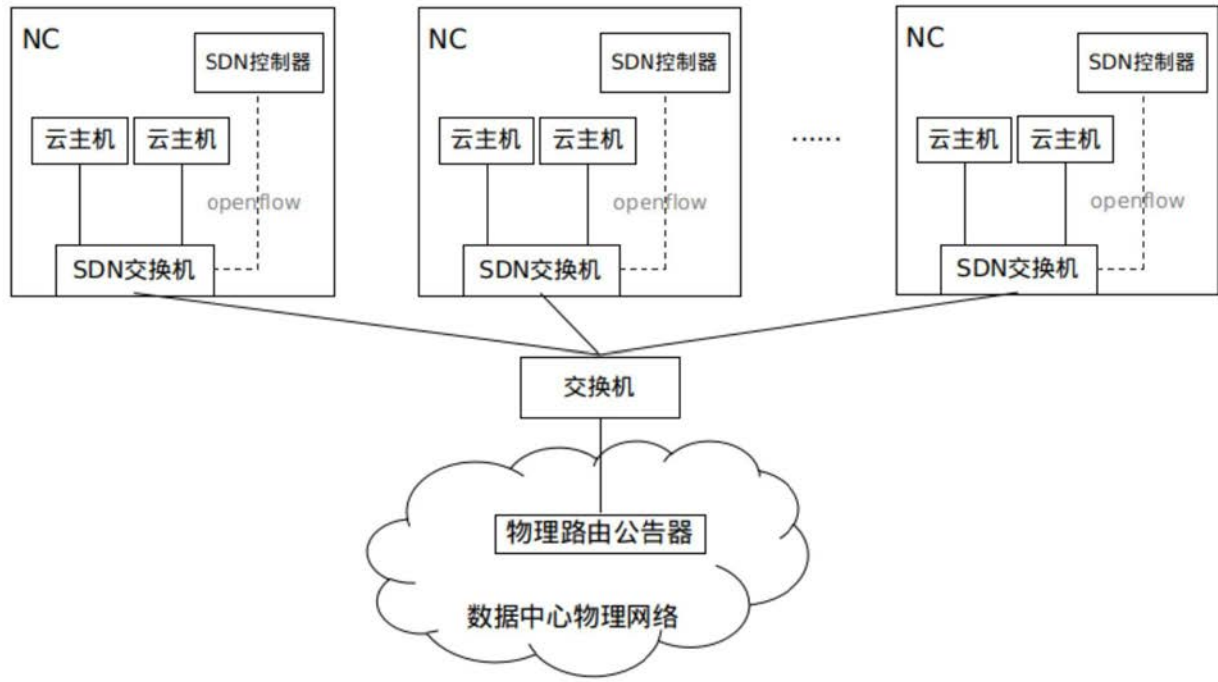


图1

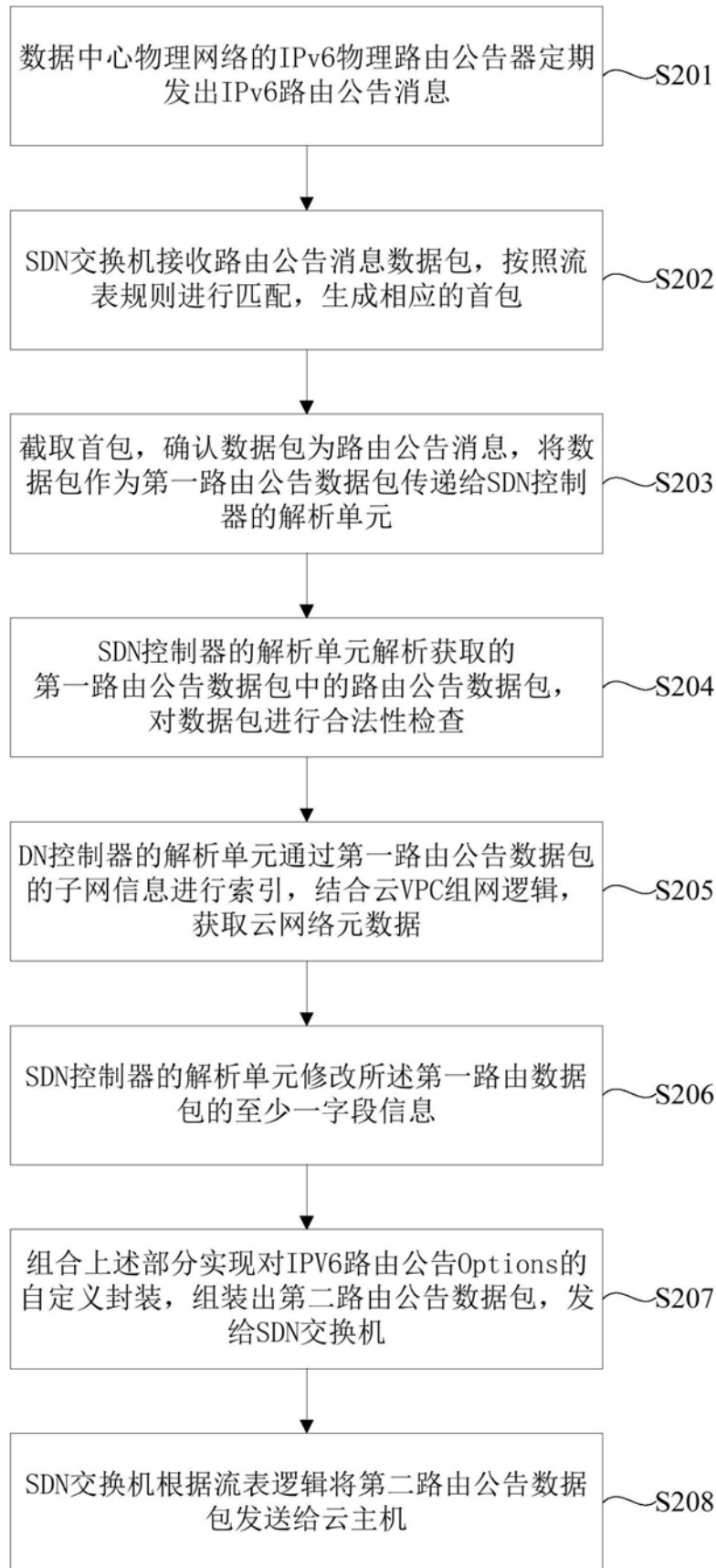


图2

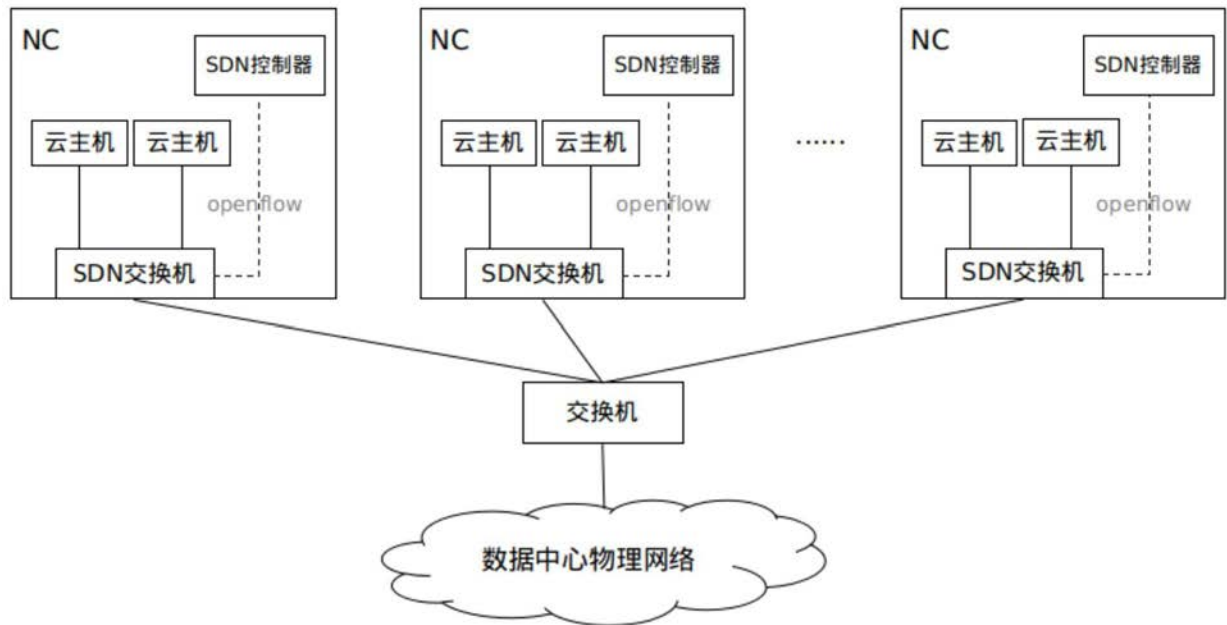


图3

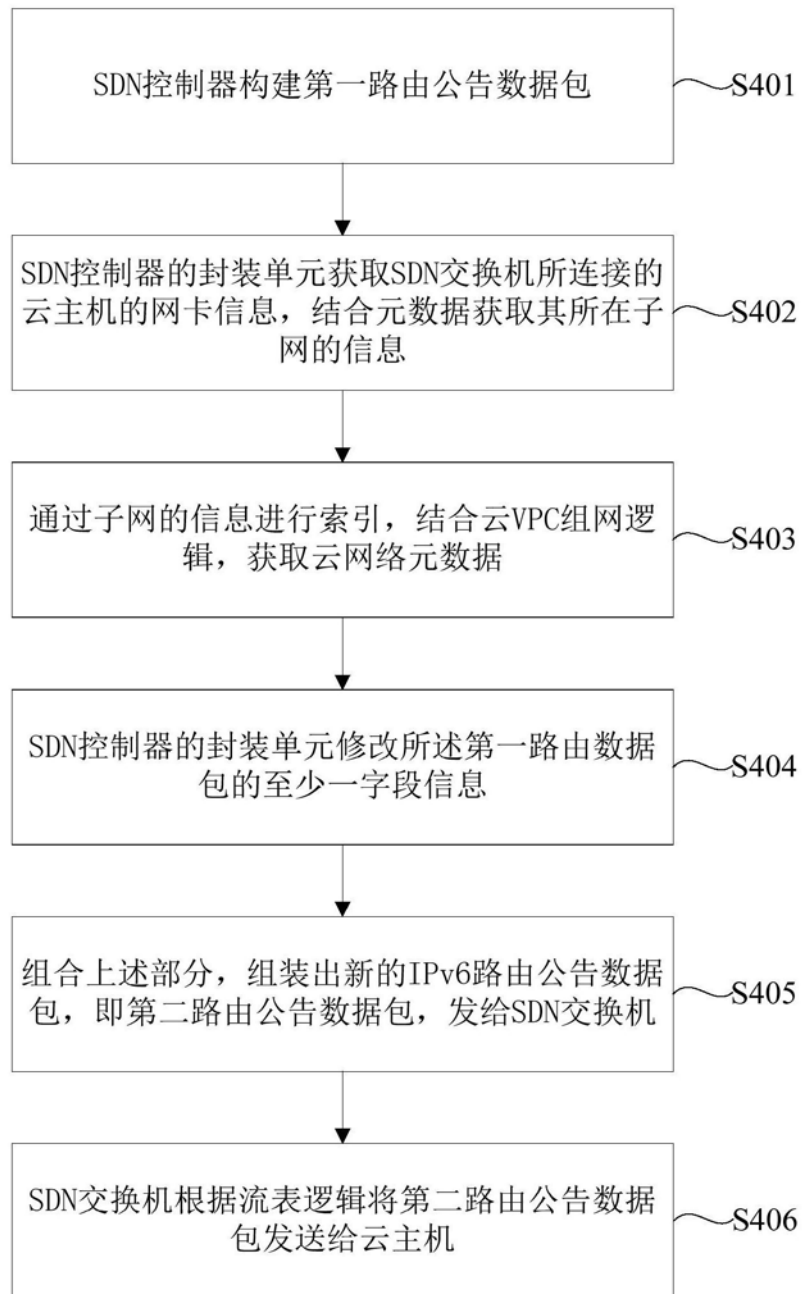


图4