(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 109327416 B
(45)授权公告日 2021.07.23

(21)申请号 201710642607.3
(22)申请日 2017.07.31
(65)同一申请的已公布的文献号
申请公布号 CN 109327416 A
(43)申请公布日 2019.02.12
(73)专利权人 北京亿阳信通科技有限公司
地址 100093 北京市海淀区杏石口路99号1幢20302
(72)发明人 陈明德 张东 李宁 江峰
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
(56)对比文件
CN 106789667 A,2017.05.31
CN 104813617 A,2015.07.29
CN 105933235 A,2016.09.07
CN 104871483 A,2015.08.26
US 2016352682 A1,2016.12.01
US 2016105393 A1,2016.04.14
吴霜等.私有云跨域互连解决方案.《数据通信》.2015,全文.
审查员 文华胤

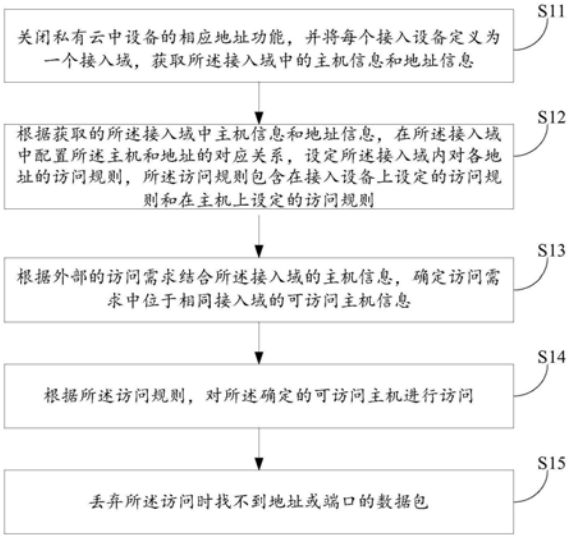
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种SDN网络中私有云的访问控制方法和装置

(57)摘要

本发明实施例公开了一种SDN网络中私有云的访问控制方法,所述方法包括:关闭私有云中设备的相应地址功能,并将每个接入设备定义为一个接入域,获取所述接入域中的主机信息和地址信息;根据获取的所述接入域中主机信息和地址信息,在所述接入域中配置所述主机和地址的对应关系,设定所述接入域内对各地址的访问规则,所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则;根据外部的访问需求结合所述接入域的主机信息,确定访问需求中位于相同接入域的可访问主机信息;根据所述访问规则,对所述确定的可访问主机进行访问。本发明实施例还公开一种SDN网络中私有云的访问控制装置。



CN 109327416 B

1.一种SDN网络中私有云的访问控制方法,其特征在于,所述方法包括:

关闭私有云中设备的相应地址功能,并将每个接入设备定义为一个接入域,获取所述接入域中的主机信息和地址信息;所述相应地址功能具体为地址解析协议和反向地址解析协议;

根据获取的所述接入域中主机信息和地址信息,在所述接入域中配置所述主机和地址的对应关系,设定所述接入域内对各地址的访问规则,所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则;

根据外部的访问需求结合所述接入域的主机信息,确定访问需求中位于相同接入域的可访问主机信息;

根据所述访问规则,对所述确定的可访问主机进行访问;

所述在所述接入域中配置所述主机和地址的对应关系具体为:

根据所述在所述接入域中的接入设备上,配置连接在接入设备的主机地址和MAC地址的对应关系;

在所述接入域中的主机上,配置该主机可访问主机地址与所述该主机的MAC地址的对应关系。

2.根据权利要求1所述的方法,其特征在于,所述在接入设备上设定的访问规则具体为:

在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对;

将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口MAC地址,转发至各自对应的端口。

3.根据权利要求1所述的方法,其特征在于,所述在主机上设定的访问规则具体为:

在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC地址进行配对;

在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

4.根据权利要求1-3中任一所述的方法,其特征在于,所述方法还包括:

丢弃所述访问时找不到地址或端口的数据包。

5.一种SDN网络中私有云的访问控制装置,其特征在于,所述装置包括:

信息获取单元,用于关闭私有云中设备的相应地址功能,并将每个接入设备定义为一个接入域,获取所述接入域中的主机信息和地址信息;所述相应地址功能具体为地址解析协议和反向地址解析协议;

访问规则设定单元,用于根据所述信息获取单元获取的信息,在所述接入域中配置所述主机和地址的对应关系,设定所述接入域内对各地址的访问规则,所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则;

可访问主机确定单元,根据外部的访问需求结合所述信息获取单元获取的接入域主机信息,确定访问需求中位于相同接入域的可访问主机信息;

访问控制单元,根据所述访问规则设定单元设定的访问规则,对所述可访问主机确定单元中确定的可访问主机进行访问;

所述访问规则设定单元进一步包括:

地址关系配置模块，用于根据所述信息获取单元获取的接入域中的主机信息和地址信息，在所述接入域中的接入设备上，配置连接在接入设备的主机地址和MAC地址的对应关系；在所述接入域中的主机上，配置该主机可访问主机地址与所述该主机的MAC地址的对应关系；

访问规则设定模块，用于在接入设备上设定访问规则和在主机上设定访问规则。

6.根据权利要求5所述的装置，其特征在于，所述访问规则设定模块在接入设备上设定的访问规则具体为：

在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对；

将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口MAC地址，转发至各自对应的端口。

7.根据权利要求5所述的装置，其特征在于，所述访问规则设定模块在主机上设定的访问规则具体为：

在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC地址进行配对；

在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

8.根据权利要求5-7中任一所述的装置，其特征在于：

所述访问控制单元，丢弃所述访问时找不到地址或端口的数据包。

一种SDN网络中私有云的访问控制方法和装置

技术领域

[0001] 本发明涉及计算机软件,更具体地说,涉及一种私有云主机访问控制技术。

背景技术

[0002] 私有云,私有云(Private Clouds)是为一个公司单独使用而构建的,因而提供对数据、安全性和服务质量的最有效控制。该公司拥有基础设施,并可以控制在此基础设施上部署应用程序的方式。

[0003] 伴随着云计算技术的发展,越来越多的公司应用了私有云平台。但是如何对私有云平台中,特别是跨多个IDC机房的私有云平台中主机相互访问进行管理控制尚未得到有效解决。目前已有的方案都是改造虚拟机发出数据包,在数据包上附加上扩展VLAN的信息,将私有云平台切分成多个子网。但是这种方案需要在主机上增加处理数据包的模块,同时也没有解决跨子网间主机访问问题。

[0004] 因此私有云各子网主机间的访问控制问题亟待解决。

发明内容

[0005] 本发明提供了如下技术方案一种SDN网络中私有云的访问控制方法,包括:

[0006] 关闭私有云中设备的相应地址功能,并将每个接入设备定义为一个接入域,获取所述接入域中的主机信息和地址信息;

[0007] 根据获取的所述接入域中主机信息和地址信息,在所述接入域中配置所述主机和地址的对应关系,设定所述接入域内对各地址的访问规则,所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则;

[0008] 根据外部的访问需求结合所述接入域的主机信息,确定访问需求中位于相同接入域的可访问主机信息;

[0009] 根据所述访问规则,对所述确定的可访问主机进行访问。

[0010] 所述方法还包括:

[0011] 丢弃所述访问时找不到地址或端口的数据包。

[0012] 所述在所述接入域中配置所述主机和地址的对应关系具体为:

[0013] 根据所述在所述接入域中的接入设备上,配置连接在接入设备的主机地址和MAC地址的对应关系;

[0014] 在所述接入域中的主机上,配置该主机可访问主机地址与所述该主机的 MAC地址的对应关系。

[0015] 所述在接入设备上设定的访问规则具体为:

[0016] 在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对;

[0017] 将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口 MAC地址,转发至各自对应的端口。

[0018] 所述在主机上设定的访问规则具体为:

[0019] 在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC 地址进行配对；

[0020] 在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

[0021] 本发明还公开一种SDN网络中私有云的访问控制装置，其特征在于，所述装置包括：

[0022] 信息获取单元，用于关闭私有云中设备的相应地址功能，并将每个接入设备定义为一个接入域，获取所述接入域中的主机信息和地址信息；

[0023] 访问规则设定单元，用于根据所述信息获取单元获取的信息，在所述接入域中配置所述主机和地址的对应关系，设定所述接入域内对各地址的访问规则，所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则；

[0024] 可访问主机确定单元，根据外部的访问需求结合所述信息获取单元获取的接入域主机信息，确定访问需求中位于相同接入域的可访问主机信息；

[0025] 访问控制单元，根据所述访问规则设定单元设定的访问规则，对所述可访问主机确定单元中确定的可访问主机进行访问。

[0026] 所述访问控制单元，丢弃所述访问时找不到地址或端口的数据包。

[0027] 优选的，所述访问规则设定单元进一步包括：

[0028] 地址关系配置模块，用于根据所述信息获取单元获取的接入域中的主机信息和地址信息，在所述接入域中的接入设备上，配置连接在接入设备的主机地址和MAC地址的对应关系；在所述接入域中的主机上，配置该主机可访问主机地址与所述该主机的MAC地址的对应关系；

[0029] 访问规则设定模块，用于在接入设备上设定访问规则和在主机上设定访问规则。

[0030] 优选的，所述访问规则设定模块在接入设备上设定的访问规则具体为：

[0031] 在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对；

[0032] 将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口 MAC地址，转发至各自对应的端口。

[0033] 所述访问规则设定模块在主机上设定的访问规则具体为：

[0034] 在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC 地址进行配对；

[0035] 在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

[0036] 通过以上方案可知，本发明首先在主机和接入交换机上禁用了ARP和 RARP功能的同时，通过在静态IP地址与MAC地址的配对，结合交换机和主机上配置访问规则，实现了私有云跨域主机间的访问控制，使得不需要在主机上增加处理数据包模块的情况下解决跨子网间主机访问问题。

附图说明

[0037] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或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

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。

[0038] 图1为本申请实施例提供的一种SDN网络中私有云的访问控制方法流程图;

[0039] 图2为本申请实施例二提供的方法流程图;

[0040] 图3为本申请实施例三提供的云平台示意;

[0041] 图4为本申请实施例四一种SDN网络中私有云的访问控制装置结构示意图。

[0042] 图5为本申请实施例五提供的装置结构示意图。

具体实施方式

[0043] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有付出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0044] 请参阅图1,图1为本申请实施例提供的一种SDN网络中私有云的访问控制方法实现流程图,可以包括:

[0045] 步骤S11:关闭私有云中设备的相应地址功能,并将每个接入设备定义为一个接入域,获取所述接入域中的主机信息和地址信息。

[0046] 私有云,私有云(Private Clouds)是为一个公司单独使用而构建的,因而提供对数据、安全性和服务质量的最有效控制。该公司拥有基础设施,并可以控制在此基础设施上部署应用程序的方式。

[0047] 相应地址功能是指地址解析协议和反向地址转换协议。地址解析协议,即 ARP(Address Resolution Protocol),是根据IP地址获取物理地址的一个TCP/IP 协议。主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机,并接收返回消息,以此确定目标的物理地址;收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间,下次请求时直接查询ARP缓存以节约资源。

[0048] 反向地址转换协议(RARP:Reverse Address Resolution Protocol)反向地址转换协议(RARP)允许局域网的物理机器从网关服务器的ARP表或者缓存上请求其IP地址。网络管理员在局域网网关路由器里创建一个表以映射物理地址(MAC)和与其对应的IP地址。

[0049] 所述接入设备一般是指具有交换功能的交换机等,一个交换机上会连接多个主机,将一个交换机定义为一个接入域,可获知接入该交换机的主机信息和地址信息,其中地址信息可以是IP地址信息和MAC地址信息。

[0050] 步骤S12:根据获取的所述接入域中主机信息和地址信息,在所述接入域中配置所述主机和地址的对应关系,设定所述接入域内对各地址的访问规则,所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则。

[0051] 获取接入域中的主机信息和地址信息,包括接入域标识、接入域交换机标识、接入网络端口标识、接入网络端口MAC、接入域中的主机标识、主机IP 地址、主机MAC地址等。

[0052] 在接入域中配置所述主机和地址的对应关系,分两个部分进行操作,一是在接入设备即交换机上进行配置,在地址表中将连接在接入交换机的主机IP地址和MAC地址进行配对;二是在接入域中的主机上进行配置,即将一个接入域的可访问主机IP地址与该主机

的MAC地址进行配对，或将不在同一个接入域的可访问主机IP地址与该接入域接入交换机的接入网络端口MAC进行配对。

[0053] 访问规则也是，分别在接入设备上设定访问规则，在主机上设定访问规则。设定访问规则方法可以是在接入设备和主机上进行配置。

[0054] 步骤S13：根据外部的访问需求结合所述接入域的主机信息，确定访问需求中位于相同接入域的可访问主机信息。

[0055] 外部访问需求，会提供主机标识，可访问主机标识，根据这些可访问主机标识，结合上面步骤中接入域的主机信息，可获知可访问的主机是不是在相同的接入域中，进而明确在相同接入域的可访问主机信息。

[0056] 步骤S14：根据所述访问规则，对所述确定的可访问主机进行访问。

[0057] 优选的，为了解决找不到相应访问地址的问题，本发明还包括：

[0058] 步骤S15：丢弃所述访问时找不到地址或端口的数据包。

[0059] 丢弃找不到MAC地址和转发端口的数据包，这样实现了业务人员在使用主机时，与非许可的主机通信时，主机直接将数据包丢弃，同时还可以正常的与被许可的主机进行通信。

[0060] 本发明实施例中，先关闭了SDN网络中的相应地址功能，通过主机静态IP 和MAC地址的对应关系，以及设定访问规则，实现私有云跨主机间访问控制，并没有在主机上增加处理数据包的模块，节省了成本和开发周期。

[0061] 为了进一步的描述如何设置访问规则，给出本发明的实施例二，如图2所示。

[0062] 步骤S21：根据所述在所述接入域中的接入设备上，配置连接在接入设备的主机地址和MAC地址的对应关系。

[0063] 步骤S22：在所述接入域中的主机上，配置该主机可访问主机地址与所述该主机的MAC地址的对应关系。

[0064] 步骤S23：所述在接入设备上设定的访问规则

[0065] 步骤S231：在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对。

[0066] 步骤S232：将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口MAC地址，转发至各自对应的端口。

[0067] 步骤S24：在主机上设定的访问规则。

[0068] 步骤S241：在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC地址进行配对。

[0069] 步骤S242：在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

[0070] 为了更好的说明本发明的SDN网络中私有云的访问控制方法步骤，下面结合实例给出本发明的实施例三，某私有云平台示例如图3所示。

[0071] 接入交换机1、接入交换机2可以在一个IDC机房也可以在多个IDC机房。1)接入交换机1、接入交换机2、主机1、主机2、主机3、主机4、主机5取消ARP、RARP功能，完全由静态配置IP地址与MAC地址匹配规则、数据报转发规则。

[0072] 2)私有云中每个接入交换机都定义为一个接入域。

[0073] 已知私有云的接入交换机接入网络的端口及其MAC地址，连接主机的交换机端口。各主机的IP地址与MAC地址，如表1、表2所示。

[0074] 表1

[0075]

接入域标识	接入交换机标识	接入网络端口标识	接入网络端口MAC
接入域1	接入交换机1	接入交换机1-接入	MAC接入交换机1-接入
接入域2	接入交换机2	接入交换机2-接入	MAC接入交换机2-接入

[0076] 表2

[0077]

接入域标识	接入交换机标识	接入端口标识	主机标识	主机IP地址	主机MAC地址
接入域1	接入交换机1	接入交换机1-主机1	主机1	IP主机1	MAC主机1
接入域1	接入交换机1	接入交换机1-主机2	主机2	IP主机2	MAC主机2
接入域1	接入交换机1	接入交换机1-主机3	主机3	IP主机3	MAC主机3
接入域2	接入交换机2	接入交换机2-主机4	主机4	IP主机4	MAC主机4
接入域2	接入交换机2	接入交换机2-主机5	主机5	IP主机5	MAC主机5

[0078] 3)SDN控制器在接入交换机上作如下配置：

[0079] ●在ARP表中将连接在接入交换机的主机和MAC地址配对。

[0080] 在接入交换机1上：

[0081] IP主机1-MAC主机1

[0082] IP主机2-MAC主机2

[0083] IP主机3-MAC主机3

[0084] 在接入交换机2上：

[0085] IP主机4-MAC主机4

[0086] IP主机5-MAC主机5

[0087] ●在转发表中制定规则：将目的地址为连接在该交换机上的主机MAC地址和接入网络端口MAC，转发至各自对应的端口。

[0088] 在接入交换机1上：

[0089] 转发端口标识 目的MAC地址

[0090] 接入交换机1-主机1----------MAC主机1

[0091] 接入交换机1-主机2----------MAC主机2

[0092] 接入交换机1-主机3----------MAC主机3

[0093] 接入交换机1-接入----------MAC接入交换机1-接入

[0094] 在接入交换机2上：

[0095] 转发端口标识 目的MAC地址

[0096] 接入交换机2-主机4--------MAC主机4

[0097] 接入交换机2-主机5--------MAC主机5

[0098] 接入交换机2-接入----------MAC接入交换机2-接入

[0099] ●默认规则，丢弃找不到MAC地址的数据报

[0100] ●默认规则，丢弃找不到转发端口的数据报

[0101] 4)从外部接收主机间访问需求，如表3所示

[0102] 表3

[0103]

主机标识	可访问主机标识
主机1	主机2
主机1	主机4
……	……

[0104] 关联表3、表2数据，查看哪些互通的主机在一个接入域内，如表4所示：

[0105] 表4

[0106]

主机标识	可访问主机标识	可访问主机IP地址	可访问主机MAC地址	是否在同一个接入域
主机1	主机2	IP主机2	MAC主机2	是
主机1	主机4	IP主机4	MAC主机4	否
……	……	……	……	……

[0107] 5)SDN控制器在主机上做如下配置：

[0108] ●ARP表中同一个接入域内的可访问主机，IP地址与该主机的MAC匹配

[0109] 主机1上：IP主机2----MAC主机2

[0110] 主机2上：IP主机1----MAC主机1

[0111] ●ARP表中不在同一个接入域内的可访问主机，IP地址与该接入域接入交换机的接入网络端口MAC匹配

[0112] 主机4接入在接入交换机2上，则在主机1上：

[0113] IP主机4----MAC接入交换机1-接入

[0114] 主机1接入在接入交换机1上，则在主机4上：

[0115] IP主机1----MAC接入交换机2-接入

[0116] ●默认规则，丢弃找不到目的MAC地址的数据报。

[0117] 主机1、主机2、主机4均作配置。

[0118] 当主机1向主机2发数据报，则查找主机1上的ARP表，得到目的MAC为“MAC主机2”。主机1向接入交换机1发出目的IP地址为“IP主机2”、目的 MAC地址为“MAC主机2”的数据报。接入交换机1将其转发至“接入交换机1- 主机2端口”。则数据报到达主机2。主机2返回数据报类似。

[0119] 当主机1向主机2发数据报，则查找主机1上的ARP表，得到目的MAC为“MAC接入交换机1-接入”。主机1向接入交换机1发出目的IP地址为“IP主机 4”、目的MAC地址为“MAC接入交换机1-接入”的数据报。接入交换机1将其转发至“MAC接入交换机1-接入”，数据报进入接入交换机间的网络。当数据报到达接入交换机2时，接入交换机2查找ARP表得到“IP主机4”对应MAC地址为“MAC主机4”，又查找转发表得到“MAC主机4”的对应转发端口为“接入交换机2-主机4”。接入交换机2将数据报转发至该端口，数据报到达主机4。主机2返回数据报类似。

[0120] 当主机1向主机3发送数据报，则查找主机1上的ARP表，找不到“IP 主机3”对应的MAC地址，因此丢弃该数据报。主机1无法跟主机3通信。

[0121] 与方法实施例相对应，本发明实施例四还提供一种SDN网络中私有云的访问控制装置，如图4所示，可以包括：

[0122] 信息获取单元1，用于关闭私有云中设备的相应地址功能，并将每个接入设备定义

为一个接入域，获取所述接入域中的主机信息和地址信息。

[0123] 访问规则设定单元2，用于根据所述信息获取单元获取的信息，在所述接入域中配置所述主机和地址的对应关系，设定所述接入域内对各地址的访问规则，所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则。

[0124] 可访问主机确定单元3，根据外部的访问需求结合所述信息获取单元获取的接入域主机信息，确定访问需求中位于相同接入域的可访问主机信息；

[0125] 访问控制单元4，根据所述访问规则设定单元设定的访问规则，对所述可访问主机确定单元中确定的可访问主机进行访问。

[0126] 所述访问控制单元，丢弃所述访问时找不到地址或端口的数据包。

[0127] 优选的，为了使得核查后同步现网资源和核查资源，给出本发明的实施例五如图5所示。

[0128] 信息获取单元1，用于关闭私有云中设备的相应地址功能，并将每个接入设备定义为一个接入域，获取所述接入域中的主机信息和地址信息。

[0129] 访问规则设定单元2进一步包括：

[0130] 地址关系配置模块21，用于根据所述信息获取单元获取的接入域中的主机信息和地址信息，在所述接入域中的接入设备上，配置连接在接入设备的主机地址和MAC地址的对应关系；在所述接入域中的主机上，配置该主机可访问主机地址与所述该主机的MAC地址的对应关系。

[0131] 访问规则设定模块22，用于在接入设备上设定访问规则和在主机上设定访问规则

[0132] 所述访问规则设定模块在接入设备上设定的访问规则具体为：

[0133] 在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对；

[0134] 将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口 MAC地址，转发至各自对应的端口。

[0135] 所述访问规则设定模块在主机上设定的访问规则具体为：

[0136] 在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC 地址进行配对；

[0137] 在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对。

[0138] 可访问主机确定单元3，根据外部的访问需求结合所述信息获取单元获取的接入域主机信息，确定访问需求中位于相同接入域的可访问主机信息；

[0139] 访问控制单元4，根据所述访问规则设定单元设定的访问规则，对所述可访问主机确定单元中确定的可访问主机进行访问。

[0140] 所述访问控制单元，丢弃所述访问时找不到地址或端口的数据包。

[0141] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、单元和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0142] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一

致的最宽的范围。

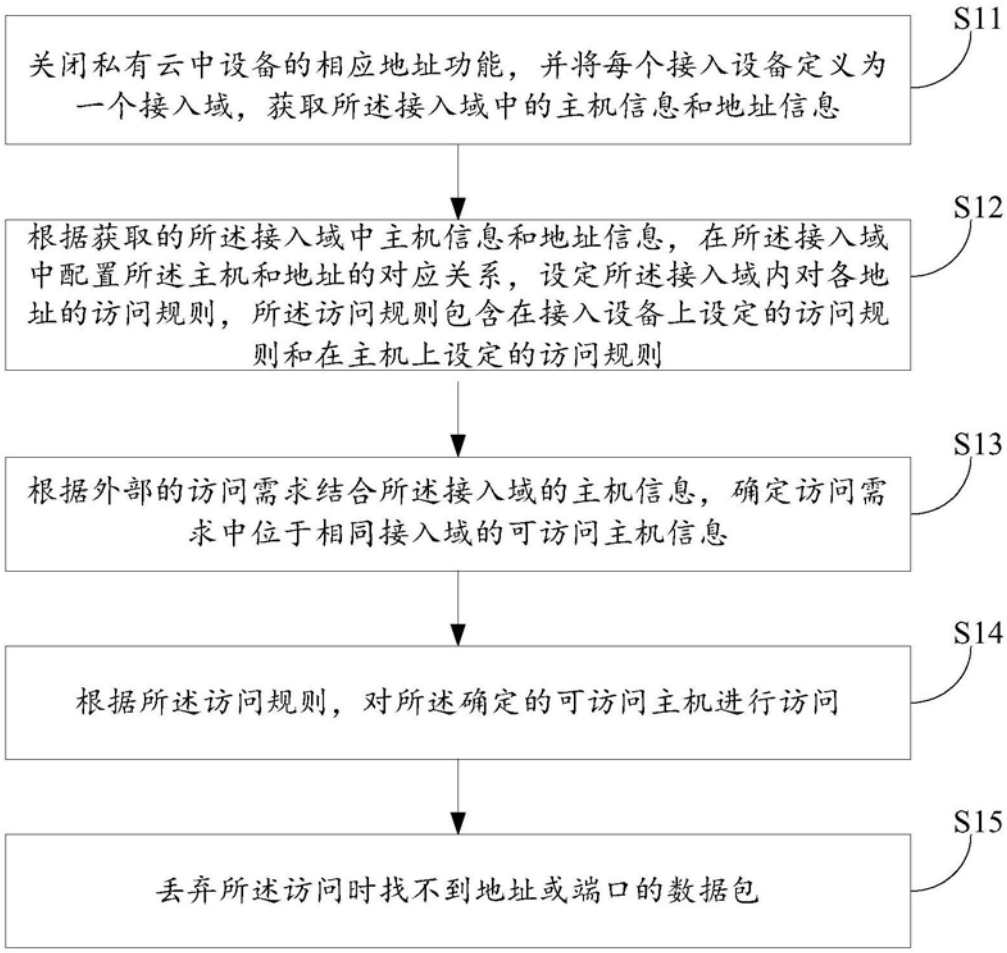

S11
关闭私有云中设备的相应地址功能，并将每个接入设备定义为一个接入域，获取所述接入域中的主机信息和地址信息
S12
根据获取的所述接入域中主机信息和地址信息，在所述接入域中配置所述主机和地址的对应关系，设定所述接入域内对各地址的访问规则，所述访问规则包含在接入设备上设定的访问规则和在主机上设定的访问规则
S13
根据外部的访问需求结合所述接入域的主机信息，确定访问需求中位于相同接入域的可访问主机信息
S14
根据所述访问规则，对所述确定的可访问主机进行访问
S15
丢弃所述访问时找不到地址或端口的数据包

图1

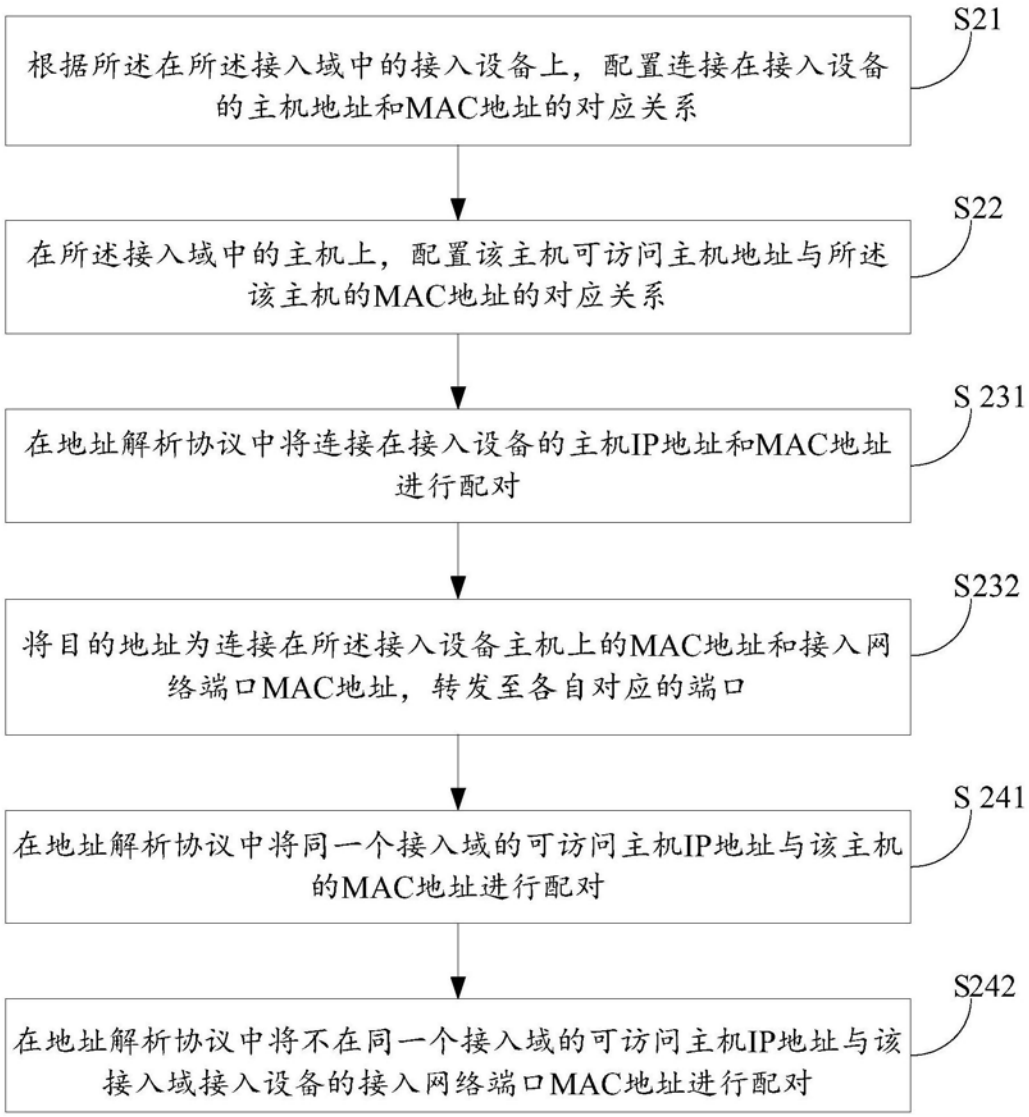

S21
根据所述在所述接入域中的接入设备上，配置连接在接入设备的主机地址和MAC地址的对应关系
S22
在所述接入域中的主机上，配置该主机可访问主机地址与所述该主机的MAC地址的对应关系
S 231
在地址解析协议中将连接在接入设备的主机IP地址和MAC地址进行配对
S232
将目的地址为连接在所述接入设备主机上的MAC地址和接入网络端口MAC地址，转发至各自对应的端口
S 241
在地址解析协议中将同一个接入域的可访问主机IP地址与该主机的MAC地址进行配对
S242
在地址解析协议中将不在同一个接入域的可访问主机IP地址与该接入域接入设备的接入网络端口MAC地址进行配对

图2

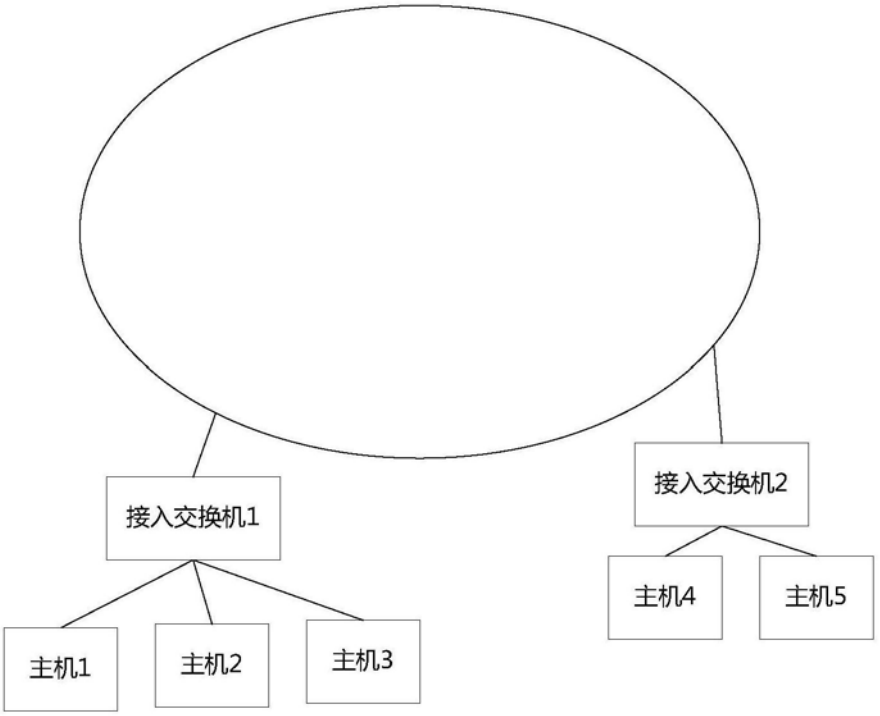

接入交换机1
接入交换机2
主机1
主机2
主机3
主机4
主机5

图3

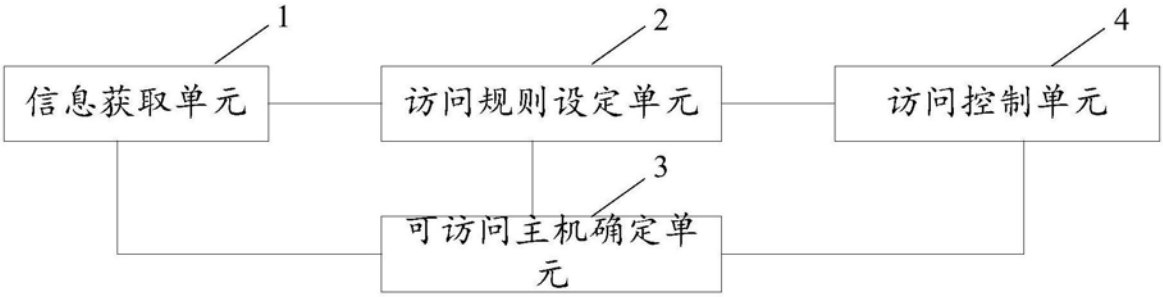

1
2
4
信息获取单元
访问规则设定单元
访问控制单元
3
可访问主机确定单元

图4

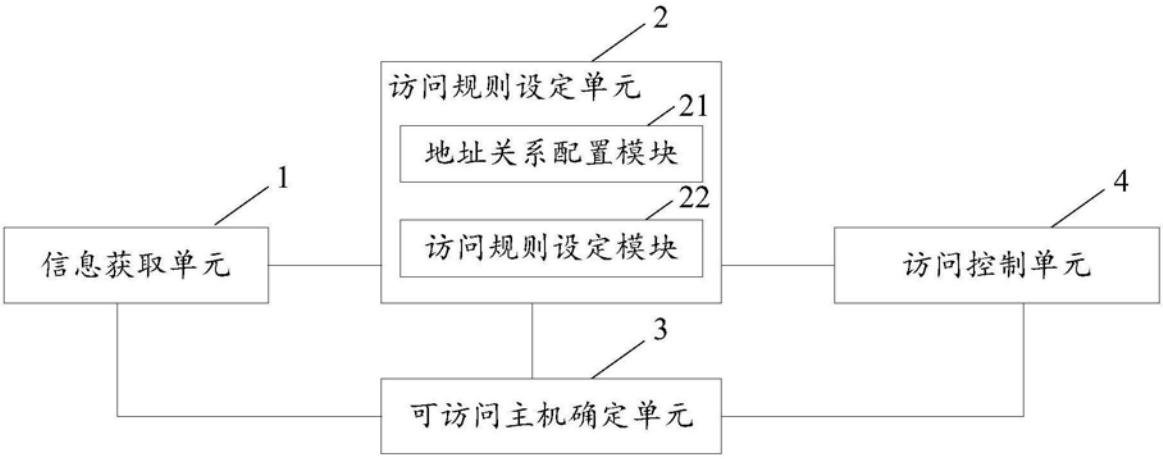

2
访问规则设定单元
21
地址关系配置模块
22
访问规则设定模块
1
信息获取单元
4
访问控制单元
3
可访问主机确定单元

图5